



POLITIQUE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME (LBC/FT)

ORGANISATION:

**ONG - ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-
NUMÉRIQUE (AGCE International – AGCE Canada).**

Version 1.0

Date d'entrée en vigueur: 30 Juillet 2026

AGCE International
Douala - Cameroun



© AGCE International – AGCE Canada. Document classé « Diffusion contrôlée ». Reproduction, copie, transmission ou divulgation interdites sans autorisation écrite. Tous droits réservés.

CADRE OFFICIEL DE CONTACTS

ONG AGCE INTERNATIONAL

AGCE Canada (Québec)

- Action Globale Caritative et Economique-Numérique -

Siège Mondial : Quartier Nylon, République du Cameroun (Douala)

« Plateforme officielle de partenariat, de participation et d'engagement. »

CONTACTS OFFICIELS

 **Téléphones :**

Siège Mondial : (+237) 694 79 47 17 / (+237) 671 40 09 30 / +1(819) 489 0722

Canada +1 (367) 331-1013 / +1 (581) 349-1998



Email :

agce@agce-international.org



WhatsApp officiel :

(+237) 694 79 47 17 / +1 (581) 349-1998 / +1(819) 489 0722

Sites webs:

<https://www.agce-international.org>

<https://www.agceappcenter.store>

PERSONNE RESSOURCE PRINCIPALE

Adresses :

Siège mondial :

Rue coté face au parc de Bonaloka, immeuble du Conseil Supérieur de la Famille Bazou. App 1.
Quartier Nylon - Douala, Cameroun

Emplacement Québec - Canada

227 rue saint Jacques , saint jean sur Richelieu J3B 2k6, App 201 - Canada

DATES & HORAIRES OFFICIELS D'OUVERTURE



Du Lundi au Vendredi



Horaires officiels : 8h00 – 17h00

Classification du document

Nature du document

La présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** constitue un document institutionnel officiel de gouvernance, de conformité financière et de contrôle interne de l'ONG **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle établit le cadre de référence applicable à la prévention, à la détection, à la gestion et au traitement des risques liés au blanchiment de capitaux, au financement du terrorisme, à la fraude financière et aux autres infractions financières susceptibles d'affecter les activités de l'Organisation.

Niveau de classification

Diffusion contrôlée – Usage institutionnel interne et externe autorisé

Ce document est destiné à être communiqué aux membres des organes de gouvernance, aux administrateurs, aux responsables financiers, aux employés, aux bénévoles, aux représentants des antennes nationales et internationales, aux partenaires institutionnels, aux établissements bancaires, aux prestataires de services de paiement, aux auditeurs, aux bailleurs de fonds, aux autorités compétentes ainsi qu'à toute personne ou organisation dont les fonctions nécessitent la connaissance des exigences de conformité appliquées par AGCE International.

Niveau de confidentialité

Le contenu de cette politique est classé « **Diffusion contrôlée** ». Il peut être communiqué dans le cadre des activités institutionnelles de l'Organisation, notamment lors des procédures de vérification préalable (Due Diligence), des audits, des demandes de financement, des évaluations de conformité ou des partenariats stratégiques. En revanche, toute reproduction, modification ou diffusion partielle ou intégrale en dehors de ces finalités doit être préalablement autorisée par l'autorité compétente d'AGCE International.

Caractère obligatoire

Les dispositions de la présente politique sont obligatoires pour l'ensemble des personnes physiques et morales agissant pour le compte ou au nom d'AGCE International – AGCE Canada. Elles s'appliquent à toutes les opérations financières, aux dons, aux cotisations, aux adhésions, aux subventions, aux partenariats, aux projets, aux activités numériques, aux transactions bancaires et aux paiements électroniques réalisés ou administrés par l'Organisation.

Autorité de référence

La présente politique est approuvée par les organes compétents de gouvernance d'AGCE International donc, par le Président Général et Coordinateur Général du Collège Central de l'Organisation ACTION GLOBALE CARITATIVE ET ECONOMIQUE-NUMERIQUE (AGCE International - AGCE Canada et de toute Antenne AGCE dans le monde). Elle constitue un document de référence du dispositif institutionnel de conformité et doit être appliquée conjointement avec les Statuts juridiques et sociaux, le Règlement intérieur, le Code d'éthique et d'intégrité, le Manuel de contrôle interne, la Politique de protection des données et de sécurité numérique, la Politique de gestion des risques, la Politique de lutte contre la fraude et la corruption, ainsi que toute autre politique ou procédure adoptée par l'Organisation.

Durée de validité et révision

La présente politique entre en vigueur à compter de sa date d'approbation par l'autorité compétente de l'Organisation AGCE International. Elle demeure applicable jusqu'à son remplacement ou sa révision officielle. Une évaluation périodique est réalisée afin de garantir son adéquation avec l'évolution de la réglementation, des normes internationales, des risques identifiés et des activités d'AGCE International – AGCE Canada.

Référence documentaire

Pour assurer une gestion documentaire rigoureuse, chaque exemplaire de cette politique fait l'objet d'un système d'identification comprenant un numéro de référence, une version, une date d'entrée en vigueur, une date de révision, un niveau de classification, un statut (brouillon, en cours de validation ou approuvé) ainsi que l'identification de l'autorité ayant procédé à son approbation. Cette traçabilité garantit l'authenticité du document, facilite son suivi administratif et contribue au respect des exigences de gouvernance, de conformité et d'audit applicables aux organisations à vocation nationale et internationale.

Historique des versions

L'historique des versions constitue le registre officiel de gestion documentaire de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de l'ONG **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il assure la traçabilité complète de toutes les modifications apportées au document depuis sa création, en précisant notamment le numéro de version, la date d'émission ou de révision, la nature des changements effectués, les motifs de la mise à jour, les services ou organes responsables de leur élaboration ainsi que l'autorité ayant procédé à leur validation. Ce dispositif garantit que seuls les exemplaires officiellement approuvés sont utilisés au sein de l'Organisation, tout en facilitant les contrôles internes, les audits, les évaluations de conformité et les procédures de gouvernance. Il permet également d'assurer une amélioration continue de la politique afin qu'elle demeure conforme aux évolutions réglementaires, aux normes internationales, aux exigences des partenaires financiers et aux besoins opérationnels d'AGCE International – AGCE Canada.

Version : 1.0

Statut : Première édition officielle

Date d'entrée en vigueur : 30 Juillet 2026

Nous avons intégrer un identifiant documentaire complet afin de faciliter les recherches:

Élément	Référence
Code du document	AGCE-POL-LBCFT-001
Version	V1.0
Édition	Première édition
Statut	Approuvée
Date d'émission	30 Juin 2026
Date d'entrée en vigueur	30 Juillet 2026
Date de révision prévue	29 Juillet 2027
Classification	Diffusion contrôlée

Historique des versions

Version	Date	Nature des modifications	Auteur	Validation
V1.0	30 Juillet 2026	Création et approbation de la première édition de la Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT).	Cellule Conformité et Gouvernance AGCE	Président Général et Coordinateur général du Collège Central / Organe compétent

Cette codification est établie à des fins professionnels, afin de permettre l'exploitation facile lors des audits et peut être harmonisée avec les autres documents institutionnels de l'Organisation AGCE (Manuel de contrôle interne, Charte d'éthique et norme de fonctionnement, Politique de protection des données, Politique de gestion des risques, etc.).

Caractère de diffusion

La présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** est classée « **Diffusion contrôlée – Usage institutionnel** ». Elle est destinée aux organes de gouvernance, aux administrateurs, aux responsables de la conformité, aux collaborateurs, aux auditeurs, aux établissements financiers, aux prestataires de paiement, aux partenaires institutionnels et aux autorités compétentes. Toute reproduction, modification, publication ou diffusion, totale ou partielle, en dehors des finalités institutionnelles d'AGCE International – AGCE Canada est soumise à une autorisation préalable de l'autorité compétente de l'Organisation.

TABLE DES MATIÈRES

A.	PRÉAMBULE.....	Page 9
B.	ACTION GLOBALE CARITATIVE ET ECONOMIQUE-NUMERIQUE C'EST QUOI?.....	Page 10
C.	MISSION - VISION.....	Page 11
D.	ENGAGEMENTS ÉTHIQUES - CONFORMITÉ.....	Page 12
E.	TRANSPARENCE.....	Page 13
F.	RESPONSABILITÉ FINANCIÈRE.....	Page 14
G.	CHAPITRE 1 - DISPOSITIONS GÉNÉRALES.....	Page 15
H.	KYC (KNOW YOUR CUSTOMER / CONNAISSANCE DES MEMBRES,	
I.	PARTENAIRES ET PARTIES PRENANTES).....	Page 19
J.	CHAPITRE 2 - CADRE JURIDIQUE.....	Page 25
K.	CHAPITRE 3 - PRINCIPES FONDAMENTAUX	Page 33
L.	CHAPITRE 4 - GOUVERNANCE LBC/FT.....	Page 42
M.	CHAPITRE 5 - APPROCHE BASÉE SUR LES RISQUES	Page 59
N.	CHAPITRE 6 - KYC – CONNAISSANCE DES MEMBRES ET PARTENAIRES.....	Page 74
O.	CHAPITRE 7 - ACCEPTATION DES DONS ET FINANCEMENTS.....	Page 83
P.	CHAPITRE 8 - CONTRÔLE OPÉRATIONNEL, SURVEILLANCE DES OPÉRATIONS, SÉCURITÉ FINANCIÈRE, CONFORMITÉ ET AMÉLIORATION CONTINUE	Page 93
Q.	SECTION I - SURVEILLANCE PERMANENTE DES OPÉRATIONS FINANCIÈRES.....	Page 96
R.	SECTION II - DÉTECTION DES OPÉRATIONS SUSPECTES.....	Page 106
S.	SECTION III - CONTRÔLE INTERNE.....	Page 117
T.	SECTION IV - SÉCURITÉ DES PAIEMENTS.....	Page 128
U.	SECTION V - CONSERVATION DOCUMENTAIRE.....	Page 150
V.	SECTION VI - PROTECTION DES LANCEURS D'ALERTE.....	Page 62
W.	SECTION VII - FORMATION ET SENSIBILISATION.....	Page 173
X.	SECTION VIII - GESTION DES INCIDENTS	Page 189
Y.	SECTION IX - AUDIT, CONFORMITÉ ET AMÉLIORATION CONTINUE.....	Page 207
Z.	SECTION X - ANCTIONS DISCIPLINAIRES.....	Page 224
AA.	SECTION XI - RÉVISION DE LA POLITIQUE.....	Page 240
AB.	ANNEXES.....	Page 256
AC.	FORMULAIRE OFFICIEL DE DÉCLARATION D'OPÉRATION SUSPECTE (DOS).....	Page 272
AD.	CHARTRE D'ENGAGEMENT DES COLLABORATEURS EN MATIÈRE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME (LBC/FT).....	Page 292

PRÉAMBULE

Présentation

La présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** constitue un document institutionnel de référence de l'ONG **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle s'inscrit dans la volonté permanente de l'Organisation de promouvoir une gouvernance responsable, une gestion financière transparente et une conformité rigoureuse aux normes nationales et internationales applicables aux organisations à but non lucratif, aux organismes de bienfaisance et aux partenaires de coopération internationale.

En tant qu'organisation engagée dans l'action humanitaire, le développement durable, l'inclusion sociale, l'innovation numérique, la formation, la santé, l'éducation et l'autonomisation économique des populations, AGCE International mobilise et administre des ressources financières provenant notamment des cotisations, adhésions, dons, subventions, partenariats, prestations de services et autres financements licites. À ce titre, elle reconnaît sa responsabilité de protéger l'intégrité de ses activités contre tout risque d'utilisation abusive à des fins de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption ou de toute autre activité financière illicite.

Cette politique établit les principes, responsabilités, procédures et mécanismes de contrôle destinés à prévenir, détecter, évaluer et traiter les risques liés à la criminalité financière. Elle repose sur une approche fondée sur les risques, la vigilance raisonnable, la traçabilité des opérations, la connaissance des membres, partenaires et donateurs, ainsi que le renforcement des dispositifs de contrôle interne et d'audit. Elle s'applique à l'ensemble des organes de gouvernance, dirigeants, administrateurs, collaborateurs, bénévoles, représentants des antennes nationales et internationales, partenaires techniques et financiers, ainsi qu'à toute personne agissant pour le compte ou au nom d'AGCE International – AGCE Canada. Par cette démarche, l'Organisation réaffirme son engagement en faveur de l'intégrité, de la transparence, de la redevabilité et du respect des meilleures pratiques internationales de conformité financière.

ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE- NUMÉRIQUE (AGCE)

C'est quoi?

(AGCE International – AGCE Canada)

L'**ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE)**, connue sous les appellations **AGCE International** et **AGCE Canada** pour son antenne nord-américaine, est une organisation non gouvernementale à vocation nationale et internationale, engagée dans la promotion du développement humain durable, de l'action humanitaire, de l'inclusion sociale, de l'innovation numérique, de l'éducation, de la santé, de la protection de l'environnement, de la bonne gouvernance et de l'autonomisation économique des populations. À travers ses programmes et partenariats, l'Organisation œuvre à renforcer les capacités des individus, des communautés, des institutions et des entreprises en favorisant des solutions durables, inclusives et innovantes répondant aux enjeux contemporains du développement.

Le **siège mondial d'AGCE International** est situé au **Quartier Nylon, Immeuble du Conseil Supérieur de la Famille Bazou, 3^e étage, Appartement 1, Rue du côté du Parc de Bonaloka, Douala, République du Cameroun**. Son **antenne officielle en Amérique du Nord, AGCE Canada**, est établie au **227, rue Saint-Jacques, Appartement 201, Saint-Jean-sur-Richelieu, Québec J3B 2K6, Canada**. Cette implantation internationale permet à l'Organisation de coordonner efficacement ses actions de coopération, de solidarité, de mobilisation des ressources et de développement de partenariats stratégiques entre l'Afrique, le Canada et le reste du monde.

Dans le cadre de son expansion internationale, **AGCE International dispose également de représentants et d'antennes officielles dans plus de quinze (15) pays**, couvrant notamment plusieurs États d'Afrique, d'Amérique du Nord et d'Europe, y compris la **France** ainsi que d'autres pays de l'**Union européenne**. Ce réseau international favorise la mise en œuvre de projets de coopération, le renforcement des échanges institutionnels, la mobilisation des compétences et la réalisation d'initiatives humanitaires et de développement au bénéfice des populations.

Afin d'obtenir des informations actualisées sur la gouvernance de l'Organisation, ses représentations nationales et internationales, ses programmes, ses projets, ses partenaires, ses modalités d'adhésion ainsi que ses activités institutionnelles, les lecteurs sont invités à consulter la **plateforme web officielle d'AGCE International**, qui constitue la source officielle de référence pour l'ensemble des informations, publications et communications de l'Organisation. Cette plateforme permet également de découvrir le réseau mondial d'AGCE, ses opportunités de collaboration et les moyens de contribuer à ses actions au service d'un développement durable, solidaire et responsable.

Mission

La mission de l'**ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** est de promouvoir un développement humain, économique, social et numérique inclusif au bénéfice des populations, en particulier des personnes vulnérables, des jeunes, des femmes, des enfants, des personnes en situation de handicap, des communautés rurales, des entrepreneurs, des organisations communautaires et des institutions publiques ou privées. L'Organisation agit comme un acteur de solidarité, de coopération et d'innovation en concevant, coordonnant et mettant en œuvre des programmes à fort impact dans les domaines de l'action humanitaire, de la santé, de l'éducation, de la formation professionnelle, de la transformation numérique, de la protection de l'environnement, de l'inclusion financière, de l'entrepreneuriat, de la création d'emplois durables et du renforcement des capacités institutionnelles. Par ses partenariats nationaux et internationaux, AGCE International favorise également la mobilisation des ressources, le transfert de compétences, l'accompagnement des projets de développement, la promotion des bonnes pratiques de gouvernance, ainsi que l'utilisation responsable des technologies numériques au service du bien commun. Dans l'ensemble de ses interventions, l'Organisation veille à agir dans le respect des principes d'éthique, de transparence, de responsabilité, de conformité, de redevabilité et de dignité humaine, afin de contribuer durablement à l'amélioration des conditions de vie des populations et à la réalisation des Objectifs de Développement Durable.

Vision

La vision d'**AGCE International – AGCE Canada** est de devenir une organisation de référence, reconnue au Cameroun, au Canada et à l'échelle internationale pour son engagement en faveur d'un développement durable, solidaire et innovant, fondé sur la coopération internationale, la bonne gouvernance et la transformation numérique. L'Organisation ambitionne de bâtir un réseau mondial capable de rapprocher les citoyens, les collectivités, les entreprises, les institutions publiques, les universités, les fondations et les partenaires techniques et financiers autour de projets générateurs d'impacts économiques, sociaux et environnementaux mesurables. Elle aspire à faire du numérique un levier d'inclusion, de création d'emplois, d'amélioration des services essentiels et de réduction des inégalités, tout en renforçant la résilience des communautés face aux défis contemporains. À travers une gouvernance exemplaire, une gestion transparente des ressources et une culture permanente de l'innovation, AGCE International entend développer un modèle institutionnel fondé sur la confiance, la conformité, la responsabilité et l'excellence opérationnelle. Sa vision est de contribuer à l'émergence d'une société où chaque individu, organisation et communauté dispose des moyens de participer pleinement au développement économique, social et humain, dans un esprit de solidarité internationale, de paix, de justice, d'inclusion et de prospérité partagée.

Engagements éthiques

L'**ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** fonde l'ensemble de ses activités sur des valeurs d'intégrité, de responsabilité, de transparence, de respect de la dignité humaine et d'intérêt général. Convaincue que la confiance constitue le fondement de toute action humanitaire, sociale et institutionnelle durable, l'Organisation s'engage à exercer ses missions avec impartialité, honnêteté, professionnalisme et équité, dans le strict respect des lois applicables et des principes universels des droits humains. Chaque décision, chaque partenariat, chaque projet et chaque opération financière doit contribuer à la réalisation de sa mission sans porter atteinte aux valeurs qui guident son action.

À ce titre, AGCE International applique une politique de **tolérance zéro** à l'égard de toute forme de corruption, de fraude, de blanchiment de capitaux, de financement du terrorisme, de détournement de ressources, de conflit d'intérêts, de discrimination, de harcèlement, d'exploitation, de favoritisme, de trafic d'influence ou de toute autre pratique contraire aux principes de bonne gouvernance. Les administrateurs, dirigeants, membres, salariés, bénévoles, consultants, représentants nationaux et internationaux, partenaires, prestataires ainsi que toute personne agissant pour le compte de l'Organisation sont tenus d'adopter un comportement exemplaire, loyal et conforme aux règles éthiques définies par les documents institutionnels d'AGCE International.

L'Organisation veille également à promouvoir une culture institutionnelle fondée sur la responsabilité individuelle et collective, la protection des lanceurs d'alerte, la confidentialité des informations sensibles, la prévention des risques, la reddition des comptes, l'utilisation responsable des ressources financières, matérielles et numériques, ainsi que le respect des engagements pris envers les bénéficiaires, les donateurs, les bailleurs de fonds, les autorités publiques et les partenaires nationaux et internationaux. Ces engagements éthiques constituent un cadre permanent de référence pour préserver la crédibilité, la réputation et la pérennité de l'Organisation dans toutes les juridictions où elle exerce ses activités.

Conformité

La conformité représente un pilier fondamental du système de gouvernance d'**AGCE International – AGCE Canada**. L'Organisation s'engage à exercer l'ensemble de ses activités dans le respect des dispositions légales, réglementaires, fiscales, comptables, administratives et financières applicables dans les pays où elle intervient, ainsi qu'en conformité avec les exigences des partenaires techniques et financiers, des institutions bancaires, des organismes de contrôle et des standards internationaux de gouvernance des organisations à but non lucratif.

Afin de garantir une gestion responsable et sécurisée de ses opérations, AGCE International met en œuvre un dispositif intégré de conformité reposant notamment sur la gestion des

risques, le contrôle interne, la séparation des fonctions, la traçabilité des opérations, les procédures de validation et d'autorisation, la conservation des documents, la protection des données, la cybersécurité, les dispositifs de connaissance des membres et partenaires (KYC), les mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), la prévention de la fraude et de la corruption, ainsi que les mécanismes d'audit interne et externe.

Cette démarche est soutenue par un ensemble cohérent de politiques, manuels, procédures, codes de conduite et mécanismes de suivi permettant d'assurer une amélioration continue du système de gouvernance institutionnelle. Chaque collaborateur, administrateur, membre ou représentant de l'Organisation est responsable du respect des exigences de conformité applicables à ses fonctions et doit signaler sans délai toute situation susceptible de compromettre l'intégrité de l'Organisation ou de contrevenir aux lois en vigueur.

Par cette approche proactive, AGCE International renforce la confiance de ses bénéficiaires, de ses partenaires, des bailleurs de fonds, des autorités publiques et des institutions financières. Elle affirme ainsi sa volonté de maintenir un environnement institutionnel fondé sur la légalité, la transparence, la redevabilité, la maîtrise des risques et l'amélioration continue, afin de garantir la pérennité de ses missions humanitaires, sociales et de développement durable.

Transparence

L'ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada) considère la transparence comme un principe fondamental de sa gouvernance institutionnelle et de sa relation de confiance avec ses membres, bénéficiaires, donateurs, partenaires, autorités publiques, institutions financières et bailleurs de fonds. L'Organisation s'engage à conduire l'ensemble de ses activités avec clarté, honnêteté et ouverture, en veillant à ce que chaque décision administrative, financière et opérationnelle puisse être justifiée, documentée, contrôlée et, lorsque cela est approprié, communiquée aux parties prenantes concernées.

Cette exigence de transparence s'applique à toutes les étapes du cycle de gestion des ressources de l'Organisation, depuis la mobilisation des financements jusqu'à leur affectation, leur utilisation, leur suivi et leur évaluation. AGCE International met en œuvre des procédures garantissant la traçabilité des opérations, la conservation des pièces justificatives, l'enregistrement fidèle des transactions, la séparation des responsabilités, la validation des engagements financiers ainsi que la production régulière de rapports administratifs, financiers et techniques permettant d'apprécier l'utilisation des ressources conformément aux objectifs institutionnels.

L'Organisation veille également à fournir à ses partenaires et aux autorités compétentes des informations fiables, exactes, actualisées et vérifiables concernant ses activités, sa gouvernance, ses projets, ses mécanismes de contrôle interne et sa situation financière, dans

le respect des obligations légales, réglementaires, contractuelles et des exigences de confidentialité. Cette démarche favorise un climat de confiance durable, renforce la crédibilité institutionnelle d'AGCE International et contribue à prévenir les risques de fraude, de corruption, de mauvaise gestion, de conflits d'intérêts et de toute utilisation abusive des ressources.

La transparence constitue ainsi un levier essentiel de bonne gouvernance permettant d'assurer la redevabilité de l'Organisation envers l'ensemble de ses parties prenantes, de soutenir une prise de décision éclairée et de consolider la réputation d'AGCE International comme organisation responsable, intègre et conforme aux meilleures pratiques nationales et internationales.

Responsabilité financière

La responsabilité financière constitue un engagement permanent d'**AGCE International – AGCE Canada** en faveur d'une gestion rigoureuse, prudente et efficiente des ressources qui lui sont confiées. Qu'elles proviennent des cotisations des membres, des dons, des subventions, des partenariats, des prestations de services, des activités génératrices de revenus ou de toute autre source licite, ces ressources sont administrées dans le seul intérêt de la mission institutionnelle et conformément aux principes de légalité, d'efficacité, d'économie, de transparence et de redevabilité.

L'Organisation met en place un système structuré de gouvernance financière reposant sur des règles de contrôle interne, la séparation des fonctions, la validation hiérarchique des dépenses, l'autorisation préalable des engagements financiers, la gestion budgétaire, le rapprochement bancaire, la traçabilité des paiements, l'archivage des pièces comptables ainsi que des mécanismes réguliers de contrôle, d'audit et d'évaluation. Chaque opération financière doit être justifiée, documentée, enregistrée de manière fidèle et pouvoir être vérifiée à tout moment par les instances compétentes ou les organismes de contrôle autorisés.

Les administrateurs, dirigeants, responsables financiers, gestionnaires de projets, collaborateurs, représentants d'antennes et toute personne amenée à gérer ou engager des ressources de l'Organisation sont individuellement et collectivement responsables du respect des procédures financières en vigueur. Ils doivent exercer leurs fonctions avec intégrité, diligence et impartialité, prévenir toute situation de conflit d'intérêts, signaler toute anomalie ou irrégularité constatée et coopérer pleinement avec les dispositifs de contrôle interne et externe.

Dans cette perspective, AGCE International s'engage à maintenir un environnement financier sécurisé, conforme aux exigences réglementaires, aux normes comptables applicables et aux standards internationaux de gouvernance des organisations à but non lucratif. Cette responsabilité financière contribue à préserver la confiance des donateurs, des membres, des partenaires institutionnels, des établissements financiers et des bailleurs de fonds, tout en garantissant la pérennité des programmes humanitaires, sociaux, éducatifs, sanitaires et de développement durable portés par l'Organisation.

CHAPITRE 1

DISPOSITIONS GÉNÉRALES

Le présent chapitre établit les dispositions générales applicables à la **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de l'**ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il définit le cadre institutionnel dans lequel s'inscrivent les principes, règles et mécanismes destinés à prévenir, détecter, signaler et traiter les risques liés au blanchiment de capitaux, au financement du terrorisme et aux autres formes de criminalité financière susceptibles d'affecter l'Organisation, ses partenaires ou ses bénéficiaires.

Cette politique constitue une référence obligatoire pour l'ensemble des organes de gouvernance, des dirigeants, des administrateurs, des collaborateurs, des bénévoles, des représentants des antennes nationales et internationales, des consultants, des prestataires, des partenaires institutionnels et de toute personne physique ou morale agissant pour le compte d'AGCE International – AGCE Canada. Elle s'applique à toutes les activités, opérations financières, partenariats, programmes, projets, collectes de fonds, dons, cotisations, subventions, prestations de services et transactions réalisées ou administrées par l'Organisation, quels que soient leur nature, leur montant ou leur origine.

Les dispositions du présent chapitre doivent être interprétées conjointement avec les statuts de l'Organisation, son règlement intérieur, son code d'éthique, ses politiques de gouvernance, de contrôle interne, de gestion des risques, de protection des données, de lutte contre la fraude et la corruption, ainsi qu'avec l'ensemble des lois, règlements et normes applicables dans les pays où AGCE International exerce ses missions. Elles constituent le socle juridique, administratif et opérationnel garantissant une gouvernance responsable, une conformité permanente, une gestion transparente des ressources et la protection de l'intégrité institutionnelle de l'Organisation.

1.1 Objet

La présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** a pour objet d'établir le cadre institutionnel, les principes directeurs, les responsabilités, les procédures et les mécanismes de contrôle permettant à l'**ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de prévenir, détecter, évaluer, signaler et gérer les risques liés au blanchiment de capitaux, au financement du terrorisme, à la fraude, à la corruption et à toute autre forme de criminalité financière susceptible de compromettre l'intégrité de l'Organisation. Elle vise à garantir que toutes les ressources financières, matérielles, humaines et numériques mobilisées ou administrées par AGCE International proviennent de sources licites, sont utilisées conformément à leur destination et font l'objet d'une gestion transparente, traçable et conforme aux exigences légales, réglementaires et institutionnelles applicables.

Cette politique constitue également un référentiel obligatoire pour l'ensemble des acteurs intervenant dans les activités de l'Organisation et contribue à renforcer la confiance des membres, des bénéficiaires, des partenaires, des établissements financiers, des bailleurs de fonds et des autorités publiques.

1.2 Champ d'application

La présente politique s'applique à l'ensemble des structures, programmes, projets, représentations nationales et internationales, antennes, bureaux de liaison et entités opérationnelles de **l'AGCE International**, y compris **AGCE Canada** ainsi que toute autre représentation officielle créée conformément aux statuts de l'Organisation. Elle est obligatoire pour les membres des organes de gouvernance, les dirigeants, les administrateurs, les responsables financiers, les gestionnaires de projets, les salariés, les bénévoles, les consultants, les représentants, les partenaires techniques et financiers, les prestataires, les fournisseurs, les intermédiaires, les donateurs et toute personne physique ou morale agissant directement ou indirectement pour le compte de l'Organisation. Elle couvre l'ensemble des opérations financières, bancaires, comptables, administratives et numériques, notamment les adhésions, cotisations, dons, subventions, financements, appels à projets, marchés, conventions, achats, ventes de services, transferts de fonds, paiements électroniques, opérations internationales, collectes de fonds, campagnes de financement participatif et toute autre transaction susceptible d'exposer l'Organisation à un risque de criminalité financière.

1.3 Finalités

La présente politique a pour finalité de protéger l'intégrité institutionnelle, financière et réputationnelle d'**AGCE International – AGCE Canada** en mettant en place un dispositif permanent de prévention, de vigilance et de maîtrise des risques liés au blanchiment de capitaux et au financement du terrorisme. Elle vise à assurer la conformité de l'Organisation aux exigences légales et réglementaires applicables, à renforcer la gouvernance, à sécuriser les relations avec les partenaires nationaux et internationaux, les établissements financiers, les organismes de coopération et les bailleurs de fonds, ainsi qu'à garantir une utilisation responsable, transparente et traçable des ressources confiées à l'Organisation. Cette politique favorise également le développement d'une culture institutionnelle fondée sur l'éthique, la responsabilité, la redevabilité, la vigilance, le contrôle interne, la gestion des risques et l'amélioration continue, afin de préserver durablement la crédibilité d'AGCE International, de soutenir la réalisation de ses missions humanitaires, sociales et de développement durable, et de contribuer activement à la lutte contre toutes les formes de criminalité financière au niveau national et international.

1.4 Définitions

Aux fins de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, les termes ci-après sont interprétés conformément aux principes généralement reconnus en matière de conformité financière, de gouvernance, de prévention de la criminalité financière et aux réglementations applicables dans les juridictions où **AGCE International – AGCE Canada** exerce ses activités. Ces définitions constituent un cadre commun de compréhension destiné à assurer une application uniforme de la présente politique au sein de l'ensemble des organes de gouvernance, des antennes nationales et internationales, des collaborateurs, des partenaires et des parties prenantes de l'Organisation.

Blanchiment de capitaux

Le **blanchiment de capitaux** désigne tout processus, toute opération ou tout ensemble d'actes visant à dissimuler, transformer, transférer, convertir, utiliser ou intégrer dans les circuits économiques et financiers légaux des biens, fonds, valeurs ou actifs provenant directement ou indirectement d'une activité criminelle ou illicite. Cette pratique a pour objectif de masquer l'origine réelle des ressources afin de leur conférer une apparence de légalité et de permettre leur réutilisation dans des opérations financières, commerciales ou patrimoniales.

Le blanchiment de capitaux peut prendre différentes formes, notamment par l'utilisation de comptes bancaires, de sociétés écrans, d'organisations fictives, de transactions internationales, de dons, de subventions, d'opérations commerciales simulées, d'investissements, d'actifs numériques ou de tout autre mécanisme destiné à rendre difficile l'identification de l'origine des fonds. Les méthodes employées évoluent constamment et peuvent exploiter les nouvelles technologies, les plateformes numériques ou les flux financiers transfrontaliers.

Dans le cadre de ses activités, **AGCE International – AGCE Canada** interdit strictement toute participation, directe ou indirecte, à une opération susceptible de favoriser le blanchiment de capitaux. L'Organisation met en œuvre des procédures de vigilance, de connaissance des membres et partenaires (KYC), de vérification de l'origine des fonds, de traçabilité des transactions, de contrôle interne, d'audit et de gestion des risques afin de prévenir toute tentative d'utilisation abusive de ses structures, de ses programmes, de ses plateformes numériques ou de ses ressources à des fins de blanchiment.

Terrorisme

Le **terrorisme** désigne tout acte, toute menace, toute organisation ou toute activité ayant pour objectif de provoquer un climat de peur, de violence ou d'intimidation afin d'imposer des revendications idéologiques, politiques, religieuses ou criminelles par des moyens contraires aux lois nationales et au droit international. Le **financement du terrorisme** consiste

à fournir, collecter, transférer, mettre à disposition, gérer ou faciliter, directement ou indirectement, des fonds, des biens, des ressources matérielles, des services ou tout autre moyen destiné à soutenir, préparer ou permettre la réalisation d'activités terroristes ou le fonctionnement d'organisations, de groupes ou d'individus impliqués dans de telles activités, indépendamment de l'origine licite ou illicite des ressources utilisées.

AGCE International – AGCE Canada applique une politique de **tolérance zéro** à l'égard de toute forme de terrorisme, d'extrémisme violent et de financement d'activités terroristes. À cette fin, l'Organisation met en œuvre des mesures de diligence raisonnable, de vérification des partenaires, des bénéficiaires, des donateurs, des fournisseurs et des autres parties prenantes, ainsi que des mécanismes de surveillance des opérations financières, de signalement des situations suspectes, de coopération avec les autorités compétentes dans le respect du cadre légal applicable et de formation continue des personnes concernées. Ces mesures visent à préserver l'intégrité de l'Organisation, à protéger ses ressources et à garantir que l'ensemble de ses activités humanitaires, sociales, éducatives et de développement durable demeure exclusivement consacré à des objectifs licites, pacifiques et conformes à ses valeurs institutionnelles.

Financement du terrorisme

Le **financement du terrorisme** désigne tout acte consistant à collecter, fournir, recevoir, détenir, transférer, gérer, mettre à disposition ou utiliser, directement ou indirectement, des fonds, des biens, des ressources matérielles, des services, des actifs numériques ou tout autre moyen ayant pour objet ou pour effet de soutenir la préparation, l'organisation, le fonctionnement ou la réalisation d'activités terroristes. Contrairement au blanchiment de capitaux, les ressources utilisées pour financer des activités terroristes peuvent provenir aussi bien d'activités illicites que de sources parfaitement licites, telles que des dons, des cotisations, des subventions, des collectes de fonds, des revenus commerciaux ou des contributions individuelles, lorsqu'elles sont détournées de leur finalité initiale.

Consciente de cette réalité, **AGCE International – AGCE Canada** applique une politique de **tolérance zéro** envers toute forme de financement du terrorisme, de soutien à des organisations interdites, à des groupes extrémistes ou à des individus impliqués dans des activités criminelles ou violentes. L'Organisation veille à ce qu'aucune de ses ressources humaines, financières, matérielles, logistiques, numériques ou institutionnelles ne puisse être utilisée, directement ou indirectement, pour faciliter ou favoriser de telles activités.

Afin de prévenir ces risques, AGCE International met en œuvre un dispositif permanent de vigilance reposant sur l'identification et la vérification des parties prenantes, l'analyse de l'origine et de la destination des fonds, la traçabilité des opérations financières, la surveillance des transactions nationales et internationales, l'évaluation des risques liés aux projets, aux partenaires, aux bénéficiaires et aux fournisseurs, ainsi que l'application de procédures de contrôle interne, d'audit et de signalement des opérations inhabituelles ou suspectes. L'Organisation s'engage également à coopérer avec les autorités légalement

compétentes dans le respect des lois applicables, des obligations de confidentialité et des principes de protection des données personnelles.

L'ensemble des administrateurs, dirigeants, collaborateurs, bénévoles, représentants des antennes, consultants, partenaires et prestataires sont tenus de respecter strictement ces exigences et de signaler sans délai toute situation susceptible de présenter un risque de financement du terrorisme. Cette vigilance collective contribue à protéger l'intégrité, la réputation et la crédibilité d'AGCE International tout en garantissant que ses ressources demeurent exclusivement affectées à des objectifs humanitaires, sociaux, éducatifs, sanitaires, environnementaux et de développement durable.

KYC (Know Your Customer / Connaissance des Membres, Partenaires et Parties Prenantes)

Le **KYC (Know Your Customer)**, ou **Connaissance des Membres, Partenaires et Parties Prenantes**, constitue un mécanisme essentiel du dispositif de conformité de **AGCE International – AGCE Canada**. Il regroupe l'ensemble des procédures permettant d'identifier, de vérifier, de documenter et d'actualiser les informations relatives aux personnes physiques ou morales qui entretiennent une relation avec l'Organisation, notamment les membres, donateurs, bénéficiaires, partenaires institutionnels, bailleurs de fonds, fournisseurs, prestataires, consultants, représentants d'antennes et autres parties prenantes.

L'objectif principal du KYC est de permettre à l'Organisation de connaître avec un niveau raisonnable de certitude l'identité, le statut juridique, les activités, la provenance des ressources, les bénéficiaires effectifs, la réputation et, lorsque cela est pertinent, le niveau de risque associé à chaque relation. Cette démarche contribue à prévenir le blanchiment de capitaux, le financement du terrorisme, la fraude, la corruption, les conflits d'intérêts, les usurpations d'identité et toute tentative d'utilisation abusive des activités ou des ressources d'AGCE International.

Dans le cadre de ce dispositif, l'Organisation peut demander des documents d'identification, des justificatifs de domicile, des pièces d'immatriculation, des statuts, des informations sur les représentants légaux, des références bancaires, des justificatifs de l'origine des fonds ou tout autre document nécessaire à l'évaluation du niveau de risque. Les informations recueillies sont vérifiées, mises à jour périodiquement, conservées de manière sécurisée et traitées conformément à la politique de protection des données personnelles et aux obligations légales applicables.

Le niveau de diligence appliqué est proportionné au risque présenté par chaque relation. Les situations présentant un risque élevé peuvent faire l'objet de contrôles renforcés, d'une surveillance accrue, d'une validation hiérarchique spécifique ou, si nécessaire, du refus, de la suspension ou de la cessation de la relation institutionnelle. Par cette approche fondée sur les risques, AGCE International renforce la sécurité de ses opérations, protège ses parties prenantes et consolide son engagement en faveur d'une gouvernance responsable,

transparente, conforme et respectueuse des meilleures pratiques internationales en matière de conformité financière.

Personne Politiquement Exposée (PPE)

Une **Personne Politiquement Exposée (PPE)** est une personne physique qui exerce ou a exercé d'importantes fonctions publiques au niveau national, régional ou international, ainsi que les membres de sa famille proche et les personnes connues pour lui être étroitement associées. En raison des responsabilités qu'elles occupent ou ont occupées, ces personnes peuvent être davantage exposées aux risques de corruption, de détournement de fonds publics, de trafic d'influence, de blanchiment de capitaux ou d'autres infractions financières. Cette qualification ne constitue en aucun cas une présomption de culpabilité ou d'irrégularité, mais implique l'application de mesures de vigilance renforcées conformément aux exigences de conformité et de gestion des risques.

Aux fins de la présente politique, peuvent notamment être considérés comme PPE les chefs d'État et de gouvernement, ministres, parlementaires, hauts magistrats, responsables des forces de défense et de sécurité, dirigeants d'entreprises publiques, hauts fonctionnaires, ambassadeurs, dirigeants d'organisations internationales, responsables d'autorités administratives indépendantes ainsi que toute autre personne occupant une fonction équivalente définie par la réglementation applicable.

Dans le cadre de ses activités, **AGCE International – AGCE Canada** applique une approche fondée sur les risques lorsqu'une relation est établie avec une PPE. Cette approche comprend notamment l'identification de la qualité de PPE, la vérification de l'identité, l'évaluation de l'origine des fonds, l'analyse de la nature de la relation envisagée, l'autorisation préalable par les responsables compétents lorsque cela est requis, ainsi qu'un suivi renforcé des opérations présentant un niveau de risque élevé. Ces contrôles sont réalisés dans le respect des principes de confidentialité, de non-discrimination, de protection des données personnelles et des droits fondamentaux des personnes concernées.

L'Organisation veille à ce que toute relation avec une PPE demeure conforme aux lois applicables, aux exigences de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), ainsi qu'à ses propres règles de gouvernance, d'éthique et de transparence. Les informations recueillies sont strictement limitées à ce qui est nécessaire pour apprécier le niveau de risque et sont conservées de manière sécurisée conformément aux politiques internes de protection des données.

Donateur

Au sens de la présente politique, un **donateur** désigne toute personne physique ou morale qui apporte volontairement à **AGCE International – AGCE Canada** un soutien financier, matériel, technique, technologique ou en nature, sans contrepartie commerciale

directe, afin de contribuer à la réalisation de ses missions humanitaires, sociales, éducatives, sanitaires, environnementales, numériques, culturelles ou de développement durable. Les donateurs peuvent être des particuliers, des entreprises, des fondations, des associations, des organisations internationales, des institutions publiques, des collectivités territoriales, des établissements d'enseignement, des organismes de coopération, des partenaires philanthropiques ou toute autre entité légalement habilitée à effectuer un don.

AGCE International reconnaît que les dons constituent une ressource essentielle au financement de ses programmes et s'engage à les recevoir, les administrer et les utiliser conformément aux principes de légalité, de transparence, de traçabilité, de responsabilité financière et de redevabilité. L'Organisation veille à ce que chaque contribution soit affectée selon les objectifs convenus avec le donateur, lorsqu'une affectation spécifique est prévue, ou selon les priorités institutionnelles définies par ses organes compétents lorsque le don est non affecté.

Dans le cadre de son dispositif de conformité LBC/FT, AGCE International met en œuvre des procédures de diligence raisonnable applicables aux donateurs lorsque le niveau de risque, la nature du don, son montant, son origine géographique ou les exigences réglementaires le justifient. Ces procédures peuvent inclure la vérification de l'identité du donateur, l'identification du bénéficiaire effectif pour les personnes morales, l'évaluation de la provenance des fonds, l'analyse de la réputation du donateur, ainsi que toute autre mesure de contrôle jugée nécessaire pour prévenir les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption ou d'atteinte à l'intégrité de l'Organisation.

AGCE International se réserve le droit de refuser, de suspendre ou de restituer tout don lorsqu'il existe des motifs raisonnables de croire que les ressources proposées proviennent d'activités illicites, sont destinées à des fins incompatibles avec les valeurs de l'Organisation ou sont susceptibles d'exposer celle-ci à un risque juridique, financier, réputationnel ou de non-conformité. Par cette démarche, l'Organisation protège son indépendance, préserve la confiance de ses partenaires et garantit que l'ensemble des ressources qui lui sont confiées contribue exclusivement à des objectifs d'intérêt général, de solidarité et de développement durable.

Bénéficiaire effectif

Le **bénéficiaire effectif** désigne la ou les personnes physiques qui, en dernier ressort, possèdent, contrôlent ou exercent une influence significative sur une personne morale, une organisation, une association, une fondation, une entreprise, un partenariat, une fiducie ou tout autre dispositif juridique, ou qui tirent le bénéfice réel d'une opération, d'un contrat, d'un financement ou d'une transaction. Cette notion vise à identifier les personnes qui exercent un contrôle réel au-delà des représentants apparents ou des structures juridiques utilisées, afin de garantir une parfaite transparence sur l'identité des véritables décideurs ou bénéficiaires.

Dans le cadre de ses activités, **AGCE International – AGCE Canada** considère l'identification du bénéficiaire effectif comme une mesure essentielle de son dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Cette démarche permet de prévenir l'utilisation de sociétés écrans, d'intermédiaires, de structures complexes ou de mécanismes destinés à dissimuler l'identité des personnes bénéficiant réellement des ressources ou exerçant un contrôle sur une relation institutionnelle.

L'Organisation peut ainsi demander aux personnes morales, partenaires, fournisseurs, bailleurs de fonds, prestataires, bénéficiaires de financements, donateurs institutionnels et autres parties prenantes de communiquer les informations nécessaires permettant d'identifier leurs bénéficiaires effectifs. Ces informations peuvent notamment porter sur la structure de propriété, les personnes exerçant un contrôle direct ou indirect, les représentants légaux, les dirigeants ou toute autre personne disposant d'un pouvoir décisionnel significatif. Lorsque les circonstances le justifient, AGCE International peut également solliciter des pièces justificatives complémentaires afin de confirmer l'exactitude des informations fournies.

Les données recueillies sont analysées dans le cadre d'une approche fondée sur les risques, conservées de manière sécurisée et traitées conformément aux exigences légales, réglementaires et aux politiques internes de protection des données. Lorsque l'identité du bénéficiaire effectif ne peut être raisonnablement établie, lorsqu'une coopération insuffisante est constatée ou lorsqu'un risque élevé de criminalité financière est identifié, AGCE International se réserve le droit de refuser, suspendre ou mettre fin à la relation concernée. Cette vigilance contribue à préserver l'intégrité institutionnelle, la transparence des partenariats et la confiance accordée à l'Organisation par ses membres, ses partenaires et les autorités compétentes.

Transaction suspecte

Une **transaction suspecte** désigne toute opération financière, bancaire, patrimoniale, numérique ou matérielle qui, en raison de son montant, de sa fréquence, de sa complexité, de son caractère inhabituel, de son absence de justification économique apparente ou de son incohérence avec le profil ou les activités de la personne concernée, est susceptible de révéler une tentative de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de fonds ou de toute autre activité illicite. Une transaction peut être considérée comme suspecte indépendamment de son montant ou de son mode de paiement, dès lors que des éléments objectifs ou circonstanciels justifient un examen renforcé.

Dans le cadre de son dispositif de conformité, **AGCE International – AGCE Canada** met en œuvre des procédures destinées à identifier, analyser, documenter et traiter toute opération présentant un niveau de risque inhabituel. Les situations pouvant justifier une vigilance renforcée comprennent notamment des paiements provenant de juridictions à risque, des dons ou financements dont l'origine ne peut être raisonnablement démontrée, des transferts internationaux inhabituels, des paiements fractionnés sans justification, des changements inexplicables dans les modalités de paiement, des refus de fournir les informations

requis dans le cadre du processus KYC, ou toute autre opération incompatible avec le profil, les activités ou les objectifs déclarés d'un membre, d'un partenaire, d'un donateur ou d'un bénéficiaire.

Lorsqu'une transaction est identifiée comme potentiellement suspecte, elle fait l'objet d'une analyse confidentielle par les responsables compétents désignés par l'Organisation. Selon la nature et le niveau de risque, des vérifications complémentaires peuvent être réalisées, des documents justificatifs peuvent être demandés, la transaction peut être temporairement suspendue ou refusée, et toute autre mesure appropriée peut être prise conformément aux procédures internes et au cadre juridique applicable. Lorsque la réglementation l'impose, AGCE International coopère avec les autorités légalement compétentes dans le respect des obligations de confidentialité, de protection des données et des droits des personnes concernées.

L'ensemble des administrateurs, dirigeants, collaborateurs, bénévoles, représentants d'antennes, partenaires et prestataires sont tenus d'exercer une vigilance permanente et de signaler sans délai toute opération ou comportement susceptible de présenter un risque de criminalité financière. Cette obligation de vigilance constitue un élément essentiel du système de gouvernance, de conformité et de gestion des risques d'AGCE International, contribuant à préserver son intégrité, sa réputation et la confiance de l'ensemble de ses parties prenantes.

Risque

Au sens de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, le **risque** désigne la probabilité qu'un événement, une situation, une relation ou une opération puisse exposer **AGCE International – AGCE Canada** à des conséquences juridiques, financières, opérationnelles, réputationnelles, réglementaires ou institutionnelles liées au blanchiment de capitaux, au financement du terrorisme, à la fraude, à la corruption ou à toute autre forme de criminalité financière. L'identification et l'évaluation des risques constituent un élément fondamental du dispositif de gouvernance, de conformité et de contrôle interne de l'Organisation.

AGCE International applique une **approche fondée sur les risques**, consistant à identifier, analyser, classer, surveiller et réévaluer en permanence les risques associés à ses membres, donateurs, bénéficiaires, partenaires, fournisseurs, projets, programmes, zones géographiques, sources de financement et transactions financières. Cette démarche permet d'adapter les mesures de vigilance, les procédures de contrôle, le niveau de diligence raisonnable et les mécanismes de surveillance en fonction du niveau de risque identifié, afin d'assurer une gestion proportionnée, efficace et conforme aux exigences légales et réglementaires.

L'Organisation met en œuvre des dispositifs de prévention, de contrôle interne, d'audit, de traçabilité, de signalement et d'amélioration continue afin de réduire la probabilité de survenance des risques et d'en limiter les conséquences. Chaque administrateur, dirigeant,

collaborateur, bénévole, représentant d'antenne, partenaire ou prestataire est responsable, dans le cadre de ses fonctions, de contribuer à l'identification des risques, de respecter les procédures de maîtrise définies par l'Organisation et de signaler sans délai toute situation susceptible de compromettre l'intégrité, la conformité ou la réputation d'AGCE International – AGCE Canada.

CHAPITRE 2

CADRE JURIDIQUE

Le présent chapitre définit le cadre juridique de référence applicable à la **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de l'**ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il précise les fondements légaux, réglementaires et institutionnels qui encadrent la prévention, la détection et la gestion des risques de blanchiment de capitaux, de financement du terrorisme, de fraude et de toute autre forme de criminalité financière dans l'ensemble des activités de l'Organisation.

En tant qu'organisation non gouvernementale agréée au Cameroun et disposant d'une représentation officielle au Canada ainsi que dans plusieurs autres pays, AGCE International exerce ses missions dans le respect des législations nationales applicables à chacune de ses implantations, des règlements administratifs et financiers en vigueur, des obligations imposées par les établissements bancaires et prestataires de services de paiement, ainsi que des exigences contractuelles de ses partenaires techniques et financiers. L'Organisation veille à adapter ses procédures internes aux évolutions législatives et réglementaires afin de garantir une conformité permanente dans toutes les juridictions où elle intervient.

La présente politique s'appuie également sur les principes et standards internationaux reconnus en matière de gouvernance, de transparence financière, de gestion des risques, de diligence raisonnable, de connaissance des parties prenantes (KYC), de lutte contre la corruption, de protection des données, de contrôle interne et de redevabilité. Elle est élaborée en cohérence avec les statuts, le règlement intérieur, le code d'éthique, les politiques de gouvernance, les procédures financières et l'ensemble des instruments normatifs composant le système intégré de conformité d'AGCE International.

L'Organisation reconnaît que la conformité juridique constitue une responsabilité permanente et partagée par l'ensemble de ses organes de gouvernance, dirigeants, administrateurs, collaborateurs, bénévoles, représentants d'antennes, partenaires, prestataires et toute personne agissant en son nom. Chacun est tenu de respecter les dispositions légales applicables, les politiques internes et les procédures opérationnelles mises en place afin de préserver l'intégrité, la crédibilité et la réputation de l'Organisation.

Le présent cadre juridique a ainsi pour finalité de garantir que toutes les activités, opérations financières, partenariats, projets et programmes conduits par AGCE International – AGCE Canada soient réalisés dans le respect de la légalité, de la transparence, de l'éthique et des meilleures pratiques internationales en matière de prévention du blanchiment de capitaux et du financement du terrorisme. Il constitue le fondement de l'ensemble des obligations et responsabilités développées dans les chapitres suivants de la présente politique.

2.1 Cadre international

La présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** s'inscrit dans le respect des principes et standards internationaux reconnus en matière de prévention de la criminalité financière, de transparence, de gouvernance, de diligence raisonnable et de coopération internationale. En tant qu'organisation non gouvernementale à vocation internationale, **AGCE International – AGCE Canada** veille à ce que ses politiques, procédures et mécanismes de contrôle soient alignés sur les meilleures pratiques internationales afin de garantir une gestion responsable de ses ressources, de préserver son intégrité institutionnelle et de renforcer la confiance de ses membres, partenaires, bailleurs de fonds, institutions financières et autorités compétentes.

L'organisation s'engage à suivre les évolutions des normes internationales relatives à la lutte contre le blanchiment de capitaux, le financement du terrorisme, la prolifération des armes de destruction massive, la fraude, la corruption, le financement illicite et les autres formes de criminalité financière susceptibles d'affecter les organisations à but non lucratif. Elle adapte régulièrement son dispositif de conformité afin de tenir compte des recommandations internationales, des analyses de risques émergents et des bonnes pratiques publiées par les organismes internationaux compétents.

Recommandations du Groupe d'Action Financière (GAFI/FATF)

AGCE International – AGCE Canada reconnaît les **Recommandations du Groupe d'Action Financière (GAFI/FATF – Financial Action Task Force)** comme la principale référence internationale en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et le financement de la prolifération des armes de destruction massive. Ces recommandations constituent un cadre mondial de bonnes pratiques destiné à aider les États, les institutions financières, les organisations à but non lucratif et les autres acteurs concernés à mettre en place des systèmes efficaces de prévention, de détection, de contrôle et de coopération face aux risques de criminalité financière.

Dans cette perspective, l'Organisation met en œuvre une **approche fondée sur les risques**, renforce ses procédures de connaissance des membres et partenaires (**KYC**), identifie les bénéficiaires effectifs, applique des mesures de vigilance adaptées aux personnes et opérations présentant un niveau de risque élevé, assure la traçabilité de ses opérations financières, conserve les documents justificatifs conformément aux exigences légales et développe un dispositif permanent de contrôle interne, de formation, d'audit et d'amélioration continue. AGCE International veille également à exercer une vigilance particulière dans le cadre de ses partenariats internationaux, de ses opérations transfrontalières, de la réception des dons, des financements et des subventions, afin de réduire les risques de blanchiment de capitaux ou de financement du terrorisme.

Sans se substituer aux autorités nationales compétentes, l'Organisation s'engage à coopérer, dans le respect des lois applicables, avec les institutions de contrôle, les établissements financiers et les partenaires autorisés lorsque cette coopération est requise. Par cet engagement, AGCE International affirme sa volonté d'inscrire durablement sa gouvernance dans le respect des standards internationaux promus par le GAFI, tout en renforçant la transparence, la conformité, la redevabilité et la crédibilité de ses actions humanitaires et de développement.

Convention des Nations Unies

Dans le cadre de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, AGCE International – AGCE Canada adhère aux principes consacrés par les principales **Conventions et Résolutions des Nations Unies** relatives à la prévention de la criminalité financière, à la lutte contre le terrorisme, à la corruption, à la criminalité transnationale organisée et au renforcement de la coopération internationale. Ces instruments internationaux constituent des références essentielles pour promouvoir la transparence, l'intégrité, la responsabilité, la coopération entre les États et la protection du système financier international contre toute utilisation à des fins illicites.

L'Organisation reconnaît notamment les principes énoncés dans la **Convention des Nations Unies contre la criminalité transnationale organisée (Convention de Palerme)**, la **Convention des Nations Unies contre la corruption (Convention de Mérida)** ainsi que les conventions et résolutions pertinentes des Nations Unies relatives à la prévention et à la répression du financement du terrorisme. Ces instruments encouragent les organisations à mettre en place des mécanismes efficaces de contrôle interne, de vigilance, de coopération, de traçabilité financière, de transparence institutionnelle et de gestion des risques.

En cohérence avec ces principes, AGCE International développe un dispositif permanent de prévention reposant sur l'éthique, la conformité, la diligence raisonnable, la connaissance des parties prenantes, la protection des ressources institutionnelles, la détection des opérations atypiques et la coopération avec les autorités compétentes lorsque les dispositions légales applicables l'exigent. Par cette démarche, l'Organisation contribue à la promotion d'une gouvernance responsable et à la réalisation des objectifs internationaux de paix, de sécurité, de développement durable et de bonne gouvernance.

Normes internationales applicables

Outre les instruments des Nations Unies et les recommandations du **Groupe d'Action Financière (GAFI/FATF)**, AGCE International – AGCE Canada veille à aligner son système de gouvernance et de conformité sur les meilleures pratiques et normes internationales applicables aux organisations à but non lucratif, aux organismes de bienfaisance et aux acteurs de la coopération internationale. Cette démarche vise à renforcer la crédibilité institutionnelle de l'Organisation, à sécuriser ses opérations financières et à répondre aux

attentes des partenaires, des bailleurs de fonds, des établissements financiers et des autorités de contrôle.

À cette fin, l'Organisation applique des principes de gouvernance fondés sur la transparence, la responsabilité financière, la gestion des risques, le contrôle interne, la séparation des fonctions, la traçabilité des opérations, la conservation des documents, la protection des données personnelles, la diligence raisonnable, la connaissance des membres et partenaires (KYC), l'identification des bénéficiaires effectifs, la prévention des conflits d'intérêts ainsi que l'amélioration continue des procédures de conformité. Elle tient également compte, selon leur applicabilité, des exigences contractuelles des organismes de coopération internationale, des institutions financières, des agences de développement, des fondations et des autres partenaires techniques et financiers.

AGCE International assure une veille juridique et réglementaire permanente afin d'adapter ses politiques internes aux évolutions des normes internationales et des exigences sectorielles. Cette approche permet de maintenir un niveau élevé de conformité, de renforcer la confiance des parties prenantes et de garantir que l'ensemble des activités, projets et opérations de l'Organisation soient conduits dans le respect des principes universels de légalité, d'intégrité, de transparence, de redevabilité et de coopération internationale.

2.2 Cadre Cameroun

La présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** est mise en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International)** dans le strict respect du cadre juridique en vigueur en **République du Cameroun**. En tant qu'organisation non gouvernementale agréée et légalement constituée, AGCE International exerce l'ensemble de ses activités conformément aux lois, règlements, actes administratifs et exigences des autorités compétentes relatives à la gouvernance des organisations à but non lucratif, à la transparence financière, à la conformité, à la lutte contre la criminalité financière et à la protection de l'ordre public.

L'organisation reconnaît que le respect du droit camerounais constitue une obligation permanente pour l'ensemble de ses organes de gouvernance, de ses dirigeants, administrateurs, collaborateurs, représentants d'antennes, bénévoles, partenaires et prestataires intervenant sur le territoire national. À cet effet, AGCE International veille à adapter continuellement ses procédures internes afin de garantir leur conformité avec les évolutions de la législation et des exigences réglementaires applicables.

Conformément à son statut d'organisation non gouvernementale, AGCE International exerce notamment ses activités dans le respect de la **Loi n°90/053 du 19 décembre 1990 relative à la liberté d'association**, de la **Loi n°99/014 du 22 décembre 1999 régissant les Organisations Non Gouvernementales (ONG)**, ainsi que de leurs textes d'application. L'Organisation bénéficie d'un **agrément officiel délivré par le Ministère de l'Administration**

Territoriale (MINAT) suivant l'Arrêté n°000277/A/MINAT/SG/DAP/SDLP/SONG/BA du 03 juillet 2025, qui lui confère la qualité d'organisation non gouvernementale légalement reconnue au Cameroun.

Dans le cadre de ses obligations de conformité, AGCE International respecte également les dispositions légales et réglementaires camerounaises applicables en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme, la fraude, la corruption, la gouvernance financière, les obligations comptables, fiscales, sociales, bancaires et administratives. L'Organisation coopère, dans les limites prévues par la loi, avec les autorités publiques compétentes, les établissements financiers, les organismes de contrôle, les juridictions compétentes ainsi que les partenaires institutionnels lorsqu'une telle coopération est requise par les textes en vigueur.

Afin de garantir une conformité permanente, AGCE International met en œuvre un système intégré de gouvernance comprenant des procédures de contrôle interne, de gestion des risques, de connaissance des membres et partenaires (KYC), d'identification des bénéficiaires effectifs, de traçabilité des opérations financières, d'archivage documentaire, de protection des données, d'audit et d'amélioration continue. Ce dispositif contribue à assurer une gestion responsable, transparente et conforme des ressources de l'Organisation, tout en renforçant la confiance des autorités, des partenaires, des donateurs, des bénéficiaires et de l'ensemble des parties prenantes dans les activités conduites au Cameroun.

2.3 Cadre Canada

Dans le cadre de ses activités internationales, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International)** exerce ses opérations au Canada par l'intermédiaire de son antenne officielle **AGCE Canada**, légalement constituée dans la province de Québec sous le **Numéro d'Entreprise du Québec (NEQ) 1181903098**. À ce titre, AGCE Canada est tenue de respecter l'ensemble des lois fédérales, provinciales et des exigences réglementaires applicables aux organismes sans but lucratif, aux organismes de bienfaisance, ainsi qu'aux organisations exerçant des activités financières, humanitaires, communautaires et de coopération internationale sur le territoire canadien.

L'Organisation s'engage à exercer toutes ses activités dans le respect des exigences canadiennes relatives à la gouvernance, à la transparence, à la reddition de comptes, à la protection des renseignements personnels, à la conformité financière, à la lutte contre le blanchiment de capitaux, au financement du terrorisme, à la fraude et à toute autre forme de criminalité financière. Cette conformité constitue un principe permanent de gouvernance visant à protéger l'intégrité de l'Organisation, à préserver la confiance de ses partenaires et à garantir une utilisation responsable des ressources qui lui sont confiées.

AGCE Canada veille notamment au respect des obligations prévues par la **Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes (LRPCFAT)**, ainsi que de ses règlements d'application, qui encadrent les mesures de

prévention, de vigilance raisonnable, de conservation des documents et de déclaration des opérations lorsque ces obligations sont applicables aux activités exercées. L'Organisation tient également compte des lignes directrices publiées par le **Centre d'analyse des opérations et déclarations financières du Canada (CANAFE – FINTRAC)** afin de renforcer son dispositif interne de gestion des risques et de conformité.

Par ailleurs, AGCE Canada respecte les exigences applicables de l'**Agence du revenu du Canada (ARC)** concernant les organismes sans but lucratif et, le cas échéant, les organismes de bienfaisance enregistrés, notamment en matière de tenue de livres, de conservation des pièces justificatives, de production des déclarations réglementaires, de gestion des dons, de gouvernance financière et de reddition de comptes. L'Organisation applique également les dispositions législatives et réglementaires de la **province de Québec** relatives à son statut juridique, à son administration, à sa gestion comptable et au respect de ses obligations institutionnelles.

Afin d'assurer une conformité permanente, AGCE Canada met en œuvre un dispositif intégré reposant sur l'identification des risques, les procédures de connaissance des membres et partenaires (KYC), l'identification des bénéficiaires effectifs, la vérification de l'origine des fonds lorsque cela est requis, la surveillance des opérations, le contrôle interne, l'audit, la conservation sécurisée des documents, la protection des renseignements personnels, la formation continue des responsables et l'amélioration permanente de ses procédures. Ce dispositif permet d'assurer que toutes les activités conduites au Canada respectent les exigences légales applicables ainsi que les meilleures pratiques internationales en matière de gouvernance, de conformité et de lutte contre le blanchiment de capitaux et le financement du terrorisme, tout en soutenant la mission humanitaire et de développement durable d'AGCE International.

2.4 Autres juridictions

Principe de conformité territoriale

En raison de sa vocation internationale, de ses représentations établies dans plus de quinze pays et de ses activités transfrontalières, **AGCE International – AGCE Canada** applique la présente Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme dans toutes les juridictions où elle dispose d'une antenne, d'un représentant, d'un partenaire, d'un programme, d'un compte financier ou d'une opération. Chaque structure nationale demeure tenue de respecter la législation de son pays d'établissement, les décisions des autorités compétentes ainsi que les obligations applicables aux organisations à but non lucratif, sans pouvoir invoquer les règles du siège pour écarter une exigence locale impérative.

Articulation des normes applicables

Lorsqu'une activité implique plusieurs pays, AGCE International identifie les règles applicables au lieu d'enregistrement de l'entité, au territoire d'exécution du projet, au pays d'origine ou de destination des fonds ainsi qu'aux établissements financiers et prestataires de paiement concernés. En cas de coexistence de plusieurs exigences, l'Organisation retient, sous réserve du droit impératif local, la mesure de vigilance la plus protectrice en matière d'identification, de traçabilité, de contrôle, de conservation documentaire et de prévention des risques.

Obligation des antennes et représentants

Toute antenne, délégation, représentation ou structure partenaire agissant au nom d'AGCE International doit intégrer les exigences LBC/FT dans ses procédures administratives et financières. Elle doit vérifier l'identité de ses responsables, partenaires, donateurs et bénéficiaires effectifs, documenter l'origine et la destination des fonds, utiliser des circuits financiers autorisés, assurer la conservation des justificatifs et transmettre au siège les informations nécessaires au contrôle institutionnel. Aucun représentant ne peut engager l'Organisation dans une opération interdite, insuffisamment documentée ou contraire aux sanctions applicables.

Opérations transfrontalières et zones à risque

Les transferts internationaux, collectes de dons, financements participatifs, achats transfrontaliers, distributions humanitaires et partenariats réalisés dans des zones sensibles font l'objet d'une vigilance renforcée. Le niveau de contrôle est déterminé selon le pays concerné, la nature du projet, le canal de paiement, le profil des parties prenantes, la présence éventuelle d'intermédiaires et la qualité des pièces justificatives. Cette démarche repose sur des mesures ciblées et proportionnées, conformément à l'approche fondée sur les risques recommandée pour les organisations à but non lucratif, sans entraver indûment les activités humanitaires légitimes.

Sanctions internationales et restrictions financières

AGCE International veille à ce qu'aucun fonds, bien, avantage économique ou service ne soit directement ou indirectement mis à la disposition d'une personne ou entité faisant l'objet d'une mesure de gel, d'une interdiction ou d'une sanction juridiquement applicable. Les opérations présentant une correspondance potentielle avec une liste de sanctions doivent être suspendues, examinées et, lorsque la législation l'impose, signalées aux autorités compétentes. Les Nations Unies rappellent notamment l'importance des mécanismes de gel des avoirs et de la prévention de toute mise à disposition de ressources au profit de personnes ou groupes associés au terrorisme.

Adaptation locale et suivi juridique

Chaque représentation doit assurer une veille sur les lois, règlements, obligations déclaratives et directives nationales applicables. Toute modification importante doit être communiquée aux organes de gouvernance d'AGCE International afin de permettre l'actualisation des procédures, des formulaires KYC, des seuils de contrôle et des mécanismes de signalement. Lorsque le cadre local demeure incertain, complexe ou contradictoire, l'Organisation sollicite l'avis d'un professionnel qualifié avant l'exécution de l'opération concernée.

Respect des droits fondamentaux

L'application des mesures LBC/FT dans les autres juridictions doit demeurer conforme aux principes de légalité, de proportionnalité, de non-discrimination, de confidentialité et de protection des données. Les contrôles ne doivent pas conduire à une exclusion arbitraire des bénéficiaires ni à une interruption injustifiée des activités humanitaires. Ils doivent concilier la prévention du financement illicite avec le respect des droits humains, du droit humanitaire et des obligations internationales applicables.

CHAPITRE 3

PRINCIPES FONDAMENTAUX

Le présent chapitre établit les principes directeurs qui fondent le dispositif de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Ces principes constituent le socle de gouvernance sur lequel repose l'ensemble des politiques, procédures, contrôles et mécanismes de conformité de l'Organisation. Ils orientent les décisions stratégiques et opérationnelles afin de garantir que toutes les activités, tous les projets, toutes les ressources financières et tous les partenariats soient gérés dans le respect des exigences légales, des standards internationaux, des valeurs éthiques de l'Organisation et des attentes légitimes des autorités publiques, des partenaires institutionnels, des donateurs, des bénéficiaires et des autres parties prenantes.

Les principes fondamentaux énoncés dans le présent chapitre s'appliquent à l'ensemble des organes de gouvernance, des dirigeants, des administrateurs, des représentants nationaux et internationaux, des responsables d'antennes, des employés, des bénévoles, des consultants, des prestataires, des partenaires techniques et financiers ainsi qu'à toute personne physique ou morale agissant pour le compte ou au nom d'AGCE International. Ils demeurent applicables indépendamment du pays d'intervention, de la nature des activités ou des sources de financement mobilisées.

La présente politique repose sur une approche préventive privilégiant l'identification anticipée des risques, la transparence des opérations, la responsabilisation des acteurs, la coopération avec les autorités compétentes, la traçabilité des flux financiers et l'amélioration continue du système de conformité. L'Organisation considère que la prévention demeure le moyen le plus efficace de protéger ses ressources, de préserver sa réputation institutionnelle et de garantir que ses actions humanitaires, sociales, éducatives, sanitaires, économiques et numériques ne puissent être utilisées, directement ou indirectement, à des fins de blanchiment de capitaux, de financement du terrorisme ou de toute autre activité illicite.

L'application de ces principes s'inscrit également dans une démarche permanente de gouvernance responsable, de gestion des risques et de conformité réglementaire. AGCE International veille à maintenir un équilibre entre l'efficacité de ses interventions humanitaires et le respect des obligations légales, en mettant en œuvre des procédures proportionnées à la nature et au niveau de risque des opérations réalisées. Cette approche permet de protéger les bénéficiaires légitimes des programmes de l'Organisation tout en assurant un niveau élevé de sécurité financière, administrative et institutionnelle.

Enfin, les principes fondamentaux de la présente politique s'intègrent dans le **Cadre Intégré de Gouvernance, d'Éthique, de Conformité et de Redevabilité (CIGECR)** développé par AGCE International. Ils sont mis en œuvre en complément du Code d'éthique et de déontologie, du Manuel de contrôle interne, de la Politique de gouvernance et de

transparence, de la Politique de protection des données, de la Politique de protection des lanceurs d'alerte, des procédures financières et comptables ainsi que de l'ensemble des instruments institutionnels de gestion adoptés par l'Organisation. Leur objectif est de renforcer durablement la confiance des partenaires nationaux et internationaux, des institutions publiques, des bailleurs de fonds, des organismes de coopération, des établissements financiers et des communautés bénéficiaires, tout en consolidant la crédibilité, la transparence, la responsabilité et la pérennité des missions d'intérêt général conduites par AGCE International – AGCE Canada.

3.1 Intégrité

L'intégrité constitue l'un des principes fondateurs de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT) de ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle représente l'engagement permanent de l'Organisation à exercer l'ensemble de ses missions humanitaires, sociales, éducatives, sanitaires, économiques et numériques avec honnêteté, probité, impartialité et responsabilité. Ce principe guide toutes les décisions institutionnelles, financières et opérationnelles afin de garantir que les ressources confiées à l'Organisation soient exclusivement utilisées au service de sa mission d'intérêt général et jamais à des fins illicites ou contraires aux valeurs de l'Organisation.

L'intégrité s'impose à tous les organes de gouvernance, aux membres du Collège Central, au Bureau Exécutif, aux responsables des antennes nationales et internationales, aux administrateurs, aux collaborateurs, aux bénévoles, aux consultants, aux partenaires, aux fournisseurs ainsi qu'à toute personne agissant au nom ou pour le compte d'AGCE International. Chacun est tenu d'adopter un comportement exemplaire, conforme aux lois applicables, au Code d'éthique et de déontologie de l'Organisation, aux politiques internes ainsi qu'aux principes de bonne gouvernance reconnus à l'échelle nationale et internationale.

Afin de préserver cette intégrité institutionnelle, AGCE International applique une politique de tolérance zéro à l'égard du blanchiment de capitaux, du financement du terrorisme, de la corruption, de la fraude, du détournement de ressources, du trafic d'influence, des conflits d'intérêts non déclarés, de la falsification documentaire, de l'utilisation abusive des actifs de l'Organisation ainsi que de toute autre pratique susceptible de compromettre sa réputation, sa crédibilité ou la confiance de ses partenaires. Toute situation présentant un risque d'atteinte à l'intégrité fait l'objet d'une analyse rigoureuse, de mesures correctives appropriées et, lorsque la législation l'exige, d'une coopération avec les autorités compétentes.

L'Organisation favorise également une culture institutionnelle fondée sur l'éthique, la responsabilité individuelle, la vigilance, la redevabilité et le devoir d'alerte. Les collaborateurs sont encouragés à signaler, en toute bonne foi et dans le respect des procédures internes, tout comportement suspect ou toute irrégularité susceptible de constituer une violation de la présente politique. Aucune mesure de représailles ne peut être exercée contre une personne

ayant effectué un signalement de bonne foi conformément aux mécanismes de protection des lanceurs d'alerte adoptés par AGCE International.

L'intégrité constitue ainsi une exigence permanente qui renforce la crédibilité institutionnelle de l'Organisation, sécurise ses relations avec les partenaires nationaux et internationaux et garantit que toutes les décisions soient prises dans l'intérêt exclusif de la mission humanitaire, du développement durable, de l'inclusion économique et numérique ainsi que du respect de l'intérêt général.

3.2 Transparence

La transparence constitue un principe essentiel de gouvernance et un pilier fondamental du dispositif de conformité d'**AGCE International – AGCE Canada**. Elle repose sur l'engagement de l'Organisation à assurer une gestion claire, sincère, vérifiable et responsable de l'ensemble de ses activités, de ses ressources financières, de ses partenariats, de ses projets et de ses mécanismes décisionnels. La transparence contribue à prévenir les risques de blanchiment de capitaux, de financement du terrorisme et de fraude en garantissant la traçabilité complète des opérations réalisées par l'Organisation.

Dans cette perspective, AGCE International met en œuvre des procédures documentées permettant d'assurer l'identification des parties prenantes, la justification de l'origine et de l'utilisation des ressources financières, la conservation des pièces comptables et administratives, le suivi des opérations bancaires, la validation des dépenses, la séparation des responsabilités, ainsi que le contrôle permanent des flux financiers. Chaque opération importante doit pouvoir être retracée, vérifiée et justifiée au moyen de documents fiables, complets et régulièrement archivés conformément aux exigences légales et aux politiques internes.

La transparence s'applique également aux relations entretenues avec les donateurs, les bailleurs de fonds, les partenaires institutionnels, les établissements financiers, les autorités publiques et les bénéficiaires. AGCE International veille à fournir des informations exactes, loyales, complètes et actualisées sur sa gouvernance, ses programmes, ses mécanismes de contrôle, l'utilisation des financements reçus ainsi que les résultats obtenus dans le cadre de ses missions. Cette démarche favorise une relation durable fondée sur la confiance, la responsabilité et la redevabilité.

L'Organisation développe par ailleurs un système permanent de contrôle interne, d'audit, de suivi des risques et d'amélioration continue permettant de vérifier la conformité des opérations avec les exigences légales, réglementaires et institutionnelles. Les organes de gouvernance disposent d'informations fiables pour exercer leurs responsabilités de supervision, prendre des décisions éclairées et assurer une gestion prudente des ressources confiées à l'Organisation.

Enfin, la transparence constitue un facteur essentiel de crédibilité auprès des partenaires nationaux et internationaux. Elle démontre l'engagement d'AGCE International à promouvoir une gouvernance exemplaire, une gestion responsable des fonds, une conformité rigoureuse aux normes de lutte contre le blanchiment de capitaux et le financement du terrorisme, ainsi qu'une culture institutionnelle fondée sur l'intégrité, la confiance, la responsabilité et la reddition de comptes.

3.3 Redevabilité

La redevabilité constitue un principe fondamental de gouvernance qui engage **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** à assumer pleinement la responsabilité de l'ensemble de ses décisions, de ses actions, de sa gestion administrative, financière et opérationnelle ainsi que des résultats obtenus dans le cadre de ses missions humanitaires, sociales, éducatives, sanitaires, économiques et numériques. Elle traduit la volonté permanente de l'Organisation d'agir avec responsabilité, transparence et professionnalisme envers les autorités publiques, les partenaires techniques et financiers, les donateurs, les bénéficiaires, les institutions financières et l'ensemble des parties prenantes.

Le principe de redevabilité implique que chaque décision, chaque engagement financier, chaque partenariat, chaque programme et chaque opération réalisée au nom de l'Organisation puisse être expliqué, justifié, documenté et évalué. Les organes de gouvernance, les dirigeants, les responsables d'antennes, les administrateurs, les collaborateurs, les bénévoles, les consultants et toute personne agissant pour le compte d'AGCE International sont responsables des actes qu'ils accomplissent dans le cadre de leurs fonctions et demeurent tenus d'en rendre compte conformément aux procédures internes et aux exigences légales applicables.

Dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme, la redevabilité impose que toutes les opérations financières, les mouvements de fonds, les collectes de dons, les cotisations, les subventions, les dépenses, les acquisitions, les paiements, les transferts internationaux et les conventions de partenariat soient exécutés conformément aux procédures institutionnelles, fassent l'objet d'autorisations appropriées, soient dûment documentés et puissent être vérifiés à tout moment par les organes de contrôle compétents.

AGCE International met en œuvre un système permanent de gouvernance permettant d'assurer une répartition claire des responsabilités, la séparation des fonctions sensibles, la validation hiérarchique des opérations importantes, le contrôle interne, les audits périodiques, l'évaluation des risques, la gestion documentaire et la production de rapports administratifs, financiers et opérationnels. Ces mécanismes garantissent que chaque responsable puisse démontrer la régularité des décisions prises et l'utilisation conforme des ressources placées sous sa responsabilité.

La redevabilité s'étend également aux relations entretenues avec les bailleurs de fonds, les partenaires internationaux, les organismes de coopération, les établissements financiers, les administrations publiques et les communautés bénéficiaires. AGCE International s'engage à fournir des informations exactes, sincères, complètes et accessibles sur la mise en œuvre de ses projets, l'utilisation des financements reçus, les résultats obtenus ainsi que les mesures correctives mises en œuvre lorsque des insuffisances sont constatées. Cette démarche renforce la confiance des parties prenantes et contribue à la crédibilité durable de l'Organisation.

Enfin, la redevabilité constitue un levier essentiel d'amélioration continue. Les observations formulées lors des audits, des évaluations, des contrôles internes, des inspections ou des revues de conformité sont analysées avec rigueur afin d'identifier les axes d'amélioration, de renforcer les dispositifs de prévention des risques et d'assurer une évolution permanente du système de gouvernance, de conformité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

3.4 Traçabilité

La traçabilité constitue un principe essentiel du dispositif de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** mis en œuvre par **AGCE International – AGCE Canada**. Elle consiste à garantir que chaque opération administrative, financière, comptable ou contractuelle réalisée par l'Organisation puisse être identifiée, reconstituée, vérifiée et contrôlée tout au long de son cycle de vie. Ce principe permet d'assurer la transparence des activités, de sécuriser les flux financiers et de prévenir toute tentative de dissimulation, de fraude, de détournement ou de blanchiment de capitaux.

L'Organisation veille à ce que chaque transaction, quelle que soit sa nature ou son montant, soit appuyée par des pièces justificatives authentiques, complètes et régulièrement conservées. Les recettes, dons, cotisations, subventions, achats, paiements, remboursements, transferts bancaires, mouvements de trésorerie, contrats, conventions et autres engagements financiers doivent être enregistrés dans les systèmes de gestion de manière chronologique, fiable et sécurisée afin de permettre leur consultation, leur contrôle et leur audit.

La traçabilité repose également sur une identification rigoureuse des parties prenantes. AGCE International met en œuvre des procédures de connaissance des membres, donateurs, partenaires, fournisseurs, bénéficiaires et autres intervenants, notamment au moyen des dispositifs **KYC (Know Your Customer)** et, lorsque cela est nécessaire, de l'identification du bénéficiaire effectif, de la vérification de l'origine des fonds et de l'analyse des risques associés aux opérations. Cette vigilance contribue à prévenir l'utilisation de l'Organisation comme vecteur de financement illicite.

Afin de renforcer la fiabilité des informations, l'Organisation applique des procédures garantissant l'intégrité des données, l'horodatage des opérations, la sécurisation des archives physiques et numériques, la protection des documents contre toute modification non autorisée

ainsi que la conservation des enregistrements pendant les durées prévues par les législations applicables. Les systèmes d'information et les plateformes numériques utilisés par AGCE International doivent offrir un niveau de sécurité permettant d'assurer la confidentialité, l'authenticité, la disponibilité et la traçabilité des données traitées.

La traçabilité constitue également un outil essentiel pour les missions d'audit interne, de contrôle externe, d'inspection, d'évaluation institutionnelle et de coopération avec les autorités compétentes lorsque la loi l'exige. Elle permet de reconstituer l'historique complet d'une opération, d'identifier les personnes intervenues à chaque étape, de vérifier la conformité des décisions prises et de démontrer la bonne utilisation des ressources de l'Organisation.

Par ce principe, AGCE International affirme son engagement à maintenir un système de gestion fiable, transparent et sécurisé, garantissant que chaque ressource mobilisée, chaque décision prise et chaque opération réalisée puissent être justifiées, contrôlées et retracées dans le respect des exigences légales, réglementaires et des meilleures pratiques internationales de gouvernance, de conformité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

3.5 Tolérance zéro

La politique de **tolérance zéro** constitue l'un des fondements essentiels de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle traduit l'engagement ferme, permanent et sans équivoque de l'Organisation à prévenir, détecter et combattre toute forme de blanchiment de capitaux, de financement du terrorisme, de corruption, de fraude, de détournement de fonds, de financement illicite, de falsification documentaire, de trafic d'influence, de conflit d'intérêts dissimulé ou de toute autre activité susceptible de compromettre son intégrité institutionnelle, sa réputation ou la légalité de ses actions.

Cette politique s'impose à l'ensemble des organes de gouvernance, aux membres du Collège Central, au Bureau Exécutif, aux responsables d'antennes nationales et internationales, aux administrateurs, aux employés, aux bénévoles, aux consultants, aux partenaires techniques et financiers, aux fournisseurs, aux prestataires ainsi qu'à toute personne physique ou morale agissant directement ou indirectement au nom ou pour le compte d'AGCE International. Aucun statut hiérarchique, aucune ancienneté, aucune fonction ou qualité ne peut justifier une dérogation aux exigences de conformité définies par la présente politique.

L'Organisation interdit formellement toute opération dont l'origine, la destination, la finalité ou le bénéficiaire ne peuvent être clairement identifiés ou justifiés. Aucun don, aucune cotisation, aucun financement, aucune subvention, aucun partenariat, aucune prestation, aucun transfert financier ou avantage économique ne peut être accepté ou exécuté lorsqu'il existe un doute raisonnable quant à sa licéité, sa conformité ou son adéquation avec les valeurs et les missions de l'Organisation. En présence d'un risque significatif, le principe de

précaution prévaut et l'opération concernée peut être suspendue, refusée ou soumise à des vérifications complémentaires.

Toute violation avérée ou tentative de contournement des règles de conformité expose son auteur à des mesures disciplinaires, administratives, contractuelles ou judiciaires conformément aux lois applicables et aux règlements internes de l'Organisation. AGCE International se réserve également le droit de suspendre ou de mettre fin à toute relation avec un partenaire, un membre, un fournisseur ou toute autre partie prenante dont le comportement est incompatible avec les exigences de la présente politique. Lorsque la législation le prévoit, l'Organisation coopère pleinement avec les autorités compétentes afin de faciliter les enquêtes, les contrôles ou les procédures nécessaires.

La politique de tolérance zéro s'inscrit dans une démarche permanente de prévention, de sensibilisation, de formation, de contrôle interne et d'amélioration continue. Elle vise à instaurer une culture institutionnelle fondée sur l'éthique, la responsabilité, la vigilance et l'exemplarité, garantissant que les ressources confiées à AGCE International soient exclusivement affectées à la réalisation de ses missions humanitaires, sociales, éducatives, sanitaires, économiques et numériques.

3.6 Confidentialité

La **confidentialité** constitue un principe fondamental du dispositif de gouvernance et de conformité d'**AGCE International – AGCE Canada**. Elle garantit que toutes les informations obtenues dans le cadre de l'application de la présente Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme soient traitées avec le plus haut niveau de protection, de discrétion et de sécurité, dans le respect des lois applicables relatives à la protection des données, au secret professionnel, à la vie privée et aux obligations institutionnelles de confidentialité.

L'Organisation veille à protéger l'ensemble des informations relatives à l'identité des membres, donateurs, partenaires, bénéficiaires, fournisseurs, collaborateurs, représentants, bénéficiaires effectifs, institutions financières et autres parties prenantes. Les données personnelles, les documents d'identification, les informations financières, les rapports de contrôle, les analyses de risques, les procédures de vigilance, les signalements, les enquêtes internes ainsi que toute information sensible recueillie dans le cadre des procédures **KYC**, des contrôles de conformité ou des audits sont conservés de manière sécurisée et ne sont accessibles qu'aux personnes dûment autorisées en raison de leurs fonctions.

Chaque personne intervenant pour le compte de l'Organisation est tenue à une obligation stricte de confidentialité pendant toute la durée de sa mission et, lorsque les textes applicables ou les engagements contractuels le prévoient, après la cessation de ses fonctions. Il lui est interdit de divulguer, d'utiliser ou de communiquer à des tiers des informations confidentielles à des fins personnelles, commerciales ou étrangères aux missions de

l'Organisation. Cette obligation s'applique quels que soient le support utilisé, le mode de communication ou le lieu de conservation des informations.

AGCE International met en œuvre des mesures techniques, organisationnelles et administratives destinées à assurer la sécurité des informations, notamment le contrôle des accès, la gestion des habilitations, le chiffrement lorsque cela est approprié, l'archivage sécurisé, la sauvegarde des données, la journalisation des accès, la protection des systèmes d'information et la sensibilisation régulière des utilisateurs aux exigences de sécurité et de confidentialité.

Le principe de confidentialité ne fait toutefois pas obstacle aux obligations légales de communication imposées par les autorités judiciaires, administratives ou de contrôle compétentes. Lorsque la loi exige la transmission d'informations dans le cadre d'une enquête, d'un contrôle ou d'une procédure officielle, AGCE International coopère avec les autorités habilitées dans le respect des procédures applicables, tout en veillant à limiter les informations communiquées à celles strictement nécessaires et à préserver les droits des personnes concernées.

Par ce principe, l'Organisation réaffirme sa volonté de protéger les informations qui lui sont confiées, de renforcer la confiance de ses partenaires et de garantir que l'ensemble des dispositifs de prévention du blanchiment de capitaux et du financement du terrorisme soient mis en œuvre dans le respect de la sécurité, de la confidentialité, de la dignité des personnes et des exigences les plus élevées en matière de gouvernance et de conformité institutionnelle.

3.7 Coopération avec les autorités

La coopération avec les autorités compétentes constitue un principe fondamental de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En tant qu'organisation non gouvernementale exerçant des activités au Cameroun, au Canada et dans plusieurs autres juridictions, AGCE International reconnaît que la prévention et la lutte contre le blanchiment de capitaux, le financement du terrorisme, la corruption, la fraude et les autres formes de criminalité financière reposent sur une collaboration responsable entre les organisations de la société civile, les autorités publiques, les institutions financières, les organismes de contrôle et les partenaires internationaux.

L'Organisation s'engage à respecter pleinement les obligations légales de coopération prévues par les législations applicables dans chacun des pays où elle intervient. Cette coopération s'exerce dans le respect des compétences des autorités administratives, judiciaires, fiscales, financières, douanières, policières et des organismes de renseignement financier, conformément aux procédures prévues par les lois et règlements en vigueur. Elle est mise en œuvre dans le strict respect des droits fondamentaux, du principe de légalité, de la confidentialité des informations et de la protection des données personnelles.

AGCE International veille à répondre avec diligence, exactitude et transparence aux demandes légalement formulées par les autorités compétentes. Lorsque la loi l'autorise ou l'impose, l'Organisation met à disposition les documents administratifs, comptables, financiers, contractuels et techniques nécessaires à l'exercice des missions de contrôle, d'inspection, d'audit, d'enquête ou de vérification. Les informations communiquées doivent être complètes, sincères, exactes, vérifiables et limitées aux éléments strictement nécessaires à l'objet de la demande officielle.

Dans le cadre de cette coopération, l'Organisation facilite les opérations de contrôle portant notamment sur l'identification des membres, des partenaires, des donateurs, des bénéficiaires effectifs, des fournisseurs, des prestataires, des mouvements financiers, des conventions de partenariat, des opérations bancaires, des sources de financement, des pièces justificatives ainsi que de tout autre document permettant d'établir la régularité et la conformité de ses activités. AGCE International veille à maintenir une organisation documentaire rigoureuse garantissant la disponibilité, l'intégrité et la traçabilité des informations susceptibles d'être sollicitées par les autorités habilitées.

L'Organisation s'interdit toute action susceptible d'entraver le travail des autorités compétentes. Sont notamment prohibés la destruction, la falsification, la dissimulation ou l'altération de documents, la communication d'informations volontairement inexacts ou incomplètes, l'obstruction aux opérations de contrôle, ainsi que toute tentative de dissimulation d'opérations susceptibles de présenter un caractère illicite. Toute personne agissant au nom d'AGCE International est tenue de coopérer loyalement avec les organes de contrôle dans le respect des procédures internes et des obligations légales qui lui sont applicables.

Afin de garantir l'efficacité de cette coopération, AGCE International désigne les responsables habilités à assurer les relations avec les autorités publiques et les organismes de contrôle. Ces responsables coordonnent la préparation des réponses officielles, veillent au respect des procédures internes, assurent la conservation des preuves documentaires et s'assurent que les échanges institutionnels soient conduits avec professionnalisme, impartialité, confidentialité et diligence. Lorsque la complexité d'une situation l'exige, l'Organisation peut solliciter l'assistance de ses conseils juridiques, de ses experts-comptables, de ses auditeurs ou de tout autre professionnel qualifié afin de garantir la conformité des réponses apportées.

La coopération avec les autorités s'inscrit également dans une démarche d'amélioration continue du système de gouvernance et de conformité d'AGCE International. Les observations, recommandations, décisions, rapports d'inspection, conclusions d'audit ou demandes de régularisation formulés par les autorités compétentes sont analysés avec attention afin de renforcer les procédures internes, d'améliorer les mécanismes de prévention des risques et de consolider les dispositifs de contrôle, de transparence et de redevabilité. Par cette approche proactive, AGCE International affirme sa volonté de contribuer pleinement aux efforts nationaux et internationaux visant à protéger l'intégrité du système financier, à prévenir les flux financiers illicites et à garantir que ses ressources demeurent exclusivement consacrées à la réalisation de ses missions humanitaires, sociales et de développement durable.

CHAPITRE 4

GOUVERNANCE LBC/FT

La gouvernance de la **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** constitue un pilier essentiel du système de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle établit le cadre organisationnel, décisionnel et opérationnel permettant de prévenir, détecter, gérer et maîtriser les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption et de toute autre forme de criminalité financière susceptible d'affecter les activités de l'Organisation.

La gouvernance LBC/FT repose sur une organisation clairement structurée, une répartition précise des responsabilités, une séparation effective des fonctions, un système permanent de contrôle interne, une culture de conformité partagée et un engagement fort de la Direction Générale ainsi que des organes de gouvernance. Elle vise à garantir que chaque décision, chaque opération financière, chaque partenariat et chaque programme soient réalisés conformément aux exigences légales, réglementaires, éthiques et institutionnelles applicables.

En cohérence avec son **Cadre Intégré de Gouvernance, d'Éthique, de Conformité et de Redevabilité (CIGECR)**, AGCE International intègre les exigences LBC/FT dans l'ensemble de ses politiques, procédures administratives, financières, comptables, numériques et opérationnelles. Cette intégration favorise une approche globale de la gestion des risques et permet d'assurer une conformité homogène dans toutes les représentations nationales et internationales de l'Organisation.

La gouvernance LBC/FT s'applique à l'ensemble des organes institutionnels, notamment au **Collège Central**, au **Président Général**, au **Bureau Exécutif**, aux responsables des antennes nationales et internationales, aux commissions spécialisées, aux responsables financiers, aux responsables administratifs, aux responsables de conformité, aux collaborateurs, aux bénévoles, aux consultants, aux partenaires ainsi qu'à toute personne physique ou morale intervenant pour le compte de l'Organisation. Chaque acteur exerce les responsabilités qui lui sont confiées dans le respect du principe de responsabilité individuelle, de la séparation des fonctions et du devoir permanent de vigilance.

L'Organisation met en œuvre un dispositif de gouvernance fondé sur l'identification et l'évaluation régulière des risques, la mise en place de procédures documentées, la connaissance des parties prenantes (KYC), la vérification des bénéficiaires effectifs lorsque cela est nécessaire, le contrôle des opérations financières, la traçabilité documentaire, les audits périodiques, la formation continue, la gestion des alertes, l'amélioration permanente des procédures et la coopération avec les autorités compétentes lorsque les circonstances l'exigent.

La gouvernance LBC/FT repose également sur le principe de proportionnalité. Les mesures de contrôle sont adaptées à la nature des activités exercées, au volume des

opérations, aux pays d'intervention, aux catégories de partenaires, aux sources de financement, aux risques identifiés ainsi qu'à l'évolution des menaces liées à la criminalité financière. Cette approche permet de maintenir un équilibre entre la protection de l'Organisation, l'efficacité de ses missions humanitaires et le respect des droits des membres, partenaires, donateurs et bénéficiaires.

Enfin, AGCE International inscrit sa gouvernance LBC/FT dans une dynamique d'amélioration continue. Les résultats des audits internes et externes, les évaluations des risques, les recommandations des autorités compétentes, les évolutions des normes internationales, les retours d'expérience ainsi que les innovations technologiques sont régulièrement analysés afin d'actualiser les politiques, de renforcer les mécanismes de contrôle et d'améliorer durablement la capacité de l'Organisation à prévenir toute utilisation abusive de ses ressources. Par cette démarche, AGCE International réaffirme son engagement à promouvoir une gouvernance exemplaire, une conformité rigoureuse et une gestion responsable au service de ses missions humanitaires, sociales, éducatives, sanitaires, économiques et numériques.

4.1 Président Général et Coordinateur Général du CCA

Le **Président Général et Coordinateur Général Du Collège Central de ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**, en sa qualité de plus haute autorité exécutive de l'Organisation et **Président du Collège Central**, assure le leadership stratégique de la gouvernance en matière de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Il veille à ce que l'ensemble des activités institutionnelles soient conduites dans le respect des lois applicables, des normes internationales, des exigences réglementaires ainsi que des politiques internes de gouvernance, de conformité, d'éthique et de transparence adoptées par l'Organisation.

À ce titre, le Président Général définit les grandes orientations stratégiques du dispositif LBC/FT, approuve les politiques institutionnelles, valide les mécanismes de gouvernance, veille à l'allocation des ressources nécessaires à leur mise en œuvre et s'assure que la prévention des risques de blanchiment de capitaux et de financement du terrorisme demeure une priorité permanente dans l'ensemble des programmes, projets, partenariats et opérations nationales et internationales de l'Organisation.

Le Président Général veille à promouvoir une véritable culture institutionnelle de conformité fondée sur l'intégrité, la responsabilité, la transparence, la redevabilité et la gestion des risques. Il s'assure que les principes de vigilance, de contrôle interne, de séparation des fonctions, de traçabilité des opérations financières, de connaissance des parties prenantes (KYC) et de protection des ressources institutionnelles soient intégrés dans toutes les décisions stratégiques et dans le fonctionnement quotidien de l'Organisation.

Dans l'exercice de ses responsabilités, le Président Général supervise l'action du **Bureau Exécutif**, des responsables des antennes nationales et internationales, des directions administratives et financières ainsi que des responsables chargés de la conformité. Il reçoit périodiquement les rapports relatifs à l'évaluation des risques, aux audits, aux contrôles internes, aux incidents de conformité, aux signalements, aux recommandations formulées par les organes de contrôle et aux mesures correctives mises en œuvre. Il veille à ce que ces informations soient examinées avec rigueur afin d'assurer une amélioration continue du dispositif institutionnel de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Le Président Général veille également à ce que l'Organisation dispose de procédures adaptées permettant d'identifier, d'évaluer, de prévenir et de traiter les risques liés aux dons, aux cotisations, aux financements, aux subventions, aux partenariats, aux activités internationales, aux paiements électroniques, aux transferts bancaires et aux autres opérations financières susceptibles de présenter un niveau de risque élevé. Il encourage la mise en œuvre d'une approche fondée sur les risques, adaptée à la nature, au volume et à la complexité des activités exercées par AGCE International.

En matière de gouvernance institutionnelle, le Président Général favorise la coordination entre les différents organes de décision, les responsables opérationnels, les partenaires institutionnels, les établissements financiers, les auditeurs et, lorsque la législation applicable l'exige, les autorités administratives, judiciaires ou de contrôle compétentes. Il veille à ce que toute coopération s'effectue dans le respect des lois, de la confidentialité des informations, des droits des personnes concernées et des procédures internes de l'Organisation.

Le Président Général s'assure également que les collaborateurs, bénévoles, administrateurs et représentants de l'Organisation bénéficient de formations régulières en matière de conformité, de gouvernance, d'éthique, de prévention des risques, de lutte contre la fraude, de protection des données et de lutte contre le blanchiment de capitaux et le financement du terrorisme. Il encourage le développement d'une culture de vigilance partagée dans laquelle chaque acteur comprend ses responsabilités et contribue activement à la protection de l'intégrité institutionnelle de l'Organisation.

Enfin, le Président Général est le garant de l'engagement institutionnel d'AGCE International en faveur d'une gouvernance exemplaire, conforme aux meilleures pratiques nationales et internationales. Par son autorité, son exemplarité et son devoir de supervision, il veille à ce que l'ensemble des décisions stratégiques et opérationnelles soient prises dans le respect des principes de légalité, de transparence, de responsabilité, de bonne gouvernance et de conformité, afin de préserver durablement la crédibilité, la réputation et la mission humanitaire de l'Organisation auprès des autorités publiques, des partenaires techniques et financiers, des bailleurs de fonds, des institutions financières et des communautés bénéficiaires.

4.2 Conseil ou Comité des Sages

Le **Conseil ou Comité des Sages** constitue un organe consultatif stratégique de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**, chargé d'accompagner le Président Général, le Collège Central et le Bureau Exécutif dans la consolidation d'une gouvernance exemplaire en matière de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Par son indépendance morale, son expérience, son impartialité et son expertise multidisciplinaire, il contribue au renforcement de l'intégrité institutionnelle, de la transparence, de la conformité et de la gestion responsable des risques auxquels l'Organisation peut être confrontée.

Le Conseil ou Comité des Sages intervient comme une instance de réflexion, d'orientation et de conseil sur les questions présentant des enjeux majeurs de gouvernance, d'éthique, de conformité réglementaire, de responsabilité institutionnelle et de protection de la réputation de l'Organisation. Il apporte un avis indépendant sur les politiques, procédures et dispositifs internes destinés à prévenir les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de conflits d'intérêts, de détournement de ressources ou de toute autre atteinte aux valeurs fondamentales d'AGCE International.

Dans le cadre de ses missions, le Conseil ou Comité des Sages examine les orientations stratégiques proposées en matière de conformité LBC/FT afin d'apprécier leur cohérence avec les objectifs institutionnels, les exigences légales, les normes internationales et les principes de bonne gouvernance. Il peut formuler des recommandations visant à améliorer les procédures internes, à renforcer les mécanismes de contrôle, à consolider les dispositifs de prévention des risques et à promouvoir une culture organisationnelle fondée sur l'éthique, la responsabilité et la transparence.

Le Conseil ou Comité des Sages veille également à préserver les intérêts supérieurs de l'Organisation en attirant l'attention des organes dirigeants sur les risques stratégiques susceptibles d'affecter la crédibilité, la réputation ou la pérennité d'AGCE International. À cet effet, il peut être consulté sur les partenariats sensibles, les projets de coopération internationale, les mécanismes de financement, les opérations présentant un niveau de risque élevé, les situations exceptionnelles ou les décisions pouvant avoir un impact significatif sur la gouvernance institutionnelle.

Dans l'exercice de ses responsabilités, le Conseil ou Comité des Sages encourage le respect des principes de séparation des fonctions, de redevabilité, de traçabilité, de contrôle interne, de gestion des conflits d'intérêts et de protection des ressources institutionnelles. Il veille à ce que les mécanismes de gouvernance permettent une prise de décision objective, documentée, transparente et conforme aux politiques internes de l'Organisation ainsi qu'aux exigences applicables en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Le Conseil ou Comité des Sages peut être saisi par le Président Général, le Collège Central, le Bureau Exécutif ou tout organe compétent lorsque des questions de gouvernance, de conformité ou d'éthique nécessitent une appréciation indépendante. Ses avis, bien que consultatifs, constituent un appui stratégique important pour éclairer les décisions des instances dirigeantes et favoriser une gestion prudente des risques institutionnels. Il peut également proposer des recommandations de nature préventive afin d'anticiper les évolutions réglementaires, les nouvelles menaces liées à la criminalité financière ou les améliorations susceptibles de renforcer le dispositif LBC/FT de l'Organisation.

Le Conseil ou Comité des Sages veille en outre à promouvoir une culture institutionnelle reposant sur l'exemplarité, l'intégrité personnelle des dirigeants, le respect des obligations de conformité et la protection de l'intérêt général poursuivi par AGCE International. Il encourage le développement de bonnes pratiques de gouvernance, la sensibilisation des responsables aux risques émergents et l'adoption de mesures proportionnées permettant de garantir une gestion saine, transparente et responsable des ressources confiées à l'Organisation.

Les membres du Conseil ou Comité des Sages exercent leurs fonctions avec indépendance, objectivité, impartialité, discrétion et loyauté. Ils sont soumis à une obligation stricte de confidentialité concernant les informations auxquelles ils ont accès dans le cadre de leurs missions et s'abstiennent de participer à toute délibération susceptible de les placer en situation de conflit d'intérêts. Ils agissent exclusivement dans l'intérêt de l'Organisation, sans rechercher d'avantage personnel ou de bénéfice indu.

Enfin, le Conseil ou Comité des Sages contribue à l'amélioration continue du système de gouvernance d'AGCE International en évaluant régulièrement la pertinence des dispositifs de conformité, en encourageant l'adoption des meilleures pratiques nationales et internationales et en formulant des recommandations destinées à renforcer durablement la prévention du blanchiment de capitaux, du financement du terrorisme et de toute forme de criminalité financière. Par son rôle de garant moral et institutionnel, il participe activement à la consolidation de la confiance des autorités publiques, des partenaires techniques et financiers, des bailleurs de fonds, des institutions financières et des communautés bénéficiaires envers AGCE International.

4.3 Responsable Conformité

Le **Responsable Conformité** occupe une fonction stratégique au sein du dispositif de gouvernance de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il est chargé de concevoir, coordonner, superviser et faire évoluer le système institutionnel de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** afin de garantir que l'ensemble des activités de l'Organisation soient conduites dans le respect des lois applicables, des normes internationales, des politiques internes et des principes de bonne gouvernance. Son action contribue directement à la protection de l'intégrité, de la réputation et de la crédibilité de l'Organisation

auprès des autorités publiques, des partenaires techniques et financiers, des bailleurs de fonds, des institutions financières et des bénéficiaires.

Le Responsable Conformité exerce ses missions avec indépendance fonctionnelle, impartialité, objectivité et confidentialité. Il dispose d'un accès direct au **Président Général**, au **Collège Central** ainsi qu'au **Bureau Exécutif** pour toute question présentant un risque significatif en matière de conformité ou nécessitant une décision stratégique. Dans l'exercice de ses responsabilités, il agit sans subir d'influence susceptible de compromettre son jugement professionnel et bénéficie des moyens humains, techniques et organisationnels nécessaires à l'accomplissement de ses missions.

Il est chargé d'élaborer, de mettre à jour et de diffuser les politiques, procédures, guides opérationnels et référentiels internes relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Il veille à ce que ces documents soient conformes aux exigences légales et réglementaires en vigueur dans les juridictions où AGCE International exerce ses activités, tout en intégrant les meilleures pratiques internationales en matière de gouvernance, de gestion des risques et de conformité institutionnelle.

Le Responsable Conformité met en œuvre une approche fondée sur les risques afin d'identifier, d'évaluer, de hiérarchiser et de surveiller les risques susceptibles d'affecter l'Organisation. À cette fin, il réalise des évaluations périodiques portant notamment sur les sources de financement, les dons, les cotisations, les partenariats, les projets internationaux, les opérations financières, les paiements électroniques, les transferts de fonds, les fournisseurs, les prestataires, les bénéficiaires effectifs et toute autre activité présentant un risque particulier. Les résultats de ces analyses donnent lieu à des recommandations destinées à renforcer les mesures de prévention et de contrôle.

Dans le cadre des procédures de vigilance, le Responsable Conformité supervise la mise en œuvre des mécanismes de connaissance des membres, des donateurs, des partenaires, des bénéficiaires, des fournisseurs et des autres parties prenantes, conformément aux principes de **Know Your Customer (KYC)**, de vérification de l'identité, d'identification du bénéficiaire effectif lorsque cela est nécessaire, d'analyse de l'origine des fonds et d'évaluation du niveau de risque associé aux relations d'affaires ou de coopération. Il veille à ce que les diligences appropriées soient réalisées avant toute opération significative ou tout engagement institutionnel.

Le Responsable Conformité assure également une mission permanente de contrôle et de surveillance. Il vérifie la correcte application des procédures internes, contrôle la qualité des dispositifs de traçabilité documentaire, examine les opérations susceptibles de présenter un caractère inhabituel ou à risque, analyse les alertes de conformité et coordonne les investigations internes lorsque des anomalies, des irrégularités ou des indices de blanchiment de capitaux ou de financement du terrorisme sont identifiés. Il formule, le cas échéant, les recommandations nécessaires afin de prévenir la réitération des incidents constatés.

Il organise et anime les programmes de sensibilisation et de formation destinés aux administrateurs, responsables d'antennes, collaborateurs, bénévoles, consultants et partenaires intervenant pour le compte de l'Organisation. Ces actions visent à développer une culture institutionnelle de conformité, à renforcer la compréhension des obligations légales et réglementaires, à améliorer la capacité de détection des risques et à promouvoir les bonnes pratiques en matière de gouvernance, d'éthique et de prévention de la criminalité financière.

Le Responsable Conformité établit périodiquement des rapports destinés au Président Général, au Collège Central et au Bureau Exécutif. Ces rapports présentent notamment l'état de conformité de l'Organisation, les résultats des évaluations des risques, les incidents constatés, les mesures correctives engagées, les recommandations d'amélioration ainsi que les évolutions réglementaires susceptibles d'avoir un impact sur les activités d'AGCE International. Il assure également le suivi de la mise en œuvre des recommandations issues des audits internes, des audits externes, des inspections ou des contrôles réalisés par les autorités compétentes.

Dans le cadre de ses fonctions, le Responsable Conformité entretient des relations professionnelles avec les établissements financiers, les auditeurs, les commissaires aux comptes, les experts indépendants et, lorsque la loi l'exige, les autorités administratives, judiciaires, fiscales ou de renseignement financier. Toute coopération s'effectue dans le strict respect des procédures internes, des obligations légales, du secret professionnel, de la confidentialité des informations et de la protection des données personnelles.

Enfin, le Responsable Conformité constitue un acteur essentiel de l'amélioration continue du système de gouvernance d'AGCE International. Il assure une veille permanente sur les évolutions législatives, réglementaires, normatives et technologiques relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme, propose les adaptations nécessaires des politiques institutionnelles et contribue au renforcement durable de la résilience, de la transparence et de la conformité de l'Organisation face aux risques émergents de criminalité financière.

4.4 Responsable Financier

Le **Responsable Financier** occupe une fonction essentielle dans le dispositif de gouvernance de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Dans le cadre de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, il est chargé d'assurer une gestion financière conforme aux exigences légales, réglementaires, comptables et institutionnelles, tout en garantissant la transparence, la traçabilité, la sécurité et la régularité de l'ensemble des flux financiers de l'Organisation. Son action contribue directement à la préservation de l'intégrité financière de l'Organisation ainsi qu'à la prévention des risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption et de détournement de ressources.

Le Responsable Financier veille à ce que toutes les recettes, dépenses, dons, cotisations, subventions, financements, paiements, remboursements, acquisitions, transferts bancaires, opérations de change et autres mouvements financiers soient réalisés conformément aux procédures internes de gestion financière, aux règles de contrôle interne, aux principes comptables applicables ainsi qu'aux exigences définies dans la présente politique. Il s'assure que chaque opération repose sur une justification légitime, une autorisation préalable appropriée, une documentation complète et une comptabilisation fidèle permettant d'en garantir la parfaite traçabilité.

Dans l'exercice de ses responsabilités, le Responsable Financier participe activement à l'identification et à l'évaluation des risques financiers susceptibles d'affecter l'Organisation. En collaboration avec le Responsable Conformité et les autres organes de gouvernance, il met en œuvre une approche fondée sur les risques afin de détecter les opérations inhabituelles, les transactions complexes, les flux financiers atypiques, les paiements non justifiés, les mouvements internationaux sensibles ou toute autre opération pouvant présenter un risque de blanchiment de capitaux ou de financement du terrorisme. Lorsque des anomalies sont identifiées, il applique les procédures internes de vigilance, suspend les opérations lorsque cela est nécessaire et informe sans délai les autorités internes compétentes conformément aux procédures institutionnelles.

Le Responsable Financier assure la supervision des relations avec les établissements bancaires, les organismes de paiement, les partenaires financiers et les prestataires de services financiers utilisés par AGCE International. Il veille à ce que les comptes bancaires soient ouverts, utilisés et administrés conformément aux autorisations institutionnelles, que les opérations soient exécutées dans un environnement sécurisé et que les mécanismes de contrôle des paiements garantissent une protection efficace contre les risques de fraude, de falsification, d'usurpation d'identité ou de détournement de fonds.

Il est responsable de la fiabilité des enregistrements comptables, de la qualité des justificatifs financiers, de la conservation des pièces comptables et de l'intégrité des systèmes d'information financière. Il veille à ce que toutes les opérations soient enregistrées de manière chronologique, exhaustive, exacte et vérifiable, permettant ainsi aux auditeurs internes, aux commissaires aux comptes, aux autorités compétentes et aux partenaires habilités de reconstituer l'historique complet des opérations réalisées par l'Organisation. Il s'assure également que les documents financiers soient conservés pendant les délais prévus par les législations applicables et les politiques internes d'archivage.

Le Responsable Financier participe à la préparation des budgets institutionnels, au suivi de leur exécution et à la production des états financiers, rapports de gestion, tableaux de bord et autres documents destinés aux organes de gouvernance. Il veille à ce que les informations financières communiquées soient exactes, sincères, complètes et conformes à la réalité des opérations réalisées. Il contribue ainsi au renforcement de la transparence financière, de la redevabilité et de la confiance accordée à AGCE International par les donateurs, les partenaires techniques et financiers, les bailleurs de fonds, les institutions financières et les autorités publiques.

En matière de contrôle interne, le Responsable Financier applique rigoureusement les principes de séparation des fonctions, de double validation des opérations sensibles, de limitation des pouvoirs de signature, de contrôle des accès aux systèmes financiers et de rapprochement régulier des comptes. Il participe aux audits internes et externes, met en œuvre les recommandations formulées à l'issue des contrôles et propose toute mesure susceptible d'améliorer la sécurité financière, la qualité des procédures et l'efficacité du dispositif LBC/FT.

Le Responsable Financier contribue également au développement d'une culture institutionnelle de conformité financière. Il sensibilise les collaborateurs concernés aux bonnes pratiques de gestion financière, aux obligations réglementaires, aux procédures de vigilance applicables aux flux financiers et aux risques liés au blanchiment de capitaux et au financement du terrorisme. Il favorise une gestion prudente, responsable et documentée des ressources confiées à l'Organisation.

Enfin, le Responsable Financier agit en étroite coordination avec le Président Général, le Collège Central, le Bureau Exécutif, le Responsable Conformité, les auditeurs internes et externes ainsi que les autorités compétentes lorsque la législation l'exige. Par son expertise technique, son devoir de vigilance et son engagement en faveur de la transparence, il constitue un acteur majeur du dispositif institutionnel de gouvernance financière et de conformité d'AGCE International, garantissant que l'ensemble des ressources financières de l'Organisation soient gérées avec intégrité, responsabilité et dans le strict respect des exigences de lutte contre le blanchiment de capitaux et le financement du terrorisme.

4.5 Responsable Informatique

Le **Responsable Informatique** occupe une fonction stratégique dans le dispositif de gouvernance de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Dans le cadre de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, il est chargé de garantir la sécurité, l'intégrité, la disponibilité, la confidentialité et la traçabilité des systèmes d'information, des infrastructures numériques, des plateformes technologiques et des données utilisées par l'Organisation. Son rôle est essentiel pour prévenir les risques de criminalité financière liés aux technologies numériques, protéger les actifs informationnels et assurer la conformité des traitements informatiques avec les exigences légales, réglementaires et institutionnelles.

Le Responsable Informatique conçoit, déploie, administre et maintient les infrastructures numériques de l'Organisation en veillant à ce qu'elles offrent un niveau élevé de sécurité face aux risques de cybercriminalité, d'accès non autorisés, de fraude électronique, d'usurpation d'identité, de falsification documentaire, de manipulation des données, d'intrusion informatique, de rançongiciels, de compromission des systèmes ou de toute autre menace susceptible de porter atteinte au dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme. Il veille à ce que les solutions numériques mises en œuvre soient

adaptées aux besoins opérationnels d'AGCE International et respectent les principes de sécurité dès la conception.

Le Responsable Informatique garantit la mise en œuvre de mécanismes de contrôle d'accès robustes fondés sur le principe du moindre privilège. Chaque utilisateur bénéficie uniquement des droits strictement nécessaires à l'exercice de ses fonctions. Les habilitations sont créées, modifiées, suspendues ou supprimées selon des procédures formalisées, documentées et régulièrement révisées. Les accès aux applications financières, aux bases de données, aux plateformes de gestion des membres, aux systèmes comptables, aux outils de paiement électronique et aux espaces d'administration font l'objet d'une surveillance renforcée afin de limiter les risques d'utilisation abusive ou frauduleuse.

Dans le cadre du dispositif LBC/FT, le Responsable Informatique assure la fiabilité et la traçabilité des traitements numériques. Il veille à ce que chaque opération réalisée sur les systèmes d'information fasse l'objet d'un enregistrement sécurisé permettant d'identifier l'utilisateur concerné, la date, l'heure, la nature de l'action effectuée ainsi que les modifications apportées aux données. Ces journaux d'événements sont protégés contre toute altération, conservés conformément aux politiques d'archivage de l'Organisation et mis à disposition des personnes habilitées dans le cadre des audits, des contrôles internes ou des investigations autorisées.

Le Responsable Informatique participe activement à la protection des données personnelles, des informations financières, des documents institutionnels et des informations confidentielles traitées par AGCE International. Il met en œuvre des solutions de chiffrement, d'authentification forte, de segmentation des réseaux, de protection contre les logiciels malveillants, de surveillance des infrastructures, de sauvegarde régulière des données et de reprise d'activité en cas d'incident majeur. Il veille également à ce que les équipements informatiques, les serveurs, les services infonuagiques (cloud), les applications mobiles et les plateformes web respectent les exigences de sécurité définies par les politiques internes de l'Organisation.

En collaboration avec le Responsable Conformité et le Responsable Financier, le Responsable Informatique contribue à la mise en œuvre des dispositifs numériques de connaissance des parties prenantes (KYC), de vérification documentaire, d'analyse des risques, de surveillance des transactions électroniques et de conservation des preuves numériques. Il participe à l'intégration de solutions technologiques permettant d'améliorer la détection des comportements anormaux, la sécurisation des paiements, l'authentification des utilisateurs et la prévention des tentatives de fraude ou de blanchiment de capitaux utilisant les technologies numériques.

Le Responsable Informatique assure également une veille permanente sur les évolutions technologiques, les nouvelles menaces cybernétiques, les vulnérabilités des systèmes, les exigences réglementaires relatives à la cybersécurité ainsi que les innovations susceptibles de renforcer les capacités de prévention et de contrôle de l'Organisation. Il organise régulièrement des évaluations de sécurité, des tests de vulnérabilité, des contrôles

techniques et des exercices de gestion de crise afin d'améliorer la résilience des infrastructures numériques et de réduire les risques opérationnels.

Il sensibilise et forme les administrateurs, les collaborateurs, les bénévoles, les responsables d'antennes et les partenaires utilisant les systèmes d'information d'AGCE International aux bonnes pratiques de cybersécurité, à la protection des données, à la gestion sécurisée des identifiants, à la détection des tentatives d'hameçonnage, à la prévention des fraudes électroniques et aux obligations liées à la présente Politique LBC/FT. Cette démarche contribue au développement d'une culture institutionnelle de sécurité numérique reposant sur la vigilance, la responsabilité et la prévention.

Enfin, le Responsable Informatique travaille en étroite coordination avec le Président Général, le Collège Central, le Bureau Exécutif, le Responsable Conformité, le Responsable Financier, les auditeurs internes et externes ainsi que, lorsque la législation l'exige, les autorités compétentes. Il veille à ce que les systèmes d'information constituent un véritable levier de gouvernance, de transparence et de conformité, permettant à AGCE International de protéger durablement ses ressources numériques, de sécuriser ses opérations financières et de garantir l'intégrité de son dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme.

4.6 Auditeur interne

L'**Auditeur interne** constitue un acteur indépendant et essentiel du dispositif de gouvernance de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Dans le cadre de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, il a pour mission d'évaluer de manière objective, impartiale et méthodique l'efficacité des mécanismes de gouvernance, de gestion des risques, de contrôle interne et de conformité mis en œuvre par l'Organisation. Son intervention vise à fournir aux organes dirigeants une assurance raisonnable sur la maîtrise des risques liés au blanchiment de capitaux, au financement du terrorisme, à la fraude, à la corruption, au détournement de ressources et aux autres formes de criminalité financière.

L'Auditeur interne exerce ses fonctions en toute indépendance vis-à-vis des activités qu'il contrôle. Afin de préserver son objectivité, il ne participe pas directement à l'exécution des opérations qu'il est amené à auditer et ne peut être placé dans une situation de conflit d'intérêts susceptible d'altérer son jugement professionnel. Il rend compte de ses travaux au **Président Général**, au **Collège Central**, au **Bureau Exécutif** ou à tout organe de gouvernance compétent désigné par l'Organisation, garantissant ainsi la transparence et la crédibilité de ses conclusions.

Dans le cadre de ses missions, l'Auditeur interne procède à des évaluations régulières des politiques, procédures, mécanismes de contrôle et dispositifs opérationnels relatifs à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Il vérifie notamment

que les procédures de connaissance des parties prenantes (KYC), les mesures de vigilance, les contrôles financiers, les mécanismes d'autorisation, les processus de validation, les dispositifs de traçabilité, les systèmes d'information, les procédures documentaires ainsi que les obligations de conservation des données sont effectivement appliqués et demeurent conformes aux exigences légales, réglementaires et institutionnelles.

L'Auditeur interne évalue également l'efficacité du dispositif de gestion des risques adopté par AGCE International. Il apprécie la pertinence des méthodes d'identification, d'analyse, de hiérarchisation et de traitement des risques liés aux activités de l'Organisation. À cette fin, il examine les opérations financières, les partenariats nationaux et internationaux, les dons, les subventions, les cotisations, les transferts bancaires, les acquisitions, les contrats, les projets et toute activité présentant un niveau de risque susceptible d'exposer l'Organisation à des tentatives de blanchiment de capitaux ou de financement du terrorisme.

Dans le cadre de ses contrôles, l'Auditeur interne dispose d'un droit d'accès aux informations, documents, systèmes d'information, registres administratifs, pièces comptables, justificatifs financiers et autres éléments nécessaires à l'accomplissement de ses missions, sous réserve du respect des règles relatives à la confidentialité, à la protection des données personnelles et au secret professionnel. Les responsables, collaborateurs, bénévoles et représentants de l'Organisation sont tenus de coopérer pleinement avec l'Auditeur interne en lui fournissant les informations exactes, complètes et sincères nécessaires à la réalisation de ses travaux.

À l'issue de chaque mission, l'Auditeur interne établit un rapport détaillé présentant les constats effectués, les risques identifiés, les écarts observés, les insuffisances relevées ainsi que les recommandations destinées à renforcer le dispositif de gouvernance, de contrôle interne et de conformité. Ces rapports comportent, lorsque cela est pertinent, un plan d'actions correctives, des priorités de mise en œuvre, des délais de réalisation et un suivi des recommandations formulées lors des audits précédents. L'objectif est de favoriser une amélioration continue des pratiques de gestion et de prévenir la réapparition des anomalies constatées.

L'Auditeur interne assure également un suivi régulier de la mise en œuvre des recommandations issues des audits internes, des audits externes, des inspections réglementaires, des évaluations de conformité et des contrôles réalisés par les autorités compétentes. Il vérifie que les mesures correctives décidées par les organes dirigeants sont effectivement appliquées, adaptées aux risques identifiés et suffisamment efficaces pour prévenir leur récurrence. En cas de manquement significatif ou de risque majeur, il en informe sans délai les instances de gouvernance compétentes afin que les décisions appropriées puissent être prises.

Par ailleurs, l'Auditeur interne contribue activement au développement d'une culture institutionnelle fondée sur la maîtrise des risques, l'éthique, la transparence et la responsabilité. Sans se substituer aux fonctions opérationnelles, il participe aux actions de sensibilisation en partageant les bonnes pratiques issues de ses missions, en formulant des recommandations

d'amélioration des procédures et en accompagnant les responsables dans le renforcement des dispositifs de contrôle interne. Son rôle est avant tout préventif, pédagogique et stratégique, visant à accroître la maturité du système de gouvernance de l'Organisation.

Enfin, l'Auditeur interne assure une veille permanente sur l'évolution des normes professionnelles d'audit, des référentiels internationaux de gouvernance, des exigences réglementaires en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme ainsi que des risques émergents susceptibles d'affecter les organisations à but non lucratif. Par son indépendance, son expertise et la qualité de ses évaluations, il contribue au renforcement durable de la gouvernance, de la conformité et de la crédibilité d'AGCE International, garantissant que les ressources confiées à l'Organisation soient gérées avec intégrité, transparence, efficacité et dans le strict respect des meilleures pratiques nationales et internationales.

4.7 Commissaire aux comptes

Le **Commissaire aux comptes** constitue un acteur indépendant de la gouvernance financière et de la conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Dans le cadre de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, il exerce une mission d'intérêt général visant à renforcer la transparence, la fiabilité des informations financières, la crédibilité institutionnelle et la confiance des membres, des partenaires, des donateurs, des bailleurs de fonds, des institutions financières et des autorités compétentes. Son intervention contribue à garantir que les ressources de l'Organisation soient administrées conformément aux exigences légales, réglementaires, comptables et aux principes de bonne gouvernance.

Le Commissaire aux comptes exerce ses missions en toute indépendance, impartialité, objectivité et intégrité professionnelle. Il ne peut recevoir aucune instruction susceptible d'influencer ses conclusions, ni participer à des activités incompatibles avec sa mission de contrôle. Il agit dans le respect des normes professionnelles applicables à l'audit légal et des règles déontologiques qui encadrent sa profession. Son indépendance constitue une garantie essentielle de la crédibilité de ses travaux et de la confiance accordée à ses conclusions par les organes de gouvernance et les parties prenantes.

Dans le cadre de ses missions, le Commissaire aux comptes procède à l'examen des états financiers, des registres comptables, des pièces justificatives, des opérations financières, des procédures comptables ainsi que des mécanismes de contrôle interne ayant une incidence sur la fiabilité de l'information financière. Il apprécie la sincérité, la régularité, l'exactitude et la fidélité des comptes produits par l'Organisation, tout en évaluant si les opérations financières sont correctement enregistrées, documentées et justifiées conformément aux politiques internes et aux dispositions légales applicables.

Le Commissaire aux comptes porte une attention particulière aux risques susceptibles d'affecter la sécurité financière de l'Organisation, notamment les risques de blanchiment de capitaux, de financement du terrorisme, de fraude comptable, de détournement de fonds, de falsification documentaire, de conflits d'intérêts, de paiements irréguliers ou d'utilisation abusive des ressources institutionnelles. Sans se substituer aux organes de gestion ni au Responsable Conformité, il apprécie si les dispositifs de contrôle interne mis en place sont raisonnablement adaptés pour prévenir ou détecter ces risques et formule, lorsque cela est nécessaire, des recommandations destinées à renforcer leur efficacité.

Le Commissaire aux comptes examine également la conformité des opérations financières avec les procédures d'autorisation, de validation, de séparation des fonctions, de traçabilité, de conservation des pièces justificatives et de sécurisation des flux financiers. Il vérifie que les recettes, dons, cotisations, subventions, financements, acquisitions, paiements, remboursements et transferts de fonds sont enregistrés de manière régulière et peuvent être justifiés par des documents fiables, complets et accessibles en cas de contrôle ou d'audit.

Dans l'accomplissement de sa mission, le Commissaire aux comptes bénéficie d'un droit d'accès aux documents, registres, informations et systèmes nécessaires à la réalisation de ses travaux, dans le respect des règles relatives à la confidentialité, à la protection des données personnelles et au secret professionnel. Les organes dirigeants, les responsables administratifs et financiers ainsi que les collaborateurs concernés sont tenus de faciliter l'exercice de sa mission en mettant à sa disposition les informations exactes, complètes et sincères requises pour l'évaluation des comptes et des procédures.

À l'issue de ses travaux, le Commissaire aux comptes établit un rapport présentant ses conclusions sur la régularité, la sincérité et la fidélité des états financiers ainsi que, le cas échéant, les observations, réserves ou recommandations qu'il estime nécessaires. Ces rapports sont destinés aux organes de gouvernance compétents et constituent un outil majeur d'amélioration de la gouvernance financière, du contrôle interne et du dispositif de conformité de l'Organisation. Les recommandations formulées font l'objet d'un suivi afin de s'assurer de leur mise en œuvre effective et de renforcer durablement les mécanismes de prévention des risques.

Lorsque le Commissaire aux comptes identifie des irrégularités significatives, des anomalies financières importantes ou des indices sérieux pouvant laisser présumer l'existence d'opérations illicites, il en informe les organes compétents de l'Organisation conformément aux procédures internes et aux obligations professionnelles qui lui sont applicables. Lorsque les lois en vigueur imposent une obligation de signalement ou de coopération avec les autorités compétentes, il agit dans le strict respect du cadre juridique applicable, des exigences déontologiques de sa profession et des droits des personnes concernées.

Le Commissaire aux comptes entretient une coopération constructive avec le Président Général, le Collège Central, le Bureau Exécutif, le Responsable Financier, le Responsable Conformité, l'Auditeur interne et les autres organes de gouvernance, tout en préservant son indépendance fonctionnelle. Cette collaboration permet d'améliorer la qualité

du contrôle interne, de renforcer la maîtrise des risques, de consolider la transparence financière et d'assurer une meilleure coordination des actions de prévention du blanchiment de capitaux et du financement du terrorisme.

Enfin, le Commissaire aux comptes participe au renforcement de la confiance institutionnelle d'AGCE International auprès de ses partenaires nationaux et internationaux. Par la qualité de ses vérifications, la rigueur de ses analyses, son indépendance et son professionnalisme, il contribue à démontrer que les ressources confiées à l'Organisation sont administrées avec intégrité, responsabilité, transparence et conformément aux meilleures pratiques de gouvernance financière, de conformité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

4.8 Membres et Bénévoles

Les **membres et bénévoles** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** constituent des acteurs essentiels de la réalisation de la mission humanitaire, sociale, éducative, sanitaire, économique et numérique de l'Organisation. À ce titre, ils participent activement au maintien d'une culture institutionnelle fondée sur l'intégrité, la transparence, la responsabilité et le respect des exigences de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Bien que leurs responsabilités puissent varier selon leurs fonctions, leurs niveaux d'engagement ou leurs domaines d'intervention, ils demeurent tous tenus de respecter les principes, règles et procédures définis par la présente politique ainsi que l'ensemble des textes internes régissant la gouvernance d'AGCE International.

Chaque membre et bénévole est tenu d'exercer ses activités avec honnêteté, impartialité, loyauté et professionnalisme. Il lui appartient d'agir exclusivement dans l'intérêt de l'Organisation, de préserver sa réputation et de s'abstenir de toute action susceptible de compromettre la conformité de ses activités aux lois applicables ou aux normes éthiques de l'Organisation. Toute mission confiée doit être exécutée avec diligence, dans le respect des procédures administratives, financières, opérationnelles et des règles relatives à la gestion des risques.

Les membres et bénévoles ont l'obligation de connaître et d'appliquer les politiques institutionnelles relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme. Ils doivent respecter les procédures de vigilance mises en place par l'Organisation, notamment celles relatives à l'identification des partenaires, à la protection des ressources institutionnelles, à la gestion documentaire, à la confidentialité des informations, à la prévention des conflits d'intérêts et au signalement des situations présentant un risque de fraude ou d'irrégularité. Ils contribuent ainsi, par leur comportement quotidien, à renforcer la sécurité, la transparence et la crédibilité de l'Organisation.

Dans le cadre de leurs activités, les membres et bénévoles veillent à ne jamais accepter, solliciter, faciliter ou dissimuler des opérations dont l'origine, la destination ou la

finalité apparaît douteuse ou incompatible avec les missions d'AGCE International. Ils s'abstiennent de participer à toute opération susceptible de favoriser le blanchiment de capitaux, le financement du terrorisme, la corruption, la fraude, le détournement de ressources ou toute autre activité illicite. En présence d'une situation inhabituelle ou d'un doute raisonnable, ils appliquent le principe de vigilance et informent sans délai les responsables compétents conformément aux procédures internes de signalement.

Les membres et bénévoles sont également tenus de protéger les biens matériels, financiers, documentaires, numériques et immatériels mis à leur disposition par l'Organisation. Ils utilisent les équipements, les ressources financières, les moyens de communication, les systèmes d'information, les applications numériques et les données institutionnelles exclusivement dans le cadre des missions qui leur sont confiées et conformément aux politiques de sécurité, de confidentialité et de protection des données adoptées par AGCE International. Toute utilisation abusive, non autorisée ou frauduleuse des ressources de l'Organisation est strictement interdite.

L'Organisation veille à ce que chaque membre et bénévole bénéficie d'une information appropriée ainsi que de formations régulières portant sur les principes de gouvernance, l'éthique, la prévention des risques, la conformité réglementaire, la protection des données personnelles, la cybersécurité, la lutte contre la fraude ainsi que la lutte contre le blanchiment de capitaux et le financement du terrorisme. Ces actions de sensibilisation permettent de développer une culture commune de vigilance et de responsabilité, adaptée aux missions exercées par chacun.

Les membres et bénévoles sont soumis à une obligation permanente de confidentialité concernant les informations auxquelles ils ont accès dans le cadre de leurs fonctions. Ils s'interdisent toute divulgation non autorisée d'informations relatives aux membres, donateurs, bénéficiaires, partenaires, projets, opérations financières, procédures internes, données personnelles ou informations stratégiques de l'Organisation. Cette obligation demeure applicable pendant toute la durée de leur engagement et, lorsque les textes applicables ou leurs engagements contractuels le prévoient, après la cessation de leurs fonctions.

Les membres et bénévoles sont également tenus de déclarer toute situation réelle, potentielle ou apparente de conflit d'intérêts susceptible d'affecter leur impartialité ou de compromettre les intérêts de l'Organisation. Ils doivent s'abstenir de participer à toute décision ou opération dans laquelle ils pourraient retirer un avantage personnel, direct ou indirect, ou favoriser indûment un tiers. Cette obligation participe au maintien d'une gouvernance transparente, équitable et conforme aux principes d'intégrité défendus par AGCE International.

En cas de manquement aux dispositions de la présente Politique LBC/FT, les membres et bénévoles peuvent faire l'objet de mesures disciplinaires, administratives ou de toute autre mesure prévue par les statuts, le règlement intérieur, les codes de conduite et les politiques internes de l'Organisation, sans préjudice des poursuites civiles, administratives ou pénales susceptibles d'être engagées en application des lois en vigueur.

Enfin, les membres et bénévoles constituent les premiers ambassadeurs des valeurs d'AGCE International. Par leur exemplarité, leur sens des responsabilités, leur vigilance et leur engagement quotidien, ils participent activement au renforcement du dispositif de gouvernance, de contrôle interne et de conformité de l'Organisation. Leur contribution permet de préserver la confiance des autorités publiques, des partenaires techniques et financiers, des bailleurs de fonds, des institutions financières, des donateurs et des communautés bénéficiaires, tout en garantissant que les ressources mobilisées par AGCE International soient exclusivement consacrées à la réalisation de ses missions d'intérêt général dans le respect des principes les plus exigeants de transparence, d'intégrité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

CHAPITRE 5

APPROCHE BASÉE SUR LES RISQUES

L'Approche Basée sur les Risques (ABR) constitue le principe directeur du dispositif de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle repose sur le principe selon lequel les ressources humaines, financières, techniques et organisationnelles de l'Organisation doivent être mobilisées de manière proportionnée aux risques identifiés, afin de garantir une prévention efficace des tentatives de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption et des autres formes de criminalité financière susceptibles d'affecter ses activités.

Cette approche permet à l'Organisation d'adapter ses mesures de vigilance, de contrôle, de surveillance et de conformité à la nature, à la complexité, au volume et au niveau d'exposition de chacune de ses activités. Elle favorise une gestion proactive des risques en évitant une application uniforme des contrôles, tout en assurant que les ressources institutionnelles soient concentrées sur les domaines présentant les risques les plus élevés.

L'Approche Basée sur les Risques est intégrée à l'ensemble des processus décisionnels d'AGCE International, notamment lors de l'admission des membres, de l'identification des partenaires, de la sélection des fournisseurs, de la réception des dons, de la gestion des cotisations, de l'exécution des projets, de la conclusion des conventions de partenariat, des opérations financières nationales et internationales, des paiements électroniques, des transferts bancaires, des campagnes de collecte de fonds, des activités numériques ainsi que des programmes de coopération internationale. Chaque activité fait l'objet d'une évaluation préalable permettant de déterminer le niveau de vigilance approprié.

L'Organisation procède régulièrement à l'identification des facteurs susceptibles d'accroître son exposition aux risques. Cette analyse tient notamment compte de la nature des services proposés, des catégories de membres et de partenaires, des sources de financement, des modes de paiement utilisés, des zones géographiques d'intervention, des secteurs d'activité concernés, des technologies employées, des canaux numériques, des opérations transfrontalières, des bénéficiaires effectifs ainsi que de toute évolution susceptible d'influencer le niveau global de risque. Cette évaluation est révisée de manière périodique ou lorsqu'un changement significatif intervient dans les activités de l'Organisation.

L'Approche Basée sur les Risques s'appuie sur une classification des risques permettant de distinguer les situations présentant un niveau faible, modéré, élevé ou critique. Cette classification oriente l'intensité des mesures de vigilance, la fréquence des contrôles, le niveau d'autorisation requis, les procédures de validation, les exigences documentaires ainsi que les actions de surveillance mises en œuvre. Les opérations identifiées comme présentant un niveau de risque plus important font l'objet de diligences renforcées, d'un suivi plus étroit et, lorsque cela est nécessaire, d'une validation par les autorités compétentes de l'Organisation.

La mise en œuvre de cette approche repose sur une collaboration permanente entre le Président Général, le Collège Central, le Bureau Exécutif, le Responsable Conformité, le Responsable Financier, le Responsable Informatique, l'Auditeur interne, le Commissaire aux comptes, les responsables d'antennes ainsi que l'ensemble des membres, collaborateurs et bénévoles. Chaque acteur participe, dans le cadre de ses responsabilités, à l'identification, à l'évaluation, à la prévention, au traitement et au suivi des risques pouvant affecter l'Organisation.

Afin d'assurer l'efficacité de l'Approche Basée sur les Risques, AGCE International met en œuvre des procédures documentées de collecte d'informations, de vérification de l'identité des parties prenantes, de connaissance des membres et partenaires (KYC), d'identification des bénéficiaires effectifs lorsque cela est requis, de surveillance des opérations financières, de contrôle des paiements, de conservation des pièces justificatives, de traçabilité documentaire, de contrôle interne et d'audit. Ces dispositifs sont régulièrement évalués afin de vérifier leur pertinence face à l'évolution des menaces et des exigences réglementaires.

L'Organisation développe également une veille permanente portant sur les nouvelles typologies de blanchiment de capitaux, les techniques émergentes de financement du terrorisme, les risques liés aux technologies numériques, aux plateformes de paiement, aux monnaies virtuelles, aux cybermenaces ainsi qu'aux évolutions législatives et réglementaires nationales et internationales. Cette veille permet d'adapter rapidement les politiques, procédures et outils de contrôle afin de maintenir un niveau élevé de protection institutionnelle.

Enfin, l'Approche Basée sur les Risques s'inscrit dans une dynamique d'amélioration continue. Les conclusions des évaluations des risques, des audits internes et externes, des contrôles de conformité, des inspections réglementaires, des retours d'expérience opérationnels et des recommandations formulées par les autorités compétentes sont systématiquement analysées afin d'actualiser les dispositifs de prévention, de renforcer les capacités institutionnelles et d'améliorer la résilience de l'Organisation face aux risques financiers et opérationnels. Par cette démarche, **AGCE International – AGCE Canada** réaffirme son engagement à mettre en œuvre une gouvernance fondée sur la prudence, la proportionnalité, la transparence et la conformité, garantissant que l'ensemble de ses ressources demeure exclusivement consacré à la réalisation de ses missions humanitaires, sociales, éducatives, sanitaires, économiques et numériques, dans le strict respect des meilleures pratiques internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

5.1 Identification des risques

L'identification des risques constitue la première étape du dispositif d'**Approche Basée sur les Risques (ABR)** mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** dans le cadre de sa **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Elle consiste à recenser, analyser et comprendre l'ensemble des facteurs susceptibles d'exposer l'Organisation à des risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de ressources, de cybercriminalité ou de toute autre activité financière illicite pouvant compromettre l'intégrité de ses missions, de sa gouvernance ou de sa réputation.

Cette démarche est permanente, documentée et proportionnée à la nature des activités de l'Organisation. Elle permet d'anticiper les vulnérabilités avant qu'elles ne produisent des effets préjudiciables, d'adapter les dispositifs de contrôle aux risques effectivement rencontrés et d'orienter les décisions stratégiques en matière de conformité. L'identification des risques repose sur une analyse globale de l'environnement institutionnel, opérationnel, financier, juridique, technologique et géographique dans lequel AGCE International exerce ses activités.

L'Organisation procède à l'identification des risques avant l'établissement de toute relation institutionnelle, financière ou contractuelle significative, ainsi que lors de la création de nouveaux programmes, de l'ouverture de nouvelles antennes, de la mise en œuvre de plateformes numériques, de la réception de nouveaux financements ou lorsqu'un changement important intervient dans son environnement d'activité. Cette évaluation est régulièrement actualisée afin de tenir compte des évolutions réglementaires, des nouvelles menaces identifiées et des retours d'expérience issus des contrôles internes ou des audits.

L'identification des risques couvre l'ensemble des activités exercées par AGCE International. Sont notamment analysés les risques liés aux dons, aux cotisations, aux subventions, aux financements internationaux, aux partenariats institutionnels, aux campagnes de collecte de fonds, aux transferts bancaires, aux paiements électroniques, aux opérations transfrontalières, aux achats, aux contrats de prestation, aux activités humanitaires, aux programmes de développement, aux projets numériques, aux plateformes technologiques ainsi qu'aux échanges avec les membres, les bénéficiaires, les fournisseurs, les bailleurs de fonds et les partenaires nationaux ou internationaux.

Une attention particulière est portée aux risques liés aux personnes et aux organisations avec lesquelles AGCE International entretient des relations. L'Organisation procède à une analyse préalable des membres, donateurs, partenaires, fournisseurs, prestataires, bénéficiaires, représentants et autres parties prenantes afin d'évaluer leur identité, leur réputation, leur situation juridique, la transparence de leur gouvernance, la nature de leurs activités, l'origine de leurs ressources financières ainsi que, lorsque cela est nécessaire,

l'identification de leurs bénéficiaires effectifs. Cette démarche permet d'apprécier le niveau de confiance pouvant être accordé à chaque relation institutionnelle.

L'identification des risques tient également compte des facteurs géographiques. Les activités menées dans des pays ou territoires présentant un niveau élevé de criminalité financière, des dispositifs de contrôle insuffisants, des sanctions internationales, des conflits armés, une instabilité politique ou des risques élevés de corruption font l'objet d'une vigilance renforcée. De même, les opérations internationales impliquant plusieurs juridictions sont évaluées au regard des exigences réglementaires applicables dans chacun des pays concernés.

Les risques technologiques font également l'objet d'une attention particulière. AGCE International analyse les vulnérabilités susceptibles d'affecter ses systèmes d'information, ses plateformes numériques, ses outils de paiement électronique, ses services en ligne, ses bases de données et ses infrastructures informatiques. Cette évaluation prend en considération les risques de cyberattaque, de fraude numérique, d'usurpation d'identité, de falsification documentaire, de compromission des comptes utilisateurs, de manipulation des données ou de toute utilisation abusive des technologies pouvant favoriser des opérations financières illicites.

L'identification des risques repose sur la collecte et l'analyse d'informations provenant de sources internes et externes. L'Organisation exploite notamment les résultats des procédures de connaissance des parties prenantes (KYC), les rapports d'audit, les contrôles internes, les évaluations de conformité, les signalements internes, les rapports financiers, les analyses sectorielles, les informations communiquées par les partenaires institutionnels ainsi que les évolutions des normes nationales et internationales relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Cette démarche mobilise l'ensemble des acteurs de la gouvernance de l'Organisation. Le Président Général, le Collège Central, le Bureau Exécutif, le Responsable Conformité, le Responsable Financier, le Responsable Informatique, l'Auditeur interne, le Commissaire aux comptes, les responsables d'antennes, les collaborateurs, les membres et les bénévoles participent, chacun dans le cadre de leurs responsabilités, à l'identification et au signalement des risques susceptibles d'affecter l'Organisation. Cette approche collaborative favorise une meilleure circulation de l'information et une détection plus précoce des situations à risque.

Enfin, l'identification des risques constitue un processus dynamique et évolutif. Les risques recensés font l'objet d'un suivi régulier, d'une documentation appropriée et d'une réévaluation périodique afin de garantir que les mesures de prévention, de contrôle et de surveillance demeurent adaptées à l'évolution des activités d'AGCE International, aux nouvelles méthodes employées par les acteurs de la criminalité financière et aux exigences croissantes des autorités de régulation, des partenaires techniques et financiers ainsi que des bailleurs de fonds internationaux. Par cette démarche proactive, l'Organisation renforce durablement sa résilience, protège ses ressources et assure la réalisation de ses missions dans un environnement sécurisé, transparent et conforme aux meilleures pratiques.

internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

5.1.1 Pays

Le **risque lié aux pays** constitue un élément majeur de l'Approche Basée sur les Risques adoptée par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En raison de ses activités nationales et internationales, de ses partenariats transfrontaliers, de ses programmes de coopération, de ses collectes de fonds et de ses transferts financiers, l'Organisation évalue systématiquement le niveau de risque associé aux pays dans lesquels elle intervient ou avec lesquels elle entretient des relations institutionnelles, financières ou opérationnelles.

Cette évaluation prend notamment en considération le cadre juridique et réglementaire applicable, le niveau de conformité du pays aux normes internationales de lutte contre le blanchiment de capitaux et le financement du terrorisme, la qualité des mécanismes de supervision financière, le niveau de corruption, la stabilité politique et institutionnelle, les risques de criminalité organisée, l'existence de conflits armés, les sanctions internationales, les mesures restrictives applicables ainsi que tout autre facteur susceptible d'accroître les risques liés aux opérations de l'Organisation.

Les opérations impliquant des pays présentant un niveau de risque élevé ou faisant l'objet de mesures particulières de vigilance sont soumises à des diligences renforcées. AGCE International peut exiger des vérifications complémentaires, des justificatifs supplémentaires, des autorisations spécifiques ou des contrôles approfondis avant toute décision de partenariat, de financement, de transfert de fonds ou de mise en œuvre d'un projet. Cette approche permet de protéger l'Organisation contre les risques juridiques, financiers, opérationnels et réputationnels tout en garantissant la conformité de ses activités avec les exigences nationales et internationales.

5.1.2 Bénéficiaires

L'identification et l'évaluation des **bénéficiaires** constituent un élément essentiel du dispositif de prévention des risques de blanchiment de capitaux et de financement du terrorisme d'AGCE International. L'Organisation veille à connaître avec précision les personnes physiques ou morales qui bénéficient directement ou indirectement de ses programmes, financements, subventions, dons, aides humanitaires, prestations de services ou partenariats institutionnels afin de s'assurer que les ressources mobilisées sont utilisées exclusivement pour des finalités légitimes et conformes à ses missions.

Avant toute attribution de ressources ou mise en œuvre d'un projet, AGCE International procède à des vérifications proportionnées portant notamment sur l'identité du bénéficiaire, son statut juridique lorsqu'il s'agit d'une organisation, la nature de ses activités, sa réputation, son

éligibilité, la cohérence de sa demande, l'utilisation prévue des ressources ainsi que, lorsque cela est nécessaire, l'identification de son bénéficiaire effectif. Des contrôles complémentaires peuvent être réalisés lorsque le niveau de risque identifié le justifie.

L'Organisation assure également un suivi régulier de l'utilisation des financements, équipements, matériels ou services mis à disposition des bénéficiaires afin de vérifier leur affectation conforme aux objectifs des projets. Toute anomalie, incohérence, utilisation abusive ou suspicion d'activité illicite fait l'objet d'une analyse approfondie et peut entraîner la suspension, la révision ou la cessation de l'appui accordé, conformément aux procédures internes et aux obligations légales applicables. Cette vigilance permanente contribue à préserver l'intégrité des programmes d'AGCE International et à garantir que ses ressources servent exclusivement des objectifs humanitaires, sociaux et de développement durable.

5.1.3 Partenaires

Les **partenaires** représentent un facteur important d'exposition aux risques dans le cadre des activités de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Avant d'établir toute relation de coopération, de financement, de prestation ou de partenariat stratégique, l'Organisation réalise une évaluation préalable destinée à apprécier le niveau de risque associé à la personne physique ou morale concernée. Cette démarche permet de s'assurer que les objectifs, les activités, les valeurs et les pratiques du partenaire sont compatibles avec les principes de gouvernance, de transparence, d'intégrité et de conformité défendus par AGCE International.

L'évaluation des partenaires porte notamment sur leur identité, leur existence légale, leur structure de gouvernance, leur réputation, leur expérience, leur situation financière, leurs activités principales, leurs sources de financement ainsi que, lorsque cela est nécessaire, l'identification de leurs bénéficiaires effectifs. L'Organisation apprécie également leur niveau de conformité aux obligations relatives à la lutte contre le blanchiment de capitaux, au financement du terrorisme, à la lutte contre la corruption, à la protection des données et au respect des droits humains.

Les partenariats présentant un niveau de risque élevé font l'objet de mesures de vigilance renforcées pouvant inclure des vérifications complémentaires, des clauses contractuelles spécifiques, un suivi périodique des activités, des audits de conformité ou des contrôles documentaires supplémentaires. AGCE International se réserve le droit de suspendre, de refuser ou de mettre fin à toute relation de partenariat lorsque des éléments sérieux laissent apparaître un risque de non-conformité, de fraude, de blanchiment de capitaux, de financement du terrorisme ou toute autre activité incompatible avec ses valeurs institutionnelles ou les exigences légales applicables.

5.1.4 Donateurs

Les **donateurs** constituent une composante essentielle des mécanismes de financement d'AGCE International. Afin de préserver l'intégrité de ses ressources financières et de prévenir toute utilisation abusive de ses activités à des fins illicites, l'Organisation applique des mesures de vigilance adaptées lors de la réception des dons, qu'ils soient effectués par des personnes physiques, des entreprises, des fondations, des organisations internationales ou toute autre entité publique ou privée.

Les procédures d'évaluation des donateurs reposent sur une approche proportionnée au niveau de risque. Elles peuvent comprendre la vérification de l'identité du donateur, de la provenance des fonds, de la nature du financement, de la cohérence entre le montant du don et le profil du donateur, ainsi que toute autre diligence jugée nécessaire au regard des circonstances. Lorsque les dons proviennent de juridictions à risque, présentent un caractère inhabituel ou soulèvent des interrogations légitimes, AGCE International peut demander des justificatifs complémentaires avant d'accepter les fonds.

L'Organisation veille à ce que tous les dons soient enregistrés, documentés et retracés conformément à ses procédures financières et comptables. Les informations relatives aux donateurs sont conservées dans le respect des règles de confidentialité et de protection des données personnelles. Lorsqu'un don présente un risque inacceptable, une origine incertaine ou des indices susceptibles de révéler une opération de blanchiment de capitaux, de financement du terrorisme ou une autre activité illicite, AGCE International peut refuser le don, suspendre son traitement ou prendre toute mesure appropriée conformément à sa politique interne et aux obligations légales qui lui sont applicables. Cette vigilance contribue à garantir que les ressources financières de l'Organisation proviennent exclusivement de sources licites et soutiennent durablement ses missions humanitaires, sociales et de développement.

5.1.5 Projets

Les **projets** mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** font systématiquement l'objet d'une évaluation des risques avant leur approbation, leur financement et leur exécution. Cette analyse vise à garantir que chaque projet soit conforme aux objectifs institutionnels de l'Organisation ainsi qu'aux exigences applicables en matière de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. L'évaluation porte notamment sur la nature des activités, le contexte géographique, les partenaires impliqués, les bénéficiaires, les sources de financement, les modalités de mise en œuvre ainsi que les mécanismes de contrôle prévus.

Les projets présentant des caractéristiques particulières, tels que les opérations transfrontalières, les programmes financés par plusieurs bailleurs, les interventions en zones à risque, les activités reposant sur des paiements importants ou l'utilisation de plateformes

numériques, font l'objet de mesures de vigilance renforcées. AGCE International vérifie que les ressources financières sont exclusivement affectées aux objectifs autorisés, que les dépenses sont justifiées par des pièces probantes et que les procédures de validation, de suivi et de contrôle sont effectivement appliquées.

Tout au long du cycle de vie d'un projet, l'Organisation assure un suivi permanent des risques au moyen d'évaluations périodiques, de contrôles administratifs et financiers, d'audits internes, de rapports d'exécution et de mécanismes de traçabilité documentaire. En présence d'anomalies, de modifications substantielles ou d'indices susceptibles de révéler une utilisation irrégulière des ressources, des mesures correctives immédiates peuvent être mises en œuvre, pouvant aller jusqu'à la suspension ou à la révision du projet conformément aux procédures internes et aux obligations légales applicables.

5.1.6 Moyens de paiement

Les **moyens de paiement** utilisés par AGCE International constituent un facteur essentiel de maîtrise des risques liés au blanchiment de capitaux et au financement du terrorisme. L'Organisation privilégie des instruments de paiement sécurisés, traçables et conformes aux réglementations financières applicables afin de garantir la transparence de l'ensemble de ses opérations financières nationales et internationales.

Les paiements reçus ou effectués par l'Organisation au moyen de virements bancaires, cartes bancaires, plateformes de paiement électronique, solutions numériques, services de paiement mobile ou tout autre canal autorisé font l'objet de procédures de contrôle adaptées. Chaque opération doit pouvoir être identifiée, justifiée, enregistrée et rapprochée des documents comptables et administratifs correspondants. Les paiements en espèces ou utilisant des moyens difficilement traçables sont soumis à une vigilance renforcée et peuvent être limités ou refusés lorsqu'ils présentent un niveau de risque incompatible avec les politiques internes de l'Organisation.

AGCE International veille également à sélectionner des établissements bancaires et des prestataires de services de paiement reconnus, soumis à des obligations réglementaires en matière de lutte contre le blanchiment de capitaux et disposant de dispositifs appropriés de sécurité financière. Les accès aux plateformes de paiement sont protégés par des mécanismes d'authentification renforcée, des procédures de validation des opérations, une séparation des responsabilités et un contrôle permanent des transactions.

Toute opération financière inhabituelle, incohérente avec le profil de l'utilisateur, présentant un montant anormal, une fréquence inhabituelle ou des caractéristiques atypiques fait l'objet d'une analyse spécifique. Lorsque des éléments laissent présumer un risque de fraude, de blanchiment de capitaux, de financement du terrorisme ou d'utilisation abusive des moyens de paiement, l'Organisation peut suspendre l'opération, demander des justificatifs complémentaires ou appliquer toute mesure de vigilance prévue par la présente politique et par les dispositions légales applicables.

5.2 Classification des risques

Dans le cadre de son **Approche Basée sur les Risques (ABR)**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** applique une méthode de classification permettant d'évaluer le niveau d'exposition de chaque activité, relation d'affaires, opération financière, partenaire, donateur, bénéficiaire ou projet aux risques de **blanchiment de capitaux**, de **financement du terrorisme**, de **fraude** et de **criminalité financière**. Cette classification constitue un outil d'aide à la décision permettant d'adapter les mesures de vigilance, de contrôle, de validation et de surveillance selon le degré de risque identifié.

Chaque niveau de risque fait l'objet d'une analyse documentée reposant sur plusieurs critères, notamment la nature de l'activité, le profil des parties prenantes, le pays concerné, les moyens de paiement utilisés, les montants en jeu, la complexité de l'opération, la qualité des informations disponibles ainsi que les résultats des procédures de connaissance des parties prenantes (KYC). Cette classification est révisée périodiquement ou lorsqu'un changement significatif est constaté.

Tableau de classification des risques

Niveau de risque	Caractéristiques principales	Mesures de vigilance applicables
Faible	Les opérations présentent un niveau d'exposition limité. Les parties prenantes sont clairement identifiées, disposent d'une réputation satisfaisante, exercent des activités transparentes et évoluent dans un environnement réglementaire stable. Les transactions sont cohérentes avec le profil connu de l'utilisateur et ne révèlent aucun indice d'anomalie.	Application des procédures normales de connaissance des parties prenantes (KYC), vérification standard de l'identité, contrôle documentaire habituel, enregistrement comptable, conservation des pièces justificatives et suivi périodique selon les procédures internes.

Niveau de risque	Caractéristiques principales	Mesures de vigilance applicables
Moyen	Certaines caractéristiques nécessitent une vigilance accrue sans pour autant révéler d'indices sérieux d'activité illicite. Il peut s'agir d'opérations internationales ordinaires, de nouveaux partenaires, de projets présentant une complexité particulière ou d'opérations impliquant plusieurs intervenants nécessitant des vérifications complémentaires.	Mise en œuvre de diligences renforcées proportionnées, collecte de justificatifs supplémentaires, validation hiérarchique adaptée, contrôle renforcé des opérations financières, suivi plus fréquent de la relation et réévaluation périodique du niveau de risque.
Élevé	Les opérations concernent des secteurs sensibles, des juridictions présentant un niveau de risque important, des montants financiers significatifs, des structures juridiques complexes ou des situations dans lesquelles certaines informations demeurent incomplètes ou difficiles à vérifier. Le risque de blanchiment de capitaux ou de financement du terrorisme est considéré comme important sans qu'une infraction soit nécessairement établie.	Application de mesures de vigilance renforcées, vérification approfondie de l'identité et du bénéficiaire effectif, analyse de l'origine des fonds, approbation préalable par les responsables compétents, surveillance permanente des opérations, limitation éventuelle de certaines transactions et documentation détaillée des décisions prises.
Critique	Des indices sérieux, des incohérences majeures ou des éléments objectifs laissent présumer un risque élevé d'activité illicite, de fraude, de blanchiment de capitaux, de financement du terrorisme, de corruption ou de détournement de ressources. Les informations communiquées sont insuffisantes, contradictoires ou impossibles à vérifier, ou l'opération concerne des personnes, organisations ou juridictions faisant l'objet de restrictions ou de mesures particulières.	Refus, suspension ou interruption immédiate de la relation ou de l'opération, blocage de tout engagement financier, analyse approfondie par le Responsable Conformité, information des organes de gouvernance compétents, conservation intégrale des éléments de preuve, renforcement des contrôles internes et, lorsque la législation applicable l'impose ou l'autorise, coopération avec les autorités compétentes conformément aux procédures institutionnelles et aux obligations légales.

La présente classification constitue un référentiel évolutif. AGCE International veille à son actualisation régulière afin de tenir compte de l'évolution de ses activités, des nouvelles

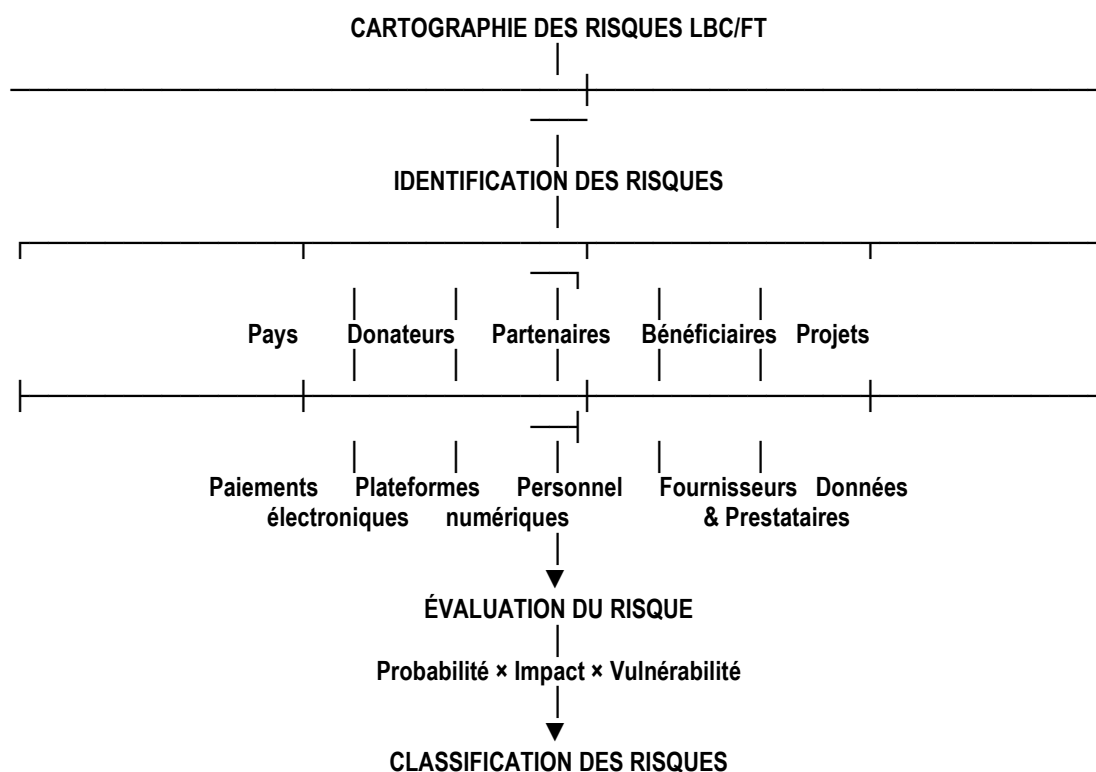
méthodes de criminalité financière, des recommandations des autorités compétentes, des résultats des audits et des meilleures pratiques internationales en matière de gouvernance, de conformité et de lutte contre le blanchiment de capitaux et le financement du terrorisme. Chaque décision prise sur la base de cette classification est documentée, justifiée et conservée afin d'assurer la transparence, la traçabilité et la redevabilité du dispositif institutionnel de gestion des risques.

5.3 Cartographie des risques

La **cartographie des risques** constitue l'un des principaux outils stratégiques de gouvernance de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** dans le cadre de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Elle permet d'identifier, d'analyser, de hiérarchiser, de surveiller et de maîtriser les risques susceptibles d'affecter les activités de l'Organisation, tout en facilitant la prise de décision par les organes de gouvernance.

Cette cartographie repose sur une approche dynamique fondée sur les risques et fait l'objet d'une actualisation régulière afin d'intégrer les évolutions des activités de l'Organisation, les nouvelles menaces, les recommandations des autorités compétentes, les résultats des audits ainsi que les meilleures pratiques internationales.

Schéma stratégique de la cartographie des risques LBC/FT



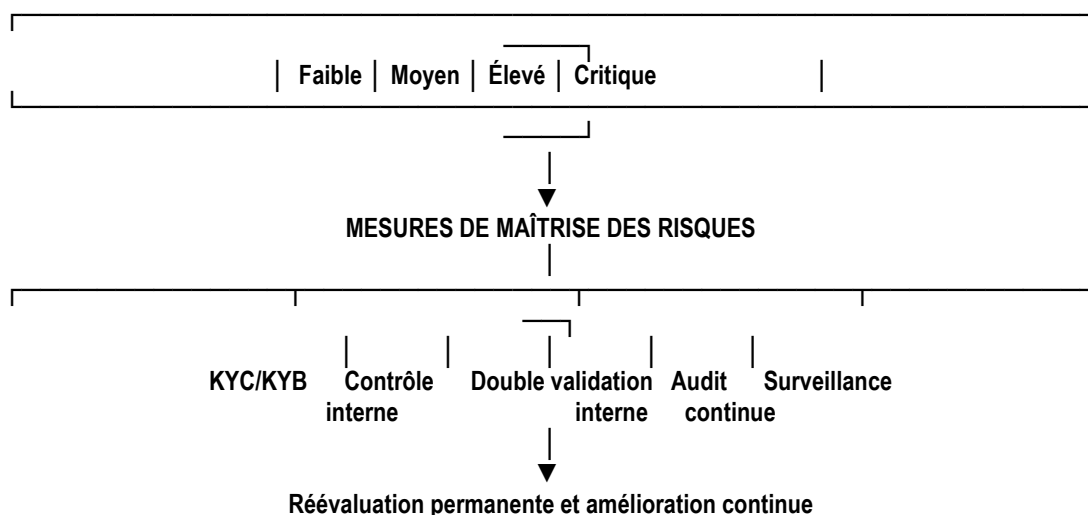


Tableau stratégique de cartographie des risques

Domaine exposé	Sources potentielles de risque	Niveau potentiel	Conséquences possibles	Mesures de maîtrise	Responsable
Pays d'intervention	Zones sous sanctions, conflits, corruption, faible réglementation	Moyen à Critique	Non-conformité réglementaire, réputation	Analyse géographique, veille réglementaire, validation renforcée	Responsable Conformité
Donateurs	Origine inconnue des fonds, dons atypiques	Moyen à Élevé	Blanchiment de capitaux	KYC, justification des fonds, contrôle documentaire	Responsable Financier
Partenaires	Gouvernance insuffisante, réputation négative	Moyen à Élevé	Risque juridique et réputationnel	Due diligence, analyse documentaire, clauses contractuelles	Président Général / Conformité
Bénéficiaires	Fausse identité, bénéficiaire effectif dissimulé	Faible à Élevé	Détournement des aides	Vérification d'identité, contrôle terrain, suivi des projets	Responsable Programme
Projets	Affectation irrégulière des ressources	Moyen à Critique	Perte financière, fraude	Suivi budgétaire, audit, contrôle permanent	Responsable Projet
Paiements	Transactions	Moyen à	Blanchiment de	Validation	Responsable Financier

Domaine exposé	Sources potentielles de risque	Niveau potentiel	Conséquences possibles	Mesures de maîtrise	Responsable
	inhabituelles ou complexes	Critique	capitaux	multiple, rapprochement bancaire	
Comptabilité	Faux justificatifs, erreurs comptables	Moyen	États financiers inexacts	Contrôle interne, audit, séparation des tâches	Responsable Financier
Informatique	Cyberattaque, fraude numérique, usurpation	Moyen à Critique	Vol de données, fraude financière	MFA, chiffrement, journalisation, sauvegardes	Responsable Informatique
Ressources humaines	Conflits d'intérêts, fraude interne	Faible à Élevé	Atteinte à la gouvernance	Déclarations d'intérêts, contrôle hiérarchique	RH / Conformité
Fournisseurs	Prestataire fictif ou à risque	Moyen	Paielements frauduleux	Vérification préalable, contrats, contrôles	Responsable Achats
Collecte de dons	Collectes non autorisées	Moyen à Critique	Détournement de fonds	Autorisation préalable, contrôle des campagnes	Responsable Collecte
Plateformes numériques	Utilisation frauduleuse des comptes	Moyen à Critique	Cybercriminalité	Authentification forte, surveillance des connexions	Responsable Informatique

Méthodologie technique d'évaluation des risques

Chaque risque identifié est évalué selon une méthode multicritère reposant sur cinq paramètres :

Critère	Description
Probabilité	Fréquence estimée de survenance du risque.
Impact	Conséquences financières, juridiques, opérationnelles et réputationnelles.

Critère	Description
Vulnérabilité	Niveau de faiblesse des dispositifs existants.
Capacité de détection	Aptitude des contrôles internes à identifier rapidement le risque.
Capacité de réponse	Aptitude de l'Organisation à limiter les conséquences du risque.

Le niveau global de risque est déterminé après analyse combinée de ces critères afin de définir les mesures de contrôle appropriées.

Matrice stratégique de criticité

Probabilité / Impact	Faible	Modéré	Important	Majeur
Très faible	Faible	Faible	Moyen	Moyen
Faible	Faible	Moyen	Moyen	Élevé
Moyenne	Moyen	Moyen	Élevé	Critique
Élevée	Moyen	Élevé	Critique	Critique
Très élevée	Élevé	Critique	Critique	Critique

Cycle institutionnel de gestion des risques

La cartographie des risques s'inscrit dans un cycle continu de gouvernance comprenant les étapes suivantes :

1. **Identification** des risques potentiels.
2. **Analyse** des causes et des facteurs de vulnérabilité.
3. **Évaluation** de la probabilité et de l'impact.
4. **Classification** selon le niveau de criticité.
5. **Définition** des mesures de prévention et de contrôle.
6. **Validation** par les organes de gouvernance compétents.
7. **Mise en œuvre** des actions correctives et préventives.
8. **Surveillance continue** au moyen d'indicateurs de conformité.
9. **Audit et réévaluation** périodiques.
10. **Actualisation** de la cartographie en fonction des nouveaux risques, des évolutions réglementaires et des enseignements tirés des contrôles.

Cette cartographie constitue un référentiel opérationnel permettant à **AGCE International – AGCE Canada** de disposer d'une vision globale, hiérarchisée et évolutive de ses risques

LBC/FT, tout en facilitant les décisions stratégiques, le contrôle interne, les audits, la conformité réglementaire et la protection durable de ses ressources, de sa réputation et de ses missions humanitaires.

CHAPITRE 6

KYC – CONNAISSANCE DES MEMBRES ET PARTENAIRES

La Connaissance des Membres et Partenaires (Know Your Customer – KYC) constitue un pilier fondamental du dispositif de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif de permettre à l'Organisation d'identifier, de vérifier et de comprendre l'identité, le profil, les activités, les relations et le niveau de risque des personnes physiques et morales avec lesquelles elle établit une relation institutionnelle, financière ou opérationnelle.

Le dispositif KYC vise à prévenir l'utilisation de l'Organisation à des fins de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, d'usurpation d'identité ou de toute autre activité illicite. Il contribue à renforcer la transparence, la traçabilité des opérations, la sécurité des partenariats et la protection de l'intégrité institutionnelle d'AGCE International.

Les procédures KYC s'appliquent notamment aux membres, bénévoles, donateurs, partenaires nationaux et internationaux, bénéficiaires, fournisseurs, prestataires, consultants, bailleurs de fonds, représentants d'antennes ainsi qu'à toute personne physique ou morale souhaitant établir une relation durable avec l'Organisation. Le niveau de vigilance appliqué est déterminé selon une **Approche Basée sur les Risques**, tenant compte de la nature de la relation, du pays concerné, des activités exercées, des montants financiers en jeu, des moyens de paiement utilisés et de tout autre facteur susceptible d'accroître le niveau de risque.

Dans le cadre du dispositif KYC, AGCE International met en œuvre des procédures d'identification, de vérification documentaire, de connaissance des bénéficiaires effectifs lorsque cela est nécessaire, d'évaluation de l'origine des fonds, de suivi des relations institutionnelles et de réévaluation périodique des informations recueillies. Les données sont traitées dans le respect des principes de confidentialité, de protection des données personnelles, de sécurité des systèmes d'information et des exigences légales applicables.

Le dispositif KYC fait l'objet d'une amélioration continue afin de tenir compte de l'évolution des risques, des nouvelles méthodes de criminalité financière, des innovations technologiques, des recommandations des autorités compétentes et des meilleures pratiques internationales. Il constitue un instrument essentiel de gouvernance permettant à AGCE International de sélectionner des partenaires fiables, de sécuriser ses opérations et de garantir que l'ensemble de ses ressources soient exclusivement mobilisées au service de ses missions humanitaires, sociales, éducatives, sanitaires, économiques et numériques.

Tableau des principaux objectifs du dispositif KYC

Objectif	Finalité
Identification	Vérifier avec certitude l'identité des membres et partenaires.
Vérification documentaire	Contrôler l'authenticité des documents et informations fournis.
Évaluation des risques	Déterminer le niveau de risque associé à chaque relation.
Connaissance du bénéficiaire effectif	Identifier les personnes exerçant un contrôle réel sur une organisation lorsque cela est requis.
Surveillance continue	Actualiser les informations et détecter toute évolution du niveau de risque.
Conformité réglementaire	Respecter les obligations nationales et internationales en matière de LBC/FT.
Protection institutionnelle	Prévenir les risques financiers, juridiques, opérationnels et réputationnels.

Ce chapitre constitue le fondement des procédures détaillées qui seront développées dans les sections suivantes relatives à l'identification, à la vérification, à la vigilance renforcée, au suivi continu et à la conservation des informations KYC.

6.1 Vérification d'identité

La **vérification d'identité** constitue une étape obligatoire du dispositif **Know Your Customer (KYC)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle vise à confirmer avec un niveau raisonnable de certitude l'identité de toute personne physique ou morale souhaitant établir une relation avec l'Organisation, afin de prévenir les risques de fraude, d'usurpation d'identité, de blanchiment de capitaux, de financement du terrorisme et de toute autre activité illicite.

Avant toute adhésion, partenariat, prestation, financement, don ou participation à un projet, AGCE International recueille les informations d'identification nécessaires et procède à leur vérification au moyen de documents officiels, fiables, valides et, lorsque cela est requis, de sources indépendantes. Les informations collectées doivent être cohérentes, exactes, complètes et régulièrement mises à jour tout au long de la relation.

Tableau des éléments de vérification

Élément vérifié	Exigences principales
Personne physique	Nom, prénoms, date de naissance, nationalité, adresse, pièce d'identité officielle valide et coordonnées.
Personne morale	Dénomination, existence légale, numéro d'enregistrement, siège social, représentants habilités et bénéficiaires effectifs, lorsque requis.
Documents justificatifs	Pièces officielles lisibles, authentiques, en cours de validité et conformes aux exigences réglementaires.
Validation	Contrôle documentaire, vérification de cohérence, analyse des risques et approbation avant l'établissement de la relation.

Lorsque des incohérences, des documents falsifiés, des informations incomplètes ou des doutes raisonnables sont constatés, AGCE International suspend ou refuse la relation jusqu'à l'obtention d'éléments satisfaisants. Toutes les vérifications sont documentées, sécurisées et conservées conformément aux exigences légales, aux politiques internes de protection des données et aux règles de conformité LBC/FT.

6.2 Vérification documentaire

La **vérification documentaire** constitue une composante essentielle du dispositif **Know Your Customer (KYC)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle consiste à examiner l'authenticité, la validité, l'intégrité et la cohérence des documents fournis par les membres, partenaires, donateurs, fournisseurs, bénéficiaires et toute autre partie prenante avant l'établissement ou le maintien d'une relation institutionnelle. Cette procédure vise à prévenir les risques de fraude documentaire, d'usurpation d'identité, de blanchiment de capitaux et de financement du terrorisme.

Les documents transmis doivent être officiels, complets, lisibles, en cours de validité et compatibles avec les informations déclarées. Lorsque cela est nécessaire, AGCE International peut solliciter des pièces complémentaires ou effectuer des vérifications auprès de sources fiables et indépendantes afin de confirmer leur authenticité.

Tableau des contrôles documentaires

Document ou information	Contrôles effectués
Pièces d'identité	Vérification de la validité, de l'authenticité, de la lisibilité et de la cohérence des informations.
Documents juridiques	Contrôle de l'existence légale, des autorisations, des statuts et des pouvoirs des représentants habilités.
Justificatifs d'adresse	Vérification de l'exactitude et de l'actualité des coordonnées déclarées.
Documents financiers	Examen de la cohérence des justificatifs relatifs aux fonds, paiements ou financements lorsque requis.
Validation finale	Approbation de la conformité documentaire avant toute décision d'adhésion, de partenariat ou d'opération financière.

En cas de document falsifié, expiré, incomplet, incohérent ou ne permettant pas une identification fiable, AGCE International suspend le traitement du dossier jusqu'à régularisation ou refuse l'établissement de la relation conformément à ses procédures internes et aux exigences de conformité LBC/FT. Toutes les vérifications sont documentées, sécurisées et conservées selon les délais prévus par la réglementation applicable.

6.3 Vérification des organisations

La **vérification des organisations** constitue une étape essentielle du dispositif **Know Your Customer (KYC)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif de confirmer l'existence juridique, la légitimité, la gouvernance, la capacité opérationnelle et la conformité des associations, entreprises, fondations, institutions publiques, organisations non gouvernementales et autres entités souhaitant établir une relation de partenariat, de financement, de prestation ou de coopération avec l'Organisation. Cette démarche contribue à prévenir les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption et de conflits d'intérêts.

Avant toute collaboration, AGCE International procède à une analyse documentaire et institutionnelle afin de vérifier l'identité de l'organisation, son statut juridique, son immatriculation, ses représentants habilités, ses bénéficiaires effectifs lorsque cela est requis, ainsi que sa réputation et sa conformité aux réglementations applicables. L'Organisation peut également apprécier la cohérence entre les activités déclarées, les ressources mobilisées, les objectifs poursuivis et la nature du partenariat envisagé.

Tableau des contrôles applicables

Élément vérifié	Contrôles réalisés
Existence juridique	Vérification des statuts, de l'immatriculation, de l'agrément ou de tout document officiel attestant de l'existence légale.
Gouvernance	Identification des dirigeants, représentants autorisés et, lorsque requis, des bénéficiaires effectifs.
Activités	Vérification de la cohérence entre les missions déclarées, les activités exercées et le partenariat proposé.
Réputation et conformité	Analyse des informations disponibles, des antécédents connus, des éventuelles sanctions et du respect des exigences réglementaires.
Validation institutionnelle	Approbation de la relation après évaluation du niveau de risque et validation par les responsables compétents.

Lorsqu'une organisation ne fournit pas les justificatifs requis, présente des informations incohérentes, fait l'objet de restrictions légales ou soulève un doute raisonnable quant à sa légitimité ou à la provenance de ses ressources, AGCE International peut suspendre l'instruction du dossier, demander des vérifications complémentaires ou refuser l'établissement de la relation conformément à sa politique de conformité **LBC/FT**. Toutes les vérifications sont documentées, conservées et réévaluées périodiquement pendant toute la durée de la relation institutionnelle.

6.4 Bénéficiaires effectifs

L'identification des **bénéficiaires effectifs** constitue une mesure essentielle du dispositif **Know Your Customer (KYC)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif de déterminer la ou les personnes physiques qui possèdent, contrôlent ou exercent, directement ou indirectement, un pouvoir de décision ou un contrôle effectif sur une organisation, une entreprise, une fondation, une association ou toute autre personne morale entretenant une relation avec l'Organisation. Cette démarche permet de garantir la transparence des structures juridiques et de prévenir les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption et de dissimulation d'identité.

Avant l'établissement ou le maintien d'une relation institutionnelle, AGCE International recueille les informations nécessaires afin d'identifier les bénéficiaires effectifs et de comprendre la structure de propriété ou de contrôle de l'entité concernée. Lorsque la structure juridique est complexe ou présente un niveau de risque élevé, des diligences renforcées peuvent être mises en œuvre afin d'obtenir des justificatifs complémentaires et de confirmer les informations déclarées.

Tableau des contrôles relatifs aux bénéficiaires effectifs

Élément vérifié	Mesures de contrôle
Identification	Recueil de l'identité complète des personnes exerçant un contrôle effectif sur l'organisation.
Structure de propriété	Analyse de l'actionnariat, de la gouvernance ou des mécanismes de contrôle direct ou indirect.
Pouvoir de décision	Vérification des personnes disposant d'un pouvoir de gestion, de représentation ou de décision stratégique.
Documents justificatifs	Contrôle des statuts, registres officiels, actes constitutifs et tout document permettant de confirmer le bénéficiaire effectif.
Réévaluation	Mise à jour des informations lors de toute modification de la gouvernance, de la propriété ou du niveau de risque.

Lorsque l'identité du bénéficiaire effectif ne peut être raisonnablement établie, que les informations fournies sont incomplètes, incohérentes ou manifestement inexactes, ou que des indices sérieux de dissimulation sont constatés, AGCE International suspend l'instruction du dossier, sollicite des informations complémentaires ou refuse d'établir ou de poursuivre la relation conformément à sa politique de conformité **LBC/FT** et aux exigences réglementaires applicables. Toutes les informations recueillies sont conservées de manière sécurisée, confidentielle et traçable pendant la durée prévue par la législation en vigueur.

6.5 Vérification des dirigeants

La **vérification des dirigeants** constitue une étape essentielle du dispositif **Know Your Customer (KYC)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle vise à confirmer l'identité, les pouvoirs, la légitimité et l'intégrité des personnes exerçant des fonctions de direction, d'administration, de représentation ou de gestion au sein des organisations souhaitant établir une relation avec l'Organisation. Cette procédure permet de réduire les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de conflits d'intérêts et de détournement des ressources.

Avant toute collaboration, AGCE International vérifie que les dirigeants disposent des autorisations nécessaires pour engager légalement leur organisation. L'Organisation procède également à l'examen des documents attestant de leur nomination, de leurs pouvoirs de représentation et, lorsque cela est requis, de leur réputation, de leur honorabilité ainsi que de leur conformité aux exigences réglementaires applicables. Une vigilance renforcée est appliquée lorsque les dirigeants exercent des fonctions exposées, représentent des structures complexes ou présentent un niveau de risque élevé.

Tableau des contrôles applicables aux dirigeants

Élément vérifié	Mesures de contrôle
Identité des dirigeants	Vérification de l'identité complète au moyen de documents officiels en cours de validité.
Pouvoirs de représentation	Contrôle des actes de nomination, mandats, procurations ou délégations de signature autorisant le dirigeant à engager l'organisation.
Fonction et responsabilités	Vérification de la qualité, du poste occupé et de l'étendue des responsabilités exercées au sein de l'organisation.
Réputation et conformité	Analyse des informations disponibles relatives à l'intégrité, aux éventuelles sanctions, condamnations, interdictions d'exercer ou mesures réglementaires applicables.
Validation et suivi	Approbation de la relation après évaluation du niveau de risque et mise à jour des informations en cas de changement de dirigeant ou de gouvernance.

Lorsque des incohérences, des documents insuffisants, des pouvoirs non établis ou des éléments susceptibles de compromettre la conformité de la relation sont constatés, AGCE International peut suspendre l'instruction du dossier, demander des justificatifs complémentaires ou refuser l'établissement ou le maintien de la relation. Toutes les vérifications sont documentées, conservées de manière sécurisée et réévaluées périodiquement conformément à la présente politique **LBC/FT**, aux procédures internes de conformité et aux exigences légales applicables.

6.6 Personnes Politiquement Exposées (PPE)

Les **Personnes Politiquement Exposées (PPE)** font l'objet d'une vigilance particulière dans le cadre du dispositif **Know Your Customer (KYC)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Une PPE est une personne physique qui exerce ou a exercé une fonction publique importante, ainsi que, lorsque la réglementation applicable l'exige, les membres de sa famille proche et les personnes connues pour lui être étroitement associées. En raison de leurs responsabilités et de leur niveau d'influence, ces personnes peuvent présenter un risque accru de corruption, de blanchiment de capitaux, de financement du terrorisme ou d'autres infractions financières. Leur qualité de PPE ne constitue toutefois pas, à elle seule, un motif de refus de relation.

Avant d'établir ou de poursuivre une relation avec une PPE, AGCE International procède à une évaluation approfondie des risques afin de s'assurer de la légitimité de la relation envisagée, de l'origine licite des fonds mobilisés, de la transparence des opérations et de la conformité aux exigences légales et réglementaires applicables. Les relations impliquant

une PPE sont soumises à une autorisation préalable des responsables compétents et à un suivi renforcé pendant toute leur durée.

Tableau des mesures de vigilance applicables aux PPE

Élément vérifié	Mesures de contrôle
Identification du statut PPE	Vérification de l'exercice actuel ou passé d'une fonction publique importante et, lorsque requis, des personnes étroitement liées.
Évaluation des risques	Analyse de la nature de la relation, du pays concerné, des activités exercées et du niveau de risque associé.
Origine des fonds	Vérification de la provenance licite des ressources financières et des justificatifs disponibles.
Validation institutionnelle	Autorisation préalable par les responsables compétents avant l'établissement de la relation.
Surveillance continue	Réévaluation périodique du statut, contrôle renforcé des opérations et actualisation des informations KYC.

Lorsqu'une PPE présente un niveau de risque élevé, que l'origine des fonds ne peut être raisonnablement démontrée ou que des opérations inhabituelles sont constatées, AGCE International met en œuvre des mesures de vigilance renforcées pouvant inclure des contrôles complémentaires, une limitation de certaines opérations, la suspension de la relation ou toute autre mesure appropriée conformément à sa politique **LBC/FT** et aux obligations légales applicables. Toutes les décisions sont documentées afin d'assurer la traçabilité, la transparence et la conformité du dispositif de gestion des risques.

6.7 Sanctions internationales

Le respect des **sanctions internationales** constitue une exigence essentielle du dispositif de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. L'Organisation s'engage à exercer ses activités dans le strict respect des mesures restrictives adoptées par les autorités nationales compétentes ainsi que par les organisations internationales auxquelles les juridictions concernées sont liées. Cette démarche vise à prévenir tout risque de financement d'activités illicites, de contournement des embargos, de soutien à des organisations criminelles ou terroristes et de violation des obligations légales applicables.

Avant d'établir une relation avec un membre, un partenaire, un donateur, un fournisseur, un prestataire, un bénéficiaire ou toute autre partie prenante, AGCE International procède, selon une approche fondée sur les risques, à des vérifications destinées à s'assurer que les personnes physiques, les personnes morales, les bénéficiaires effectifs et, lorsque cela

est pertinent, les pays concernés ne font pas l'objet de sanctions, de restrictions ou de mesures d'interdiction applicables. Ces vérifications sont renouvelées périodiquement pendant toute la durée de la relation afin de tenir compte des évolutions réglementaires et géopolitiques.

Tableau des contrôles relatifs aux sanctions internationales

Élément contrôlé	Mesures de conformité appliquées
Personnes physiques	Vérification de l'identité afin de détecter une éventuelle inscription sur une liste de sanctions applicable.
Personnes morales	Contrôle de l'organisation, de ses dirigeants et, lorsque requis, de ses bénéficiaires effectifs.
Pays et territoires	Évaluation des risques liés aux juridictions soumises à des sanctions, embargos ou restrictions internationales.
Transactions financières	Contrôle préalable des opérations nationales et internationales afin de prévenir tout transfert interdit ou à risque.
Suivi continu	Réactualisation des vérifications en cas de modification des listes de sanctions, de changement de situation ou d'évolution du niveau de risque.

Lorsqu'une correspondance potentielle est identifiée ou qu'un doute raisonnable subsiste quant à l'application d'une mesure restrictive, AGCE International suspend l'opération ou la relation concernée jusqu'à l'achèvement des vérifications nécessaires. Si la relation est incompatible avec les sanctions applicables ou présente un risque inacceptable, l'Organisation peut refuser l'adhésion, le partenariat, le financement ou toute autre opération, conformément aux dispositions légales en vigueur.

Toutes les vérifications réalisées dans le cadre du contrôle des sanctions internationales sont documentées, conservées de manière sécurisée et intégrées au dispositif global de gestion des risques. Elles participent au renforcement de la conformité institutionnelle, à la protection de la réputation de l'Organisation et à la garantie que l'ensemble de ses ressources humaines, matérielles, techniques et financières demeure exclusivement consacré à ses missions humanitaires, sociales, éducatives, sanitaires, économiques et numériques, dans le respect des normes nationales et internationales de gouvernance et de conformité.

CHAPITRE 7

ACCEPTATION DES DONS ET FINANCEMENTS

L'acceptation des dons et financements constitue une composante essentielle de la stratégie de mobilisation des ressources de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En tant qu'organisation à but non lucratif engagée dans des missions humanitaires, sociales, éducatives, sanitaires, environnementales et de développement économique et numérique, AGCE International veille à ce que l'ensemble des ressources financières, matérielles, techniques ou en nature qui lui sont confiées proviennent exclusivement de sources licites, transparentes et compatibles avec ses valeurs institutionnelles. Ce chapitre définit les principes et les exigences applicables à l'acceptation de tout don, financement, subvention, mécénat, parrainage, cotisation, contribution volontaire ou appui financier accordé à l'Organisation.

L'Organisation applique une approche fondée sur les risques afin d'évaluer chaque financement avant son acceptation. Cette évaluation prend en considération l'identité du donateur ou du bailleur de fonds, la provenance des ressources, la finalité du financement, les modalités de versement, les conditions éventuellement attachées à la contribution ainsi que les risques juridiques, financiers, opérationnels, éthiques et réputationnels susceptibles d'en résulter. Les procédures mises en œuvre s'inscrivent dans le cadre de la politique de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, des exigences de connaissance des parties prenantes (KYC), des règles de gouvernance interne et des dispositions légales applicables dans les juridictions où l'Organisation exerce ses activités.

AGCE International n'accepte aucun financement susceptible de compromettre son indépendance institutionnelle, son intégrité, sa neutralité, sa mission d'intérêt général ou le respect des lois nationales et internationales. Les contributions dont l'origine est incertaine, insuffisamment documentée, incompatible avec les objectifs de l'Organisation ou pouvant raisonnablement être associée à des activités illicites, à la corruption, au blanchiment de capitaux, au financement du terrorisme, à la fraude, au trafic illicite ou à toute autre infraction financière peuvent être refusées, suspendues ou soumises à des diligences renforcées.

Chaque don ou financement accepté fait l'objet d'une traçabilité complète, depuis son engagement jusqu'à son utilisation finale. Les opérations sont enregistrées conformément aux procédures comptables et financières de l'Organisation, accompagnées des pièces justificatives nécessaires et soumises aux mécanismes de contrôle interne, de supervision, d'audit et de redevabilité. Cette démarche garantit une gestion rigoureuse des ressources confiées à AGCE International, renforce la confiance des donateurs, des partenaires, des autorités compétentes et des bailleurs de fonds, tout en assurant une utilisation responsable, transparente et conforme des ressources au service des populations bénéficiaires.

Le présent chapitre constitue ainsi le cadre de référence applicable à toutes les décisions relatives à l'acceptation, au contrôle, au suivi et à la gestion des dons et financements reçus par AGCE International – AGCE Canada, dans le respect des principes de bonne gouvernance, de transparence, d'intégrité, de conformité réglementaire et de responsabilité institutionnelle.

7.1 Conditions d'acceptation

L'acceptation des dons et financements par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** est encadrée par des principes stricts de légalité, de transparence, d'intégrité et de conformité. Toute contribution financière, matérielle, technique ou en nature est soumise à une évaluation préalable destinée à garantir que son origine, son objet et ses modalités d'utilisation sont compatibles avec les missions de l'Organisation ainsi qu'avec les exigences applicables en matière de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Cette procédure permet de protéger l'Organisation contre les risques juridiques, financiers, opérationnels et réputationnels tout en préservant son indépendance institutionnelle.

Avant toute acceptation, AGCE International procède à une analyse du donateur ou du bailleur de fonds, de l'origine des ressources, de la finalité du financement, du montant proposé, des modalités de versement et, lorsque cela est nécessaire, des conditions particulières attachées à la contribution. Cette évaluation est réalisée selon une approche fondée sur les risques et s'appuie sur les procédures de connaissance des parties prenantes (KYC), les contrôles documentaires, les mécanismes de vigilance renforcée et les politiques internes de conformité. Les financements provenant de sources anonymes, insuffisamment identifiées, incompatibles avec les valeurs de l'Organisation ou susceptibles d'être liés à des activités illicites font l'objet d'un examen approfondi pouvant conduire à leur refus.

AGCE International n'accepte aucun don ou financement susceptible d'influencer indûment ses décisions, de compromettre son impartialité, d'imposer des conditions contraires à ses statuts, à sa mission d'intérêt général ou aux lois applicables. Les contributions assorties d'exigences incompatibles avec les principes de gouvernance, de transparence, de respect des droits humains, de lutte contre la corruption ou de conformité réglementaire sont rejetées. De même, l'Organisation se réserve le droit de refuser toute ressource dont la provenance ne peut être raisonnablement démontrée ou dont l'utilisation pourrait porter atteinte à sa réputation ou à la confiance de ses partenaires et bénéficiaires.

Toute décision d'acceptation est prise par les autorités compétentes conformément aux procédures internes de gouvernance et fait l'objet d'une documentation complète garantissant la traçabilité des vérifications effectuées. Les dons et financements acceptés sont enregistrés dans les systèmes administratifs, comptables et financiers de l'Organisation, accompagnés des pièces justificatives nécessaires et soumis aux dispositifs permanents de contrôle interne, d'audit et de suivi. Cette rigueur permet à AGCE International d'assurer une gestion responsable des ressources qui lui sont confiées et de garantir qu'elles seront

exclusivement affectées à la réalisation de ses missions humanitaires, sociales, éducatives, sanitaires, environnementales, économiques et numériques, dans le respect des normes nationales et internationales de bonne gouvernance et de conformité.

7.2 Origine des fonds

La vérification de **l'origine des fonds** constitue une exigence fondamentale du dispositif de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Avant l'acceptation de tout don, financement, subvention, mécénat, cotisation ou contribution financière, l'Organisation s'assure, dans une mesure raisonnable et proportionnée au niveau de risque, que les ressources proviennent d'activités licites, transparentes et conformes aux législations nationales et internationales applicables. Cette démarche vise à préserver l'intégrité institutionnelle de l'Organisation, à protéger sa réputation et à empêcher toute utilisation de ses activités à des fins de blanchiment de capitaux, de financement du terrorisme, de corruption, de fraude ou de criminalité financière.

L'évaluation de l'origine des fonds repose sur une approche fondée sur les risques. Elle prend en considération l'identité du donateur ou du bailleur, la nature de son activité, la provenance géographique des ressources, le mode de paiement utilisé, la cohérence entre le montant versé et le profil financier du contributeur, ainsi que les documents justificatifs disponibles. Lorsque les circonstances l'exigent, AGCE International peut demander des informations complémentaires, des justificatifs financiers ou tout document permettant d'établir la licéité des ressources avant de procéder à leur acceptation.

Les fonds présentant des caractéristiques inhabituelles, provenant de juridictions à risque élevé, transitant par des circuits financiers complexes ou faisant apparaître des incohérences significatives sont soumis à des mesures de vigilance renforcées. L'Organisation se réserve le droit de suspendre l'analyse du dossier, de différer l'acceptation des ressources ou de refuser tout financement dont l'origine ne peut être raisonnablement démontrée ou qui présente un risque incompatible avec sa politique de conformité.

Toutes les vérifications relatives à l'origine des fonds sont documentées, conservées de manière sécurisée et intégrées au dispositif de contrôle interne. Les décisions prises sont fondées sur les procédures institutionnelles de gouvernance, de conformité et de gestion des risques, garantissant une utilisation transparente, responsable et exclusivement affectée à la réalisation des missions humanitaires, sociales, éducatives, sanitaires, environnementales, économiques et numériques d'AGCE International.

7.3 Subventions

Les **subventions** constituent une source essentielle de financement des programmes et projets de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elles peuvent être accordées par des administrations publiques, des organisations internationales, des agences de coopération, des collectivités territoriales, des fondations, des institutions financières de développement ou d'autres organismes légalement habilités à soutenir des initiatives d'intérêt général. L'acceptation de ces ressources est soumise à une évaluation préalable visant à garantir leur conformité avec les objectifs statutaires de l'Organisation ainsi qu'avec les exigences applicables en matière de gouvernance, de transparence et de **LBC/FT**.

Avant toute acceptation, AGCE International examine les conditions d'octroi de la subvention, l'identité de l'organisme financeur, la légalité de la source de financement, l'objet de la contribution, les obligations contractuelles, les exigences de suivi, les modalités de justification des dépenses ainsi que les mécanismes de contrôle prévus. L'Organisation veille à ce que les conditions imposées soient compatibles avec son indépendance institutionnelle, ses valeurs, ses statuts et les lois applicables.

Les subventions acceptées sont exclusivement affectées aux finalités prévues dans les conventions ou accords de financement. Leur gestion est assurée conformément aux règles de bonne gouvernance financière, de séparation des responsabilités, de contrôle interne, de traçabilité comptable et de reddition des comptes. Chaque dépense doit être justifiée par des pièces probantes et pouvoir être retracée tout au long du cycle de vie du projet financé.

AGCE International met en œuvre un suivi permanent de l'exécution des subventions au moyen de rapports techniques et financiers, d'indicateurs de performance, de contrôles internes et, le cas échéant, d'audits internes ou externes. Toute anomalie, utilisation non conforme des fonds ou non-respect des engagements contractuels donne lieu à des mesures correctives appropriées conformément aux procédures internes et aux obligations légales. Cette approche garantit une gestion rigoureuse des subventions, renforce la confiance des bailleurs de fonds et assure que les ressources reçues contribuent efficacement à la réalisation des missions d'intérêt général portées par l'Organisation.

7.4 Financements internationaux

Les **financements internationaux** constituent un levier stratégique permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de développer ses programmes humanitaires, sociaux, éducatifs, sanitaires, environnementaux, économiques et numériques dans le respect des principes de bonne gouvernance et de conformité. Ces financements peuvent provenir d'organisations internationales, d'institutions multilatérales, d'agences de coopération, de gouvernements étrangers, de fondations internationales, de partenaires techniques et financiers ou de tout autre organisme légalement habilité à soutenir des initiatives d'intérêt général.

Avant toute acceptation, AGCE International réalise une analyse approfondie de la conformité du financement afin d'évaluer l'identité du bailleur, la légitimité de la source des fonds, les objectifs poursuivis, les obligations contractuelles, les modalités de décaissement, les exigences de suivi ainsi que les risques juridiques, financiers, opérationnels et réputationnels pouvant découler de la relation. Cette analyse s'inscrit dans le cadre des procédures de **Know Your Customer (KYC)**, de la politique de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, des contrôles internes et des règles de gouvernance institutionnelle.

L'Organisation veille à ce que tout financement international respecte les législations nationales des pays concernés, les obligations de conformité applicables, les réglementations relatives aux transferts internationaux de fonds, les exigences fiscales, les sanctions internationales en vigueur ainsi que les principes d'intégrité, de transparence et de redevabilité. Les conventions de financement définissent clairement les responsabilités des parties, les objectifs du projet, les modalités d'utilisation des ressources, les obligations de reporting, les mécanismes d'audit et les procédures de contrôle.

Les fonds reçus sont exclusivement affectés aux activités prévues dans les accords de financement et font l'objet d'un suivi permanent au moyen d'une comptabilité distincte, de rapports techniques et financiers, de contrôles internes, d'audits périodiques et d'une traçabilité complète des opérations. Toute anomalie, incohérence ou utilisation non conforme des ressources donne lieu à des mesures correctives immédiates, conformément aux procédures internes de l'Organisation et aux obligations contractuelles et réglementaires applicables.

7.5 Donateurs

Les **donateurs** occupent une place essentielle dans le financement des missions d'intérêt général de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Qu'il s'agisse de personnes physiques, d'entreprises, de fondations, d'associations, d'institutions publiques ou privées, ou d'organisations internationales, chaque contribution est accueillie avec reconnaissance tout en étant soumise à

un processus rigoureux d'évaluation et de conformité destiné à préserver l'intégrité de l'Organisation.

Avant l'acceptation d'un don, AGCE International applique des mesures de vigilance adaptées au niveau de risque afin de vérifier l'identité du donateur, la licéité de l'origine des fonds, la cohérence entre le profil du donateur et le montant de la contribution, ainsi que la conformité de l'opération avec les exigences de la politique **LBC/FT** et du dispositif **KYC**. Lorsque les circonstances le justifient, l'Organisation peut demander des justificatifs complémentaires relatifs à l'origine des ressources, à la nature de l'activité exercée ou à la finalité de la contribution.

Les dons sont acceptés uniquement lorsqu'ils sont compatibles avec les valeurs, les missions et les principes d'indépendance, de neutralité et de transparence d'AGCE International. L'Organisation refuse toute contribution susceptible de créer un conflit d'intérêts, d'exercer une influence indue sur sa gouvernance, d'imposer des conditions incompatibles avec ses objectifs statutaires ou de présenter un risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption ou de toute autre activité illicite.

Chaque don accepté fait l'objet d'un enregistrement complet dans les systèmes administratifs, comptables et financiers de l'Organisation. Les opérations sont documentées, justifiées et conservées conformément aux exigences légales et aux procédures internes de contrôle. AGCE International assure un suivi permanent de l'utilisation des ressources reçues afin de garantir leur affectation exclusive aux programmes et projets autorisés, dans le respect des engagements pris envers les donateurs, les partenaires, les bénéficiaires et les autorités compétentes. Cette démarche renforce la confiance, la transparence et la redevabilité qui fondent durablement les relations entre l'Organisation et l'ensemble de ses contributeurs.

7.6 Fondations

Les **fondations** représentent des partenaires stratégiques majeurs dans le financement des programmes de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En raison de leur rôle dans le soutien aux initiatives d'intérêt général, l'Organisation veille à établir avec elles des relations fondées sur la transparence, la confiance, la responsabilité et le respect des principes de bonne gouvernance. Toute collaboration avec une fondation est précédée d'une évaluation approfondie visant à garantir la conformité de la relation avec les exigences légales, réglementaires et institutionnelles applicables en matière de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**.

Avant d'accepter un financement ou de conclure un partenariat, AGCE International procède à la vérification de l'identité juridique de la fondation, de son statut légal, de ses organes de gouvernance, de sa mission, de ses domaines d'intervention, de son historique institutionnel ainsi que de la provenance des ressources financières destinées au financement des projets. Lorsque cela est nécessaire, l'Organisation identifie également les personnes

exerçant un contrôle effectif sur la fondation, conformément aux exigences de connaissance des partenaires (KYC).

Les conventions conclues avec les fondations précisent les objectifs poursuivis, les modalités de financement, les engagements réciproques, les mécanismes de contrôle, les exigences de reporting, les procédures d'audit ainsi que les conditions d'utilisation des ressources. AGCE International veille à préserver son indépendance institutionnelle et refuse toute contribution susceptible d'influencer ses décisions, de compromettre sa neutralité ou d'imposer des conditions incompatibles avec ses missions statutaires ou les lois applicables.

Les financements accordés par les fondations font l'objet d'une gestion rigoureuse, d'une comptabilité transparente, d'un suivi technique et financier permanent ainsi que d'une évaluation régulière des résultats obtenus. Toute anomalie, toute utilisation non conforme des fonds ou toute évolution significative du niveau de risque donne lieu à des mesures correctives appropriées conformément aux procédures internes de gouvernance, de contrôle interne et de conformité.

7.7 Entreprises

Les **entreprises** constituent des partenaires essentiels au développement durable des activités de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**, notamment dans le cadre du mécénat, de la responsabilité sociétale des entreprises (RSE), des partenariats stratégiques, des contributions financières, des dons en nature et des programmes de coopération technique. L'Organisation favorise les collaborations avec des entreprises partageant les valeurs d'éthique, de transparence, de responsabilité sociale, de développement durable et de respect des droits humains.

Avant toute relation de financement ou de partenariat, AGCE International réalise une évaluation de conformité portant sur l'existence juridique de l'entreprise, son immatriculation, ses représentants habilités, ses bénéficiaires effectifs lorsque cela est requis, son secteur d'activité, sa réputation, sa situation réglementaire ainsi que l'origine des ressources destinées au financement des projets. Cette analyse est conduite selon une approche fondée sur les risques afin de prévenir tout risque de blanchiment de capitaux, de financement du terrorisme, de corruption, de fraude ou de conflit d'intérêts.

L'Organisation s'assure que les contributions des entreprises sont compatibles avec ses missions, ses statuts et les principes de neutralité, d'indépendance et d'intégrité institutionnelle. Elle refuse tout financement provenant d'activités illicites ou incompatibles avec ses valeurs, ainsi que toute contribution assortie de conditions susceptibles de compromettre son autonomie décisionnelle, sa gouvernance ou l'intérêt général poursuivi par ses programmes.

Les partenariats conclus avec les entreprises sont formalisés par des conventions ou accords écrits précisant les droits et obligations des parties, les modalités de financement, les

objectifs du partenariat, les mécanismes de suivi, les indicateurs de performance, les procédures d'audit, les exigences de conformité et les modalités de résiliation. Les ressources reçues sont intégrées dans les systèmes comptables et financiers de l'Organisation, font l'objet d'une traçabilité complète et sont exclusivement affectées aux projets autorisés. Par cette démarche, AGCE International garantit une coopération responsable avec le secteur privé, conforme aux meilleures pratiques internationales en matière de gouvernance, de transparence et de conformité financière.

7.8 Institutions publiques

Les **institutions publiques** constituent des partenaires privilégiés de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** dans le cadre de la mise en œuvre de programmes d'intérêt général, de subventions publiques, de conventions de partenariat, de projets de coopération et d'initiatives de développement durable. Les relations établies avec les administrations nationales, les collectivités territoriales, les établissements publics, les organismes de coopération gouvernementale et les institutions internationales sont conduites dans le strict respect des principes de légalité, de transparence, d'impartialité et de bonne gouvernance.

Avant d'accepter un financement, une subvention, une convention ou tout autre appui provenant d'une institution publique, AGCE International procède à une vérification de la légitimité de l'organisme, de son habilitation légale, de la nature des ressources mises à disposition, des objectifs poursuivis ainsi que des obligations contractuelles, administratives, financières et réglementaires applicables. Cette analyse permet de garantir que les ressources publiques sont utilisées conformément à leur destination et dans le respect des exigences nationales et internationales relatives à la **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**.

Les conventions conclues avec les institutions publiques définissent de manière précise les responsabilités de chaque partie, les modalités de financement, les procédures de décaissement, les mécanismes de suivi, les obligations de reporting, les contrôles administratifs et financiers, ainsi que les conditions d'audit et d'évaluation. AGCE International veille à assurer une gestion rigoureuse des ressources publiques grâce à une comptabilité transparente, une séparation des responsabilités, un dispositif permanent de contrôle interne et une conservation sécurisée des pièces justificatives.

L'Organisation s'engage également à coopérer pleinement avec les autorités publiques compétentes dans le cadre des contrôles, inspections, audits ou demandes d'information légalement fondées. Toute anomalie, utilisation non conforme des fonds, irrégularité administrative ou manquement aux obligations contractuelles fait l'objet d'une analyse immédiate et de mesures correctives adaptées. Cette démarche garantit la protection des ressources publiques, renforce la confiance des institutions partenaires et contribue au développement d'une coopération durable fondée sur la responsabilité, la conformité et la redevabilité.

7.9 Cryptomonnaies (si autorisées)

Lorsque la législation applicable et les décisions des organes de gouvernance de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** l'autorisent, l'Organisation peut accepter des **dons ou financements en cryptomonnaies** à titre exceptionnel, sous réserve du respect de procédures de conformité renforcées. En raison des risques particuliers associés aux actifs numériques, notamment en matière de blanchiment de capitaux, de financement du terrorisme, de fraude, de cybercriminalité et de volatilité financière, ces opérations sont soumises à une vigilance accrue et à des contrôles spécifiques.

Avant l'acceptation d'un actif numérique, AGCE International procède à une évaluation approfondie de l'identité du donateur conformément aux procédures **KYC**, à une analyse de la provenance des actifs numériques dans la mesure où cela est raisonnablement possible, à la vérification de la plateforme ou du prestataire utilisé ainsi qu'à l'évaluation du niveau de risque associé à la transaction. L'Organisation privilégie, lorsque cela est possible, le recours à des prestataires de services sur actifs numériques régulièrement autorisés ou enregistrés auprès des autorités compétentes de leur juridiction.

Les dons en cryptomonnaies doivent être réalisés exclusivement au moyen des portefeuilles numériques officiellement approuvés par AGCE International. Toutes les transactions sont enregistrées, horodatées, documentées et rapprochées des informations relatives au donateur afin d'assurer une traçabilité complète des opérations. Les actifs numériques reçus peuvent, selon la politique financière de l'Organisation, être conservés temporairement ou convertis en monnaie fiduciaire par l'intermédiaire de prestataires conformes aux exigences réglementaires applicables.

AGCE International se réserve le droit de refuser toute transaction en cryptomonnaie lorsque l'identité du donateur ne peut être vérifiée de manière satisfaisante, lorsque l'origine des actifs demeure incertaine, lorsque les actifs proviennent de services anonymisants ou de plateformes présentant un risque élevé, ou lorsque la transaction est susceptible de contrevenir aux obligations légales, réglementaires ou à la présente politique **LBC/FT**. Toutes les opérations réalisées en actifs numériques demeurent soumises aux mêmes exigences de transparence, de traçabilité, de contrôle interne, d'audit et de redevabilité que les autres moyens de financement utilisés par l'Organisation.

7.10 Refus des financements illicites

Le **refus des financements illicites** constitue un principe fondamental de la politique de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. L'Organisation applique une politique de tolérance zéro à l'égard de toute ressource financière, matérielle, technique ou numérique dont l'origine, la destination ou les

conditions d'attribution sont contraires aux lois en vigueur, aux normes internationales de conformité ou aux valeurs éthiques qui fondent son action. Cette exigence vise à préserver l'intégrité institutionnelle de l'Organisation, à protéger sa réputation et à garantir que l'ensemble de ses ressources est exclusivement consacré à la réalisation de ses missions humanitaires, sociales, éducatives, sanitaires, environnementales, économiques et numériques.

Avant toute acceptation de financement, AGCE International procède à une analyse de conformité fondée sur les procédures de **Know Your Customer (KYC)**, l'évaluation des risques, la vérification de l'identité du contributeur, l'examen de l'origine des fonds, l'identification des bénéficiaires effectifs lorsque cela est requis, ainsi que le contrôle des informations disponibles relatives au donateur ou au bailleur. Toute incohérence, insuffisance documentaire, tentative de dissimulation ou élément laissant raisonnablement présumer un risque de blanchiment de capitaux, de financement du terrorisme, de corruption, de fraude, de trafic illicite, d'évasion des sanctions internationales ou de toute autre activité criminelle entraîne l'application de mesures de vigilance renforcées.

AGCE International refuse notamment les financements anonymes lorsque la législation ou le niveau de risque impose l'identification du contributeur, les ressources provenant d'activités manifestement illicites, les contributions destinées à contourner les obligations réglementaires, les financements assortis de conditions incompatibles avec les statuts ou les valeurs de l'Organisation, ainsi que toute opération susceptible de compromettre son indépendance, sa neutralité, sa transparence ou sa crédibilité institutionnelle. L'Organisation peut également refuser tout financement dont la provenance ne peut être raisonnablement démontrée ou qui présente un niveau de risque incompatible avec son dispositif de gestion des risques.

Lorsqu'un financement est identifié comme potentiellement illicite avant son acceptation, son traitement est immédiatement suspendu jusqu'à l'achèvement des vérifications nécessaires. Si le risque est confirmé, le financement est définitivement refusé et la décision est dûment documentée dans les registres de conformité. Lorsque la réglementation applicable l'impose, AGCE International coopère avec les autorités compétentes en transmettant les informations ou déclarations requises, dans le respect des obligations légales et du principe de confidentialité.

L'ensemble des décisions relatives au refus d'un financement est fondé sur des critères objectifs, proportionnés et documentés. Les analyses réalisées, les justificatifs examinés, les évaluations de risques et les décisions prises sont conservés conformément aux politiques de conservation documentaire de l'Organisation. Cette démarche garantit la transparence, la traçabilité, la redevabilité et le respect des meilleures pratiques internationales en matière de gouvernance, de conformité et de prévention du blanchiment de capitaux et du financement du terrorisme.

CHAPITRE 8

CONTRÔLE OPÉRATIONNEL, SURVEILLANCE DES OPÉRATIONS, SÉCURITÉ FINANCIÈRE, CONFORMITÉ ET AMÉLIORATION CONTINUE

Introduction générale

Dans un environnement marqué par l'intensification des flux financiers internationaux, la transformation numérique des services, la diversification des moyens de paiement électroniques et l'évolution constante des techniques de criminalité financière, les organisations de la société civile sont confrontées à des risques de plus en plus complexes susceptibles d'affecter leur gouvernance, leur stabilité financière, leur réputation et leur capacité à remplir durablement leurs missions d'intérêt général. Les dispositifs de lutte contre le blanchiment de capitaux, le financement du terrorisme, la fraude, la corruption, la cybercriminalité et les atteintes aux systèmes d'information ne constituent plus de simples exigences réglementaires ; ils représentent désormais des composantes essentielles d'une gouvernance moderne, responsable et conforme aux meilleures pratiques internationales.

Consciente de ces enjeux, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** a développé un dispositif intégré de contrôle opérationnel destiné à garantir la sécurité, la transparence, la traçabilité et la conformité de l'ensemble de ses activités administratives, financières, numériques et institutionnelles. Ce dispositif repose sur une approche préventive, proportionnée et fondée sur les risques, permettant d'identifier les vulnérabilités, d'anticiper les menaces, de détecter les anomalies, de renforcer les mécanismes de contrôle interne et d'assurer une réponse rapide et adaptée à tout incident susceptible de compromettre les ressources, les données, les opérations ou la réputation de l'Organisation.

Le présent chapitre constitue ainsi le cadre opérationnel permanent de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Il rassemble l'ensemble des procédures, mécanismes, responsabilités et outils permettant d'assurer une surveillance continue des opérations réalisées par l'Organisation, depuis la réception des ressources jusqu'à leur utilisation finale, en passant par leur validation, leur contrôle, leur enregistrement, leur conservation et leur audit. Il établit également les modalités de prévention, de détection, d'analyse, de traitement et de suivi des situations présentant un risque de non-conformité ou de criminalité financière.

L'approche retenue par AGCE International repose sur le principe selon lequel chaque opération, quelle que soit sa nature ou son montant, doit pouvoir être identifiée, justifiée, autorisée, tracée et contrôlée. À cette fin, l'Organisation met en œuvre un ensemble cohérent de procédures couvrant notamment les paiements, les cotisations, les adhésions, les

abonnements, les dons, les remboursements, les transferts nationaux et internationaux, ainsi que toute autre opération financière ou patrimoniale réalisée dans le cadre de ses activités. Chaque transaction fait l'objet d'un niveau de surveillance adapté à son niveau de risque, conformément à l'approche basée sur les risques adoptée par l'Organisation.

Ce chapitre définit également les mécanismes de détection des opérations inhabituelles ou suspectes grâce à l'utilisation d'indicateurs de risque, de critères d'analyse, de procédures documentées d'investigation et de systèmes d'alerte permettant une intervention rapide des responsables compétents. L'objectif est d'assurer une identification précoce des comportements anormaux, des incohérences documentaires, des tentatives de fraude, des manipulations financières, des cyberattaques ou de toute autre activité susceptible de porter atteinte aux intérêts de l'Organisation ou de contrevenir aux exigences légales et réglementaires applicables.

Le dispositif présenté repose également sur un système robuste de **contrôle interne**, fondé sur la séparation des responsabilités, la double validation des opérations sensibles, la supervision hiérarchique, la revue périodique des activités, la traçabilité des décisions, la tenue d'un journal des opérations et la réalisation d'audits internes et externes. Ces mécanismes permettent de réduire les risques d'erreur, de fraude, d'abus de confiance, de détournement de fonds ou de conflit d'intérêts, tout en renforçant la fiabilité des processus décisionnels et la qualité de l'information financière.

Compte tenu de l'évolution rapide des technologies financières, AGCE International accorde une importance particulière à la **sécurisation des moyens de paiement** et des infrastructures numériques utilisées dans le cadre de ses activités. Les plateformes de paiement électronique, les virements bancaires, les solutions de paiement mobile, les cartes bancaires et les autres services financiers numériques sont exploités selon des procédures de sécurité renforcées intégrant notamment l'authentification multifacteur, le chiffrement des données, la sécurisation des interfaces techniques, la surveillance des transactions, la journalisation des événements, la gestion des accès et la protection contre les cybermenaces.

La conformité institutionnelle repose également sur une gestion rigoureuse des informations et des documents produits dans le cadre des activités de l'Organisation. Les dossiers administratifs, financiers, comptables, contractuels et numériques sont conservés selon des règles précises garantissant leur intégrité, leur disponibilité, leur confidentialité et leur traçabilité pendant toute la durée prévue par les réglementations applicables. Des procédures sécurisées d'archivage, de consultation, de conservation et de destruction documentaire sont mises en œuvre afin de préserver la valeur probante des informations et de protéger les données sensibles contre tout accès non autorisé, toute perte ou toute altération.

Dans une logique de gouvernance responsable, AGCE International reconnaît également l'importance des mécanismes de **signalement interne** et de protection des lanceurs d'alerte. Toute personne agissant de bonne foi doit pouvoir signaler une irrégularité, une fraude présumée, une violation des règles internes ou un comportement contraire aux exigences de conformité, sans craindre de représailles. L'Organisation garantit la

confidentialité des signalements, l'impartialité de leur traitement et la protection des personnes concernées conformément à ses politiques internes et aux dispositions légales applicables.

Le maintien d'un dispositif de conformité performant repose également sur le développement permanent des compétences de l'ensemble des acteurs de l'Organisation. À cette fin, AGCE International met en œuvre des programmes réguliers de formation, de sensibilisation et de renforcement des capacités destinés aux administrateurs, dirigeants, responsables financiers, collaborateurs, bénévoles, partenaires et prestataires. Ces actions permettent d'assurer une compréhension homogène des risques, des obligations réglementaires, des procédures internes et des bonnes pratiques de gouvernance.

Le présent chapitre prévoit en outre les modalités de gestion des incidents susceptibles d'affecter le fonctionnement de l'Organisation, notamment les fraudes, les cyberattaques, les compromissions de comptes, les paiements frauduleux, les atteintes aux données, les interruptions de services ou tout autre événement opérationnel majeur. Des procédures de réponse, de remédiation, de communication, de continuité d'activité et de reprise sont définies afin de limiter les conséquences des incidents et de garantir la résilience de l'Organisation.

Enfin, ce dispositif s'inscrit dans une démarche d'**amélioration continue** fondée sur des audits réguliers, des évaluations périodiques, des indicateurs de performance, des tableaux de bord de conformité, des plans d'actions correctives et une révision continue des procédures. Les enseignements tirés des contrôles, des incidents, des audits et des évolutions réglementaires alimentent en permanence le renforcement du système de gouvernance et de conformité d'AGCE International.

À travers ce chapitre, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** réaffirme son engagement à mettre en œuvre un dispositif opérationnel robuste, transparent, sécurisé et conforme aux meilleures pratiques internationales. En intégrant de manière cohérente la surveillance des opérations, le contrôle interne, la sécurité des paiements, la gestion documentaire, la protection des lanceurs d'alerte, la formation, la gestion des incidents, l'audit et l'amélioration continue, l'Organisation renforce durablement la confiance de ses membres, partenaires, donateurs, bailleurs de fonds, autorités publiques et bénéficiaires, tout en garantissant une gestion responsable des ressources qui lui sont confiées au service de l'intérêt général.

SECTION I

SURVEILLANCE PERMANENTE DES OPÉRATIONS FINANCIÈRES

8.1 Principes généraux

La **surveillance permanente des opérations financières** constitue l'un des piliers essentiels du dispositif de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour finalité d'assurer un contrôle continu de l'ensemble des flux financiers, des opérations administratives et des transactions numériques réalisées par l'Organisation, afin de garantir leur légalité, leur traçabilité, leur transparence et leur conformité avec les exigences réglementaires nationales et internationales.

Cette surveillance repose sur une approche proactive et continue couvrant toutes les étapes du cycle de vie d'une opération financière, depuis son initiation jusqu'à son archivage définitif. Elle s'applique notamment aux cotisations, adhésions, abonnements, dons, subventions, paiements, remboursements, virements, transferts internationaux, contributions en nature valorisées, produits de collecte de fonds ainsi qu'à toute autre opération susceptible d'avoir un impact financier, comptable ou patrimonial sur l'Organisation. Chaque transaction est analysée selon son niveau de risque, sa nature, son montant, son origine, sa destination, son mode de paiement et le profil des personnes ou entités concernées.

La surveillance permanente vise également à détecter de manière précoce toute opération inhabituelle, incohérente ou potentiellement suspecte pouvant révéler un risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de ressources, de cybercriminalité ou de violation des procédures internes. À cette fin, AGCE International met en œuvre des mécanismes de contrôle automatisés et manuels, des seuils d'alerte, des analyses documentaires, des rapprochements comptables, des validations hiérarchiques et des revues périodiques permettant d'identifier rapidement toute anomalie nécessitant une investigation complémentaire.

La surveillance permanente s'inscrit dans une démarche d'amélioration continue et de maîtrise des risques. Les informations collectées à travers les systèmes financiers, comptables et numériques sont exploitées afin d'évaluer les tendances, de mesurer les niveaux d'exposition aux risques, de renforcer les dispositifs de contrôle interne et d'orienter les décisions des organes de gouvernance. Cette approche contribue à protéger les ressources de l'Organisation, à garantir la fiabilité des informations financières, à préserver la confiance des membres, partenaires, donateurs, bailleurs de fonds et autorités compétentes, tout en assurant une utilisation responsable des ressources mobilisées.

L'ensemble des opérations de surveillance est réalisé dans le respect des principes de confidentialité, de protection des données personnelles, de proportionnalité, de traçabilité et de responsabilité. Chaque contrôle effectué, chaque anomalie détectée, chaque décision prise et chaque mesure corrective engagée font l'objet d'une documentation appropriée garantissant la transparence du dispositif et facilitant les audits internes, les contrôles externes ainsi que les évaluations de conformité.

En intégrant des mécanismes permanents de prévention, de détection, d'analyse, de contrôle et de suivi des opérations financières, AGCE International renforce durablement son système de gouvernance financière, sa résilience face aux risques émergents et son engagement envers les meilleures pratiques internationales en matière de conformité, de transparence et de gestion responsable des ressources au service de ses missions humanitaires, sociales, éducatives, sanitaires, environnementales, économiques et numériques.

8.2 Surveillance des paiements

La **surveillance des paiements** constitue une composante essentielle du dispositif de contrôle financier de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif de garantir que tous les paiements reçus ou effectués par l'Organisation sont autorisés, légitimes, correctement documentés, traçables et conformes aux exigences de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**, ainsi qu'aux réglementations nationales et internationales applicables.

La surveillance couvre l'ensemble des moyens de paiement utilisés par l'Organisation, notamment les virements bancaires, les cartes bancaires, les plateformes de paiement électronique, les solutions de paiement mobile, les portefeuilles numériques et tout autre instrument de paiement officiellement approuvé. Chaque transaction fait l'objet d'un contrôle portant sur l'identité de l'émetteur ou du bénéficiaire, la provenance ou la destination des fonds, le montant, la devise, le motif du paiement, les justificatifs associés et le respect des procédures internes de validation.

Les paiements sont analysés selon une approche fondée sur les risques afin d'identifier toute opération inhabituelle ou incohérente. Une vigilance renforcée est appliquée aux paiements d'un montant élevé, aux opérations internationales, aux paiements fractionnés, aux transactions répétitives sans justification économique apparente, aux opérations impliquant des juridictions à risque ou des prestataires présentant un niveau de risque élevé. Lorsque des anomalies sont détectées, l'opération peut être suspendue jusqu'à l'achèvement des vérifications nécessaires.

Chaque paiement est enregistré dans les systèmes comptables et financiers de l'Organisation et fait l'objet d'un rapprochement avec les pièces justificatives, les autorisations internes et les relevés des établissements financiers. Les opérations sont conservées dans des

journaux sécurisés permettant d'assurer une traçabilité complète, de faciliter les contrôles internes, les audits et les investigations éventuelles.

La surveillance permanente des paiements permet à AGCE International de protéger ses ressources financières, de prévenir les risques de fraude, de blanchiment de capitaux, de financement du terrorisme, de cybercriminalité et d'erreurs opérationnelles, tout en garantissant une gestion responsable, transparente et conforme des ressources confiées à l'Organisation.

8.3 Surveillance des cotisations

Les **cotisations** constituent une ressource régulière contribuant au fonctionnement institutionnel et au développement des activités de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Leur surveillance permanente vise à garantir que chaque contribution est collectée, enregistrée, contrôlée et affectée conformément aux procédures financières, comptables et administratives de l'Organisation, dans le respect des exigences de conformité **LBC/FT**.

La surveillance des cotisations s'applique à l'ensemble des versements effectués par les membres, bénévoles, partenaires, organisations affiliées, entreprises, fondations, antennes nationales et internationales ou toute autre catégorie de contributeurs reconnue par les statuts et règlements de l'Organisation. Chaque cotisation est associée à l'identité du cotisant, à sa catégorie d'adhésion, à la période concernée, au montant versé, au mode de paiement utilisé et aux justificatifs correspondants.

Les informations relatives aux cotisations sont systématiquement rapprochées des registres des membres, des contrats d'adhésion, des relevés bancaires, des plateformes de paiement électronique et des écritures comptables afin de garantir l'exactitude des données et de détecter toute anomalie. Une attention particulière est portée aux paiements multiples, aux montants inhabituels, aux versements provenant de tiers non identifiés, aux retards importants, aux remboursements exceptionnels et aux opérations présentant un risque accru de fraude ou de blanchiment de capitaux.

Des mécanismes de contrôle automatisés et manuels permettent de produire des alertes en cas d'incohérences, d'écarts comptables ou de comportements atypiques. Les responsables compétents procèdent alors aux vérifications nécessaires avant toute régularisation ou validation définitive. Toutes les opérations de contrôle sont documentées et conservées conformément aux règles de conservation documentaire de l'Organisation.

Grâce à cette surveillance continue, AGCE International garantit l'intégrité de son système de collecte des cotisations, assure la fiabilité de ses ressources financières, renforce la confiance de ses membres et partenaires, et démontre son engagement constant en faveur d'une gouvernance transparente, responsable et conforme aux meilleures pratiques internationales en matière de gestion financière et de prévention des risques.

8.4 Surveillance des adhésions

La **surveillance des adhésions** constitue un élément fondamental du dispositif de contrôle institutionnel de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle vise à garantir que toute demande d'adhésion, qu'elle émane d'une personne physique ou morale, est traitée conformément aux statuts, aux règlements internes, aux procédures de gouvernance ainsi qu'aux exigences de la **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Cette surveillance permet de préserver l'intégrité de la communauté des membres et de prévenir toute tentative d'utilisation abusive de l'Organisation à des fins illicites.

Toute demande d'adhésion fait l'objet d'une procédure de vérification portant sur l'identité du demandeur, la qualité des informations fournies, la catégorie d'adhésion sollicitée, la conformité des documents justificatifs, les modalités de paiement des droits d'adhésion ainsi que le respect des critères d'éligibilité définis par l'Organisation. Les personnes morales sont soumises, en outre, à des contrôles relatifs à leur existence juridique, à leur gouvernance, à leurs représentants habilités et, lorsque cela est nécessaire, à l'identification de leurs bénéficiaires effectifs.

Les droits d'adhésion sont rapprochés des dossiers administratifs, des justificatifs de paiement, des contrats d'adhésion et des registres officiels des membres afin de garantir la cohérence des informations et la traçabilité des opérations. Toute anomalie, telle qu'une identité incomplète, des documents irréguliers, un paiement non justifié, une tentative de double adhésion ou une incohérence entre les informations déclarées et les pièces produites, fait l'objet d'une analyse approfondie avant toute validation définitive.

La surveillance des adhésions est également assurée tout au long de la relation avec le membre. AGCE International veille à la mise à jour régulière des informations administratives, à la vérification des changements de situation, au suivi du respect des engagements statutaires et à l'application des mesures de vigilance adaptées en cas d'évolution du niveau de risque. Les opérations d'adhésion sont documentées, archivées et intégrées aux dispositifs de contrôle interne, de conformité et d'audit afin de garantir une gouvernance transparente, responsable et conforme aux meilleures pratiques internationales.

8.5 Surveillance des abonnements

La **surveillance des abonnements** a pour objet d'assurer un contrôle permanent des souscriptions aux services, plateformes numériques, applications, programmes de formation, espaces membres, solutions technologiques et autres prestations proposées par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle garantit que chaque abonnement est établi, renouvelé, suspendu ou résilié dans le respect des règles contractuelles, financières, administratives et réglementaires applicables.

Avant l'activation d'un abonnement, l'Organisation vérifie l'identité du souscripteur, la validité des informations fournies, la conformité des documents justificatifs lorsque ceux-ci sont requis, la régularité du paiement, le choix de l'offre souscrite ainsi que l'acceptation des conditions générales d'utilisation, des politiques de confidentialité et des règles de conformité applicables. Les abonnements sont enregistrés dans les systèmes de gestion afin d'assurer leur suivi pendant toute leur durée de validité.

Les opérations de renouvellement, de modification, de suspension, de résiliation ou de remboursement font l'objet de contrôles réguliers destinés à détecter toute anomalie susceptible de révéler une fraude, une usurpation d'identité, une utilisation abusive des comptes, un paiement irrégulier ou toute autre opération incompatible avec les procédures internes. Les systèmes d'information de l'Organisation peuvent générer des alertes automatiques en cas de paiements multiples, d'échecs de paiement répétés, de modifications inhabituelles des informations du titulaire ou d'activités présentant un niveau de risque élevé.

L'ensemble des données relatives aux abonnements est rapproché des registres des utilisateurs, des plateformes de paiement, des écritures comptables et des contrats de service afin de garantir l'exactitude des informations et la traçabilité complète des opérations. Les responsables compétents procèdent à des revues périodiques permettant de vérifier la conformité des abonnements actifs, d'identifier les irrégularités éventuelles et de mettre en œuvre les mesures correctives appropriées.

Par cette surveillance permanente, AGCE International sécurise l'accès à ses services numériques, protège les intérêts de ses membres, partenaires et utilisateurs, garantit la fiabilité de ses recettes récurrentes et renforce son dispositif global de contrôle interne, de conformité réglementaire et de prévention des risques financiers, opérationnels et technologiques.

8.6 Surveillance des dons

La **surveillance des dons** constitue un mécanisme fondamental de gouvernance financière permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de garantir que toutes les contributions financières, matérielles, techniques ou numériques reçues par l'Organisation proviennent de sources licites, transparentes et conformes aux principes de la **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Elle vise à préserver l'intégrité des activités humanitaires et de développement de l'Organisation tout en renforçant la confiance des donateurs, des bénéficiaires, des partenaires institutionnels et des autorités de contrôle.

Tous les dons, qu'ils soient ponctuels, réguliers, affectés à un projet spécifique ou destinés au fonctionnement général de l'Organisation, font l'objet d'une procédure de vérification proportionnée au niveau de risque présenté. Cette vérification porte notamment sur l'identité du donateur, l'origine des fonds, le montant du don, le moyen de paiement utilisé, la devise, la finalité déclarée de la contribution, les éventuelles conditions imposées par le donateur ainsi que les documents justificatifs nécessaires. Lorsque le don est effectué par une

entreprise, une fondation, une association ou une institution publique, des contrôles complémentaires peuvent être réalisés afin de vérifier l'existence juridique de l'entité, l'identité de ses représentants habilités et, si nécessaire, celle de ses bénéficiaires effectifs.

L'Organisation met en œuvre des dispositifs de surveillance destinés à détecter les dons présentant un caractère inhabituel, notamment les versements d'un montant exceptionnel, les dons fractionnés, les contributions provenant de pays ou de territoires à risque, les paiements réalisés par des intermédiaires non identifiés, les dons anonymes lorsque la réglementation ne les autorise pas, ainsi que toute opération susceptible de masquer l'origine réelle des fonds. Toute situation présentant un indice de risque fait l'objet d'une analyse approfondie pouvant conduire à une demande d'informations complémentaires, à une suspension temporaire de l'opération, à un refus du don ou, lorsque les circonstances l'exigent, à un signalement auprès des autorités compétentes.

Chaque don accepté est enregistré dans les systèmes administratifs, financiers et comptables de l'Organisation. Il est rapproché des justificatifs de paiement, des conventions éventuelles, des reçus délivrés aux donateurs et des affectations budgétaires correspondantes afin d'assurer une traçabilité complète des ressources collectées. L'utilisation des fonds fait également l'objet d'un suivi permanent garantissant leur affectation conforme aux objectifs humanitaires, sociaux, éducatifs, sanitaires, environnementaux ou numériques pour lesquels ils ont été mobilisés.

Par cette surveillance continue, AGCE International protège son intégrité financière, prévient les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption et de détournement de ressources, tout en consolidant une culture de transparence, de responsabilité et de redevabilité conforme aux meilleures pratiques internationales de gestion des organisations à but non lucratif.

8.7 Surveillance des remboursements

La **surveillance des remboursements** constitue une mesure essentielle de maîtrise des risques financiers et de protection des ressources de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle garantit que toute restitution de fonds, qu'elle résulte d'une erreur de paiement, d'une annulation d'opération, de l'application d'une politique de rétractation, d'un trop-perçu ou d'une décision administrative, est effectuée dans un cadre strictement contrôlé, documenté et conforme aux exigences de la présente Politique **LBC/FT**.

Aucun remboursement ne peut être exécuté sans une vérification préalable portant sur la légitimité de la demande, l'identité du bénéficiaire, la réalité de la transaction initiale, la disponibilité des pièces justificatives et l'autorisation des responsables compétents. Les demandes de remboursement sont systématiquement comparées aux registres financiers, aux contrats, aux factures, aux reçus, aux historiques de paiement et aux informations enregistrées dans les systèmes de gestion afin de garantir leur exactitude et leur conformité.

Une vigilance particulière est exercée sur les remboursements présentant des caractéristiques inhabituelles, tels que les remboursements répétés, les demandes portant sur des montants importants, les modifications de coordonnées bancaires avant remboursement, les restitutions sollicitées vers un compte différent de celui utilisé lors du paiement initial, les remboursements internationaux ou les opérations susceptibles de constituer un mécanisme de blanchiment de capitaux ou de fraude financière. Dans de telles situations, des contrôles renforcés sont mis en œuvre avant toute décision.

Les remboursements sont soumis au principe de la double validation, impliquant les services administratifs, financiers ou de conformité selon la nature et le niveau de risque de l'opération. Chaque remboursement fait l'objet d'un enregistrement détaillé précisant son motif, son montant, sa date, son bénéficiaire, les autorisations obtenues, le moyen de paiement utilisé et les références des documents justificatifs. Ces informations sont conservées conformément à la politique de conservation documentaire de l'Organisation et demeurent disponibles pour les besoins des contrôles internes, des audits et des autorités compétentes.

Grâce à cette surveillance permanente, AGCE International assure une gestion rigoureuse des restitutions de fonds, limite les risques d'erreurs, de détournement, de fraude ou d'utilisation abusive des procédures de remboursement, tout en garantissant une gestion financière transparente, équitable et conforme aux exigences légales, réglementaires et institutionnelles applicables.

8.8 Surveillance des transferts internationaux

La **surveillance des transferts internationaux** constitue un dispositif stratégique de maîtrise des risques financiers et de conformité réglementaire mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Compte tenu de la dimension internationale de l'Organisation, de ses représentations dans plusieurs pays, de ses partenariats avec des institutions publiques et privées, de ses programmes de coopération internationale ainsi que de la diversité de ses sources de financement, les mouvements transfrontaliers de fonds font l'objet d'une vigilance renforcée afin de prévenir tout risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de contournement des sanctions internationales ou de toute autre activité financière illicite.

La présente politique s'applique à l'ensemble des transferts internationaux, qu'ils concernent les dons, les subventions, les cotisations, les adhésions, les abonnements, les financements de projets, les remboursements, les paiements de fournisseurs, les dépenses opérationnelles, les aides humanitaires ou toute autre opération financière réalisée entre deux ou plusieurs États. Chaque transfert est soumis à une analyse préalable permettant de vérifier sa légitimité, son objet, son montant, sa destination, son bénéficiaire, son mode d'exécution et sa conformité avec les réglementations applicables dans les juridictions concernées.

Avant toute exécution, l'Organisation procède à la vérification de l'identité des parties concernées, de l'origine licite des fonds, de la justification économique ou humanitaire de l'opération, de la conformité des documents justificatifs ainsi que du respect des procédures internes de validation. Une attention particulière est portée aux opérations impliquant des pays présentant un niveau de risque élevé, des juridictions faisant l'objet de sanctions internationales, des organismes insuffisamment identifiés ou des structures dont les bénéficiaires effectifs ne peuvent être clairement établis.

Les transferts internationaux sont réalisés exclusivement par l'intermédiaire d'établissements financiers, de plateformes de paiement ou de prestataires officiellement autorisés et respectant les exigences internationales en matière de conformité, de connaissance du client (KYC), de lutte contre le blanchiment de capitaux (AML) et de lutte contre le financement du terrorisme (CFT). Toute opération présentant un caractère inhabituel, un fractionnement injustifié, une destination incohérente ou des informations incomplètes peut être suspendue, faire l'objet de contrôles renforcés ou être refusée jusqu'à la levée des doutes identifiés.

Chaque transfert est enregistré dans les systèmes administratifs, financiers et comptables de l'Organisation. Les références bancaires, justificatifs de paiement, contrats, conventions, autorisations internes, preuves d'exécution et correspondances associées sont conservés afin de garantir une traçabilité complète des opérations. Les responsables de la conformité réalisent des revues périodiques des flux internationaux afin d'identifier les tendances, de mesurer les niveaux d'exposition aux risques et de renforcer les dispositifs de contrôle lorsque cela s'avère nécessaire.

Par cette surveillance permanente, AGCE International assure une gestion responsable des flux financiers internationaux, protège les ressources qui lui sont confiées, renforce la confiance de ses partenaires nationaux et internationaux et garantit le respect des meilleures pratiques internationales en matière de gouvernance financière et de conformité réglementaire.

8.9 Détection automatique des anomalies

La **détection automatique des anomalies** constitue un mécanisme permanent de prévention et d'identification précoce des risques financiers, opérationnels et technologiques au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle repose sur l'utilisation de solutions numériques, de règles de contrôle automatisées, d'algorithmes d'analyse, de systèmes d'alerte et de mécanismes de surveillance continue destinés à identifier toute opération inhabituelle susceptible de compromettre la sécurité, la conformité ou l'intégrité des activités de l'Organisation.

Les systèmes de surveillance sont configurés pour analyser en temps réel ou de manière périodique l'ensemble des opérations financières, administratives et numériques réalisées par l'Organisation. Ils prennent notamment en compte les montants des transactions,

leur fréquence, leur provenance, leur destination, les modes de paiement utilisés, les profils des utilisateurs, les historiques d'activité, les modifications des données sensibles ainsi que les comportements inhabituels susceptibles de révéler une fraude, une tentative de blanchiment de capitaux, une cyberattaque ou toute autre activité anormale.

Des alertes automatiques peuvent être générées lorsqu'une transaction dépasse les seuils de vigilance définis par l'Organisation, lorsqu'un paiement est fractionné sans justification, lorsqu'un utilisateur modifie de manière répétée ses informations d'identification, lorsqu'un compte effectue des opérations incompatibles avec son profil habituel, lorsqu'un transfert concerne une juridiction sensible ou lorsqu'une tentative d'accès non autorisée est détectée sur les systèmes d'information.

Toute anomalie identifiée fait l'objet d'une analyse par les responsables compétents afin d'évaluer son niveau de risque, d'en déterminer les causes et de décider des mesures appropriées. Selon la nature des faits constatés, l'opération peut être validée, suspendue, rejetée, faire l'objet d'investigations complémentaires ou être signalée aux autorités compétentes conformément aux procédures internes de conformité.

Les paramètres des systèmes de détection sont régulièrement révisés afin de tenir compte des évolutions réglementaires, des nouvelles typologies de fraude, des menaces émergentes, des recommandations des autorités de supervision et des enseignements tirés des audits, des incidents et des retours d'expérience. Cette démarche d'amélioration continue permet d'accroître progressivement la performance du dispositif de surveillance et de réduire les risques de faux positifs ou de détection tardive.

En intégrant des mécanismes avancés de détection automatique au sein de son système de gouvernance, AGCE International renforce sa capacité à prévenir les risques financiers et opérationnels, améliore la rapidité de ses interventions, sécurise ses ressources et garantit un niveau élevé de conformité, de transparence et de protection des intérêts de ses membres, partenaires, donateurs, bénéficiaires et institutions de contrôle.

8.10 Gestion des alertes

La **gestion des alertes** constitue un élément central du dispositif de surveillance permanente des opérations financières mis en place par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour finalité d'assurer l'identification rapide, l'analyse objective, le traitement rigoureux et le suivi documenté de toute situation susceptible de présenter un risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de cybercriminalité, de détournement de ressources, de non-conformité réglementaire ou de toute autre menace pouvant compromettre la sécurité financière, opérationnelle ou institutionnelle de l'Organisation.

Le système de gestion des alertes repose sur une approche préventive, proportionnée et fondée sur les risques. Toute anomalie détectée par les dispositifs de surveillance

automatisés, les contrôles manuels, les audits, les signalements internes, les partenaires financiers ou les autorités compétentes est enregistrée dans un dispositif sécurisé permettant d'assurer une prise en charge immédiate et adaptée à son niveau de criticité. Chaque alerte est traitée avec impartialité, confidentialité et diligence, dans le respect des droits des personnes concernées ainsi que des obligations légales et réglementaires applicables.

Les alertes peuvent notamment être déclenchées à la suite d'opérations financières inhabituelles, de paiements présentant des caractéristiques atypiques, de transferts internationaux non justifiés, de dons provenant de sources insuffisamment identifiées, de remboursements irréguliers, de tentatives d'usurpation d'identité, d'accès non autorisés aux systèmes d'information, de modifications suspectes de données sensibles, de comportements incompatibles avec les profils habituels des utilisateurs ou de tout autre événement révélant une vulnérabilité susceptible d'affecter les activités de l'Organisation.

Dès la détection d'une alerte, les responsables compétents procèdent à une évaluation préliminaire afin de déterminer la nature des faits, leur niveau de gravité, leur impact potentiel ainsi que les mesures conservatoires à mettre en œuvre. Selon les circonstances, ces mesures peuvent comprendre la suspension temporaire d'une transaction, le blocage d'un paiement, le gel d'un compte utilisateur, la demande de documents complémentaires, la réalisation de contrôles renforcés, l'ouverture d'une enquête interne ou la saisine des autorités compétentes lorsque la réglementation l'exige.

Chaque alerte fait l'objet d'une documentation complète précisant son origine, sa date de détection, les personnes concernées, les opérations visées, les analyses effectuées, les décisions prises, les mesures correctives mises en œuvre et les résultats obtenus. Cette documentation est intégrée aux registres de conformité de l'Organisation afin de garantir une parfaite traçabilité des investigations et de faciliter les contrôles internes, les audits indépendants ainsi que les éventuelles inspections des autorités de supervision.

Le traitement des alertes repose sur une collaboration étroite entre les responsables administratifs, financiers, comptables, informatiques, les responsables de la conformité, les organes de gouvernance et, lorsque cela est nécessaire, les partenaires bancaires, les prestataires de services financiers ou les autorités publiques compétentes. Cette coordination garantit une réponse rapide, cohérente et proportionnée, tout en limitant les conséquences financières, juridiques, opérationnelles et réputationnelles susceptibles de résulter d'un incident.

Afin d'améliorer en permanence l'efficacité du dispositif, AGCE International procède à une analyse régulière des alertes enregistrées. Les tendances observées, les causes récurrentes, les nouveaux modes opératoires, les vulnérabilités identifiées ainsi que les recommandations issues des audits, des contrôles et des retours d'expérience sont intégrés dans les procédures de gestion des risques et dans les programmes de formation du personnel. Cette démarche permet d'adapter continuellement les paramètres des systèmes de surveillance, de renforcer les contrôles internes et d'améliorer les capacités de prévention et de détection.

Les informations relatives aux alertes sont traitées dans le strict respect des principes de confidentialité, de protection des données personnelles, de sécurité de l'information et de présomption de bonne foi. Seules les personnes dûment habilitées peuvent accéder aux dossiers d'alerte dans la limite de leurs attributions professionnelles, et toute divulgation non autorisée d'informations confidentielles est susceptible d'entraîner des mesures disciplinaires ou des poursuites conformément aux textes applicables.

Par ce dispositif permanent de gestion des alertes, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce sa capacité à prévenir les risques, à détecter rapidement les situations anormales, à protéger les ressources qui lui sont confiées et à assurer une gouvernance exemplaire fondée sur la transparence, la responsabilité, la conformité réglementaire et l'amélioration continue. Cette organisation contribue à préserver la confiance des membres, des donateurs, des partenaires, des bailleurs de fonds, des bénéficiaires et des autorités publiques, tout en garantissant la pérennité et la crédibilité des missions humanitaires, sociales, éducatives, sanitaires, environnementales, économiques et numériques portées par l'Organisation.

SECTION II

DÉTECTION DES OPÉRATIONS SUSPECTES

8.11 Principes

La **détection des opérations suspectes** constitue l'un des fondements essentiels du dispositif de **Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)** adopté par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif d'identifier, d'analyser, de documenter et de traiter, dans les meilleurs délais, toute opération financière, administrative ou numérique susceptible de révéler un risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de ressources, de cybercriminalité ou de toute autre activité illicite pouvant compromettre la sécurité, la réputation ou la conformité de l'Organisation.

Le dispositif de détection repose sur une **approche fondée sur les risques**, permettant d'adapter le niveau de vigilance à la nature des opérations, aux profils des membres, donateurs, partenaires, prestataires et bénéficiaires, aux montants concernés, aux pays impliqués, aux moyens de paiement utilisés ainsi qu'au contexte économique, juridique et opérationnel dans lequel les transactions sont réalisées. Cette approche garantit une utilisation proportionnée des ressources de contrôle tout en assurant une surveillance permanente des opérations présentant les niveaux de risque les plus élevés.

La notion d'**opération suspecte** ne se limite pas à la constatation d'une infraction pénale. Elle couvre toute transaction, tout comportement ou toute situation qui, en raison de sa nature, de son montant, de sa fréquence, de son mode d'exécution, de son absence de

justification économique ou de son incompatibilité avec le profil habituel de la personne concernée, est susceptible de révéler un risque de criminalité financière ou une tentative de contournement des procédures internes de contrôle. Une simple présomption raisonnable ou un faisceau d'indices concordants peut justifier l'ouverture d'une analyse approfondie, sans qu'il soit nécessaire de disposer d'une preuve définitive d'une activité illicite.

AGCE International applique le principe de **vigilance permanente** à l'ensemble des opérations réalisées dans le cadre de ses activités. Cette vigilance couvre notamment les adhésions, les cotisations, les abonnements, les dons, les subventions, les paiements, les remboursements, les transferts nationaux et internationaux, les conventions de partenariat, les contrats de prestation, les achats, les projets financés ainsi que toute autre opération impliquant des flux financiers, des biens ou des ressources susceptibles de présenter un risque de non-conformité.

La détection des opérations suspectes repose sur la combinaison de plusieurs mécanismes complémentaires, notamment les contrôles documentaires, les rapprochements comptables, les vérifications d'identité, les procédures de connaissance des membres et partenaires (KYC), les systèmes automatisés de surveillance, les indicateurs de risque, les signalements internes, les audits, les contrôles hiérarchiques ainsi que les analyses réalisées par les responsables de la conformité. Cette approche multidimensionnelle permet d'améliorer la capacité de l'Organisation à identifier rapidement les situations nécessitant une investigation.

Lorsqu'une anomalie est détectée, l'Organisation procède à une évaluation objective des faits en tenant compte des informations disponibles, des explications fournies par les personnes concernées, des documents justificatifs produits, de l'historique des opérations ainsi que des risques potentiels pour l'Organisation. Les investigations sont conduites dans le respect des principes d'impartialité, de confidentialité, de proportionnalité et de présomption de bonne foi, tout en garantissant la protection des données personnelles et des informations sensibles.

Le dispositif de détection prévoit également la mise en œuvre de **mesures conservatoires** lorsque la situation l'exige. Selon le niveau de risque identifié, l'Organisation peut notamment suspendre temporairement une transaction, différer un paiement, demander des informations complémentaires, renforcer les contrôles, limiter l'accès à certains services, bloquer une opération ou engager une enquête interne avant toute décision définitive. Lorsque les éléments recueillis révèlent une suspicion sérieuse d'activité illicite, les procédures de signalement prévues par les lois applicables et par la présente politique sont mises en œuvre.

Afin de garantir l'efficacité du dispositif, chaque opération suspecte identifiée fait l'objet d'une **documentation complète et sécurisée**. Les informations relatives à la détection, aux analyses réalisées, aux décisions prises, aux mesures appliquées et aux suites données sont enregistrées dans les registres de conformité de l'Organisation. Cette documentation assure la traçabilité des investigations, facilite les audits internes et externes, permet de répondre aux demandes des autorités compétentes et contribue à l'amélioration continue du système de gestion des risques.

Les enseignements tirés des opérations suspectes détectées alimentent les programmes de formation, les évaluations des risques, les mises à jour des procédures internes ainsi que le renforcement des dispositifs de contrôle. AGCE International procède régulièrement à l'analyse des tendances observées, des nouveaux modes opératoires de fraude, des vulnérabilités identifiées et des évolutions réglementaires afin d'adapter en permanence son dispositif de conformité aux meilleures pratiques nationales et internationales.

Par l'application de ces principes, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme sa volonté de maintenir un environnement financier sûr, transparent et responsable, dans lequel chaque opération fait l'objet d'un niveau de vigilance approprié. Ce dispositif contribue à protéger les ressources confiées à l'Organisation, à préserver la confiance des membres, des donateurs, des partenaires, des bailleurs de fonds et des autorités publiques, tout en garantissant le respect des exigences de gouvernance, d'intégrité, de conformité réglementaire et de responsabilité institutionnelle qui fondent son action au service de l'intérêt général.

8.12 Critères d'identification

L'identification des opérations suspectes constitue une étape essentielle du dispositif de prévention mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** afin de lutter efficacement contre le blanchiment de capitaux, le financement du terrorisme, la fraude financière, la corruption et toute autre forme d'activité illicite. Les critères d'identification permettent d'évaluer objectivement chaque opération en tenant compte de son contexte, de sa cohérence économique, de son niveau de risque et de la qualité des informations disponibles. Ils ne visent pas à établir la preuve d'une infraction, mais à déterminer si une opération justifie un examen renforcé ou une investigation complémentaire.

L'Organisation applique une approche fondée sur les risques en prenant notamment en considération l'identité des personnes physiques ou morales impliquées, la nature de la relation entretenue avec l'Organisation, la qualité des informations d'identification fournies, l'origine et la destination des fonds, la cohérence entre le profil financier du membre, du donateur, du partenaire ou du prestataire et les montants concernés, ainsi que la justification économique, sociale, humanitaire ou institutionnelle de l'opération.

Les critères d'identification comprennent également l'analyse des montants exceptionnellement élevés, des opérations répétitives ou fractionnées, des paiements effectués selon des modalités inhabituelles, des transferts vers ou depuis des juridictions présentant un niveau de risque élevé, des changements fréquents de coordonnées bancaires, des demandes de remboursement atypiques, des dons anonymes lorsqu'ils ne sont pas autorisés, des refus de fournir les documents requis, des incohérences documentaires ou de toute autre situation susceptible de masquer l'identité réelle des personnes concernées ou l'origine effective des ressources.

Une vigilance particulière est exercée lorsque les opérations impliquent des personnes politiquement exposées (PPE), des organisations présentant une structure de propriété complexe, des partenaires récemment créés sans historique vérifiable, des intermédiaires insuffisamment identifiés, des bénéficiaires effectifs non clairement établis ou des personnes faisant l'objet de sanctions, de mesures restrictives ou de signalements publics. De même, toute opération incompatible avec les activités habituelles de l'Organisation ou dépourvue de justification raisonnable fait l'objet d'un contrôle renforcé.

L'identification repose sur la confrontation systématique des informations issues des procédures de connaissance des membres et partenaires (KYC), des documents justificatifs, des registres administratifs, des données comptables, des historiques de paiement, des conventions contractuelles, des systèmes d'information et des observations formulées par les responsables opérationnels. L'ensemble des éléments recueillis est évalué selon une approche globale permettant d'apprécier la réalité du risque avant toute décision.

Ces critères sont régulièrement révisés afin de tenir compte des évolutions réglementaires, des recommandations des autorités compétentes, des nouvelles typologies de fraude, des risques émergents liés aux technologies financières et des enseignements tirés des audits, des contrôles et des incidents enregistrés par l'Organisation.

8.13 Indicateurs d'alerte

Les **indicateurs d'alerte** constituent les signaux opérationnels permettant aux responsables de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** d'identifier rapidement les situations susceptibles de présenter un risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de ressources ou de cybercriminalité. Ils servent à déclencher des contrôles complémentaires sans préjuger du caractère illicite de l'opération concernée.

Les principaux indicateurs d'alerte comprennent notamment les paiements ou dons d'un montant inhabituellement élevé au regard du profil du contributeur, les opérations fractionnées réalisées dans le but apparent d'éviter les seuils de contrôle, les transferts internationaux dépourvus de justification économique ou humanitaire, les remboursements sollicités vers un compte bancaire différent de celui ayant servi au paiement initial, les modifications répétées des informations d'identification, les tentatives d'utilisation de plusieurs moyens de paiement pour une même opération, les paiements provenant de tiers non liés à la transaction ou les demandes accompagnées de documents manifestement incomplets, contradictoires ou falsifiés.

Des alertes peuvent également être générées lorsqu'un membre, un donateur, un partenaire ou un prestataire refuse de communiquer les informations requises dans le cadre des procédures de connaissance du client (KYC), fournit des explications incohérentes sur l'origine des fonds, cherche à accélérer de manière injustifiée le traitement d'une opération,

réalise des transactions incompatibles avec son activité habituelle ou présente des liens avec des juridictions faisant l'objet de mesures de vigilance renforcée.

Les systèmes d'information de l'Organisation peuvent produire automatiquement des alertes à partir de paramètres prédéfinis portant sur les montants, la fréquence des opérations, les anomalies de connexion, les changements de coordonnées bancaires, les tentatives d'accès non autorisées, les duplications de comptes utilisateurs, les écarts comptables ou les incohérences détectées entre les bases de données administratives, financières et comptables.

Chaque indicateur d'alerte est analysé individuellement et dans son contexte global. La présence d'un ou plusieurs indicateurs ne signifie pas nécessairement qu'une infraction a été commise ; elle impose toutefois une vigilance renforcée et peut conduire à des vérifications complémentaires, à une suspension temporaire de l'opération, à une enquête interne ou, lorsque les éléments recueillis le justifient, à un signalement conformément aux procédures prévues par la présente politique.

Les indicateurs d'alerte font l'objet d'une mise à jour régulière afin de prendre en compte l'évolution des risques, les nouvelles méthodes de fraude, les recommandations des autorités de supervision, les résultats des audits et les retours d'expérience de l'Organisation. Cette démarche d'amélioration continue permet à AGCE International de renforcer sa capacité de détection précoce, de protéger les ressources qui lui sont confiées et de maintenir un niveau élevé de conformité, de transparence et de sécurité dans l'ensemble de ses opérations financières et institutionnelles.

8.14 Analyse des opérations

L'**analyse des opérations** constitue une étape déterminante du dispositif de détection des opérations suspectes mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif d'évaluer de manière méthodique, impartiale et documentée toute opération présentant un niveau de risque susceptible de compromettre la conformité réglementaire, la sécurité financière ou l'intégrité institutionnelle de l'Organisation. Cette analyse permet de distinguer les opérations légitimes des situations nécessitant des investigations complémentaires, tout en garantissant le respect des principes de proportionnalité, de confidentialité, d'équité et de présomption de bonne foi.

Toute opération ayant fait l'objet d'une alerte, d'un contrôle renforcé ou d'un signalement interne est soumise à une analyse fondée sur une approche globale des risques. Cette analyse prend en considération l'identité des personnes physiques ou morales concernées, leur historique de relations avec l'Organisation, la nature de l'opération, son objet, son montant, la fréquence des transactions, le moyen de paiement utilisé, la provenance et la destination des fonds, les justificatifs fournis, la cohérence économique ou humanitaire de l'opération ainsi que les informations disponibles dans les registres administratifs, comptables et financiers.

Les responsables chargés de l'analyse procèdent à la vérification de l'ensemble des éléments susceptibles d'influencer l'appréciation du risque. Ils examinent notamment les documents d'identification, les contrats, les conventions, les justificatifs de paiement, les relevés bancaires, les autorisations internes, les correspondances, les historiques des transactions, les résultats des procédures de connaissance des membres et partenaires (KYC), ainsi que toute autre information utile permettant d'établir la légitimité de l'opération. Lorsque cela est nécessaire, des informations complémentaires peuvent être demandées aux personnes concernées ou auprès des partenaires financiers et des prestataires autorisés.

L'analyse repose également sur la confrontation des informations disponibles avec les critères de risque définis par l'Organisation. Une attention particulière est portée aux opérations inhabituelles, aux transactions fractionnées, aux mouvements financiers dépourvus de justification raisonnable, aux transferts internationaux sensibles, aux changements inexplicables de bénéficiaires, aux remboursements atypiques, aux opérations impliquant des personnes politiquement exposées (PPE), des juridictions à risque ou des structures juridiques complexes. Les incohérences identifiées sont évaluées dans leur contexte afin d'éviter toute interprétation erronée ou toute décision disproportionnée.

À l'issue de l'analyse, les responsables compétents établissent une évaluation motivée précisant le niveau de risque de l'opération, les éléments ayant conduit à cette appréciation, les investigations réalisées ainsi que les recommandations proposées. Selon les conclusions retenues, l'opération peut être validée, soumise à des contrôles complémentaires, suspendue temporairement, refusée, ou faire l'objet d'un signalement conformément aux procédures prévues par la présente politique et par les réglementations applicables.

Les analyses réalisées sont conduites dans des délais compatibles avec la nature des risques identifiés afin de limiter les conséquences financières, juridiques et réputationnelles susceptibles d'affecter l'Organisation. Elles participent également à l'amélioration continue du dispositif de conformité grâce à l'identification des nouvelles typologies de fraude, des vulnérabilités opérationnelles et des évolutions des risques auxquels AGCE International peut être exposée.

8.15 Documentation des investigations

La **documentation des investigations** constitue une exigence fondamentale du système de gouvernance, de conformité et de contrôle interne de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle garantit la traçabilité complète des analyses réalisées, des décisions prises et des mesures mises en œuvre dans le cadre du traitement des opérations suspectes. Cette documentation permet d'assurer la transparence des procédures, de démontrer le respect des obligations réglementaires et de faciliter les contrôles internes, les audits indépendants ainsi que les éventuelles demandes des autorités compétentes.

Toute investigation ouverte à la suite d'une alerte ou d'une opération présentant un risque fait l'objet d'un dossier spécifique contenant l'ensemble des informations utiles à la compréhension des faits. Ce dossier comprend notamment la description de l'opération concernée, les circonstances ayant conduit à son examen, les dates importantes, l'identité des personnes ou entités impliquées, les documents analysés, les vérifications effectuées, les échanges réalisés avec les parties concernées, les observations formulées par les responsables compétents ainsi que les conclusions de l'analyse.

Les investigations sont documentées de manière chronologique afin de reconstituer avec précision l'ensemble des actions entreprises depuis la détection initiale de l'anomalie jusqu'à la clôture définitive du dossier. Chaque intervention, décision, demande d'information complémentaire, mesure conservatoire, validation hiérarchique ou recommandation fait l'objet d'un enregistrement daté, signé ou validé selon les procédures internes applicables.

Les documents constituant le dossier d'investigation sont conservés sous format papier ou électronique dans des environnements sécurisés garantissant leur intégrité, leur disponibilité, leur confidentialité et leur valeur probante. L'accès à ces informations est strictement limité aux personnes habilitées dans le cadre de leurs fonctions et soumis aux règles relatives à la protection des données personnelles, au secret professionnel et à la confidentialité des investigations.

La documentation des investigations permet également d'alimenter les dispositifs d'analyse des risques, les programmes de formation, les audits internes, les évaluations de conformité et les actions d'amélioration continue. Les enseignements tirés des dossiers clôturés contribuent à renforcer les procédures de contrôle, à actualiser les indicateurs de risque et à adapter les mécanismes de surveillance aux nouvelles formes de criminalité financière et de fraude.

Lorsque les investigations aboutissent à un signalement auprès des autorités compétentes, à une mesure disciplinaire, à une action corrective ou à une décision de refus d'opération, l'ensemble des pièces justificatives et des éléments de motivation est conservé conformément aux délais de conservation documentaire définis par l'Organisation et aux exigences légales applicables.

Par cette politique de documentation rigoureuse, **AGCE International – AGCE Canada** garantit la fiabilité de son dispositif de conformité, renforce la sécurité juridique de ses décisions, protège les droits des personnes concernées et démontre sa volonté permanente d'assurer une gouvernance transparente, responsable et pleinement conforme aux meilleures pratiques internationales en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et la criminalité financière.

8.16 Décision de conformité

La **décision de conformité** constitue l'aboutissement du processus d'analyse des opérations présentant un risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de ressources ou de toute autre activité susceptible de compromettre la conformité réglementaire ou l'intégrité institutionnelle de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle consiste à statuer, de manière objective, motivée et documentée, sur la suite à réserver à une opération après examen des éléments recueillis dans le cadre des procédures de contrôle et d'investigation.

Toute décision de conformité repose sur une appréciation globale des faits, fondée sur les informations disponibles, les résultats des vérifications réalisées, les documents justificatifs, les évaluations de risques, les procédures de connaissance des membres et partenaires (KYC), les exigences réglementaires applicables ainsi que les politiques internes de gouvernance et de contrôle. Les décisions sont prises dans le respect des principes d'impartialité, de proportionnalité, de confidentialité, de traçabilité, de bonne foi et de responsabilité institutionnelle.

L'évaluation prend notamment en considération la nature de l'opération, son objet, son montant, son caractère habituel ou exceptionnel, l'identité des personnes concernées, l'origine et la destination des fonds, la cohérence économique ou humanitaire de la transaction, la qualité des justificatifs produits, les explications fournies par les parties concernées ainsi que les éventuels indicateurs de risque identifiés au cours de l'analyse. Lorsque plusieurs indices concordants laissent apparaître un risque élevé, une vigilance renforcée est appliquée avant toute décision définitive.

Selon les conclusions de l'analyse, plusieurs décisions peuvent être prises. L'opération peut être validée lorsqu'aucune anomalie significative n'est constatée et que les justificatifs fournis permettent d'établir sa régularité. Elle peut être validée sous réserve de mesures complémentaires, telles que la mise à jour des informations administratives, la production de documents additionnels, le renforcement des contrôles ou la mise sous surveillance renforcée de la relation avec la personne concernée.

Lorsque les éléments disponibles demeurent insuffisants ou contradictoires, l'Organisation peut suspendre temporairement l'opération afin de procéder à des investigations complémentaires. Cette suspension est limitée à la durée strictement nécessaire aux vérifications et s'effectue dans le respect des droits des personnes concernées ainsi que des exigences légales applicables.

Si les investigations mettent en évidence des risques incompatibles avec les exigences de conformité ou révèlent des indices sérieux d'activité illicite, AGCE International peut refuser l'opération, mettre fin à la relation concernée, suspendre certains services, résilier un partenariat ou engager les procédures de signalement prévues par la présente politique. Toute

décision défavorable est dûment motivée, documentée et conservée dans les registres de conformité de l'Organisation.

Les décisions de conformité sont prises par les responsables dûment habilités, conformément au principe de séparation des fonctions et, lorsque la sensibilité de l'opération l'exige, selon un mécanisme de validation collégiale ou de double approbation impliquant les responsables administratifs, financiers, juridiques ou de conformité. Les décisions sont enregistrées dans un registre sécurisé précisant leur date, leur fondement, les personnes ayant participé à leur validation ainsi que les mesures de suivi retenues.

Les décisions de conformité alimentent le dispositif d'amélioration continue de l'Organisation. Elles permettent d'actualiser les cartographies des risques, de renforcer les procédures internes, d'adapter les critères d'analyse et de perfectionner les programmes de formation afin d'améliorer durablement l'efficacité du système de prévention de la criminalité financière.

8.17 Signalement aux autorités compétentes

Le **signalement aux autorités compétentes** constitue une obligation essentielle du dispositif de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** lorsqu'une analyse objective fait apparaître des motifs raisonnables de soupçonner qu'une opération est susceptible d'être liée au blanchiment de capitaux, au financement du terrorisme, à la fraude, à la corruption, au détournement de ressources, à la cybercriminalité ou à toute autre infraction financière prévue par les législations applicables.

L'Organisation s'engage à coopérer pleinement avec les autorités administratives, judiciaires, fiscales, financières et les organismes de renseignement financier légalement compétents dans chacun des pays où elle exerce ses activités. Cette coopération est mise en œuvre dans le strict respect des lois nationales, des conventions internationales, des obligations de confidentialité, des règles relatives à la protection des données personnelles ainsi que des droits fondamentaux des personnes concernées.

Le signalement est précédé d'une analyse approfondie réalisée par les responsables de la conformité ou toute autre personne dûment habilitée. Cette analyse vise à vérifier la cohérence des faits, la qualité des éléments recueillis, la pertinence des indices identifiés et la conformité de la procédure avec les exigences légales et réglementaires. Le signalement repose sur un faisceau d'indices sérieux et concordants ; il n'exige pas la démonstration définitive d'une infraction pénale.

Les informations transmises aux autorités sont limitées aux éléments strictement nécessaires à l'exercice de leurs missions. Elles comprennent notamment la description des opérations concernées, les dates pertinentes, les montants en cause, les personnes ou entités impliquées, les justificatifs disponibles, les analyses réalisées par l'Organisation ainsi que toute

autre information utile à l'appréciation des faits. Chaque transmission est documentée et conservée conformément aux règles de conservation documentaire applicables.

Les personnes participant au processus de signalement sont tenues à une obligation stricte de confidentialité. Aucune information relative à un signalement ne peut être communiquée à des personnes non habilitées, et l'Organisation veille à prévenir toute divulgation susceptible de compromettre une enquête ou de porter atteinte aux droits des parties concernées. Les collaborateurs agissant de bonne foi dans le cadre d'un signalement bénéficient de la protection prévue par les politiques internes relatives aux lanceurs d'alerte et ne peuvent faire l'objet de représailles en raison de leur participation à la procédure.

À la suite d'un signalement, AGCE International assure un suivi rigoureux des mesures prises, des échanges avec les autorités compétentes et des décisions administratives ou judiciaires dont elle est informée dans les limites autorisées par la loi. Les enseignements tirés de ces situations sont intégrés aux évaluations des risques, aux audits, aux programmes de formation et aux procédures internes afin de renforcer en permanence le dispositif de prévention, de détection et de traitement des opérations suspectes.

Par cette politique de coopération responsable avec les autorités compétentes, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** réaffirme son engagement en faveur de la légalité, de la transparence, de l'intégrité institutionnelle et de la lutte active contre toutes les formes de criminalité financière, tout en contribuant à la protection des ressources qui lui sont confiées et à la préservation de la confiance de ses membres, partenaires, donateurs, bailleurs de fonds et bénéficiaires.

8.18 Archivage des dossiers

L'**archivage des dossiers** constitue une composante essentielle du dispositif de gouvernance, de conformité et de traçabilité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il garantit la conservation sécurisée, l'intégrité, la disponibilité et la confidentialité de l'ensemble des documents relatifs aux opérations financières, aux investigations, aux analyses de conformité, aux signalements, aux audits et aux décisions prises dans le cadre de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. L'archivage constitue une preuve de la diligence de l'Organisation dans l'exercice de ses obligations réglementaires et permet de démontrer, à tout moment, la conformité de ses procédures auprès des autorités compétentes, des partenaires institutionnels, des bailleurs de fonds, des auditeurs et des organismes de contrôle.

Tous les dossiers relatifs à la détection des opérations suspectes sont constitués de manière complète, organisée et chronologique. Ils regroupent notamment les alertes initiales, les rapports d'analyse, les documents d'identification, les justificatifs financiers, les échanges de correspondance, les comptes rendus d'investigation, les décisions de conformité, les autorisations hiérarchiques, les mesures conservatoires, les signalements éventuels aux

autorités compétentes ainsi que les actions correctives ou disciplinaires mises en œuvre. Chaque dossier doit permettre de reconstituer fidèlement le déroulement des faits et les décisions prises à chaque étape de la procédure.

L'Organisation applique des règles strictes de classement et de référencement afin d'assurer une identification rapide et fiable de chaque dossier. Les documents sont enregistrés selon un système normalisé comportant un numéro unique de référence, la date de création, la nature de l'affaire, le niveau de confidentialité, le responsable du dossier, le statut de traitement ainsi que les délais de conservation applicables. Cette organisation garantit la cohérence des archives et facilite les recherches lors des contrôles internes, des audits ou des demandes formulées par les autorités légalement habilitées.

Les archives peuvent être conservées sous format papier, électronique ou numérique, à condition que les dispositifs retenus garantissent leur authenticité, leur intégrité, leur lisibilité et leur disponibilité pendant toute la durée légale ou réglementaire de conservation. Les systèmes d'archivage électroniques utilisés par AGCE International intègrent des mécanismes de chiffrement, de sauvegarde régulière, de contrôle des accès, de journalisation des consultations, de protection contre les altérations, les suppressions non autorisées, les cyberattaques et toute perte accidentelle de données.

L'accès aux dossiers archivés est strictement réservé aux personnes dûment habilitées dans l'exercice de leurs fonctions. Les responsables de la conformité, les autorités de gouvernance, les auditeurs autorisés et, lorsque la loi l'exige, les autorités administratives ou judiciaires compétentes peuvent consulter les dossiers selon les procédures internes établies. Toute consultation, reproduction, modification, extraction ou communication d'un dossier fait l'objet d'une traçabilité complète permettant d'identifier la personne ayant accédé aux informations, la date de consultation ainsi que le motif de l'accès.

Les dossiers archivés demeurent soumis aux principes de confidentialité, de secret professionnel et de protection des données personnelles. Les informations qu'ils contiennent ne peuvent être utilisées qu'aux fins prévues par les lois applicables, les procédures internes de l'Organisation ou les demandes légalement formulées par les autorités compétentes. Toute divulgation, copie ou utilisation non autorisée d'informations confidentielles constitue un manquement grave susceptible d'entraîner des mesures disciplinaires, contractuelles ou judiciaires.

À l'expiration des délais de conservation prévus par la réglementation ou par les politiques internes de l'Organisation, les dossiers peuvent faire l'objet d'une destruction sécurisée après autorisation des responsables compétents et sous réserve de l'absence de procédure judiciaire, administrative, fiscale ou disciplinaire en cours. La destruction est réalisée selon des méthodes garantissant l'impossibilité de reconstituer les informations supprimées, qu'il s'agisse de documents papier ou de supports numériques. Un procès-verbal ou un registre de destruction est conservé afin d'assurer la traçabilité de cette opération.

AGCE International procède également à des revues périodiques de ses archives afin de vérifier leur intégrité, leur qualité, leur niveau de sécurité et leur conformité avec les exigences légales, réglementaires et institutionnelles. Ces contrôles permettent d'identifier les éventuelles insuffisances du système d'archivage, de renforcer les dispositifs de conservation et d'adapter les procédures aux évolutions technologiques, réglementaires et organisationnelles.

Par cette politique d'archivage rigoureuse, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** assure la pérennité de son patrimoine documentaire, renforce la fiabilité de son dispositif de conformité, facilite les contrôles internes et externes, protège les droits des personnes concernées et démontre son engagement permanent en faveur de la transparence, de la responsabilité, de la sécurité de l'information et de la bonne gouvernance conformément aux meilleures pratiques internationales en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme et la criminalité financière.

SECTION III

CONTRÔLE INTERNE

8.19 Double validation

La **double validation** constitue l'un des principes fondamentaux du système de contrôle interne de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle représente une mesure essentielle de gouvernance, de sécurité financière et de conformité destinée à prévenir les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, d'erreur administrative, de détournement de ressources, de corruption, d'abus de pouvoir et de conflits d'intérêts. En imposant l'intervention successive d'au moins deux personnes dûment habilitées dans le processus décisionnel, ce mécanisme renforce la fiabilité des opérations, améliore la qualité des contrôles et garantit une gestion responsable des ressources confiées à l'Organisation.

Le principe de la double validation s'applique à l'ensemble des opérations présentant un enjeu financier, juridique, administratif, informatique ou institutionnel significatif. Il concerne notamment les paiements, les virements bancaires, les remboursements, les transferts internationaux, les contrats, les conventions de partenariat, les achats, les engagements financiers, les subventions, les dons importants, les ouvertures ou fermetures de comptes, les modifications des coordonnées bancaires, les opérations de trésorerie, les accès aux systèmes d'information sensibles ainsi que toute autre décision identifiée comme présentant un niveau de risque élevé.

La première validation est réalisée par le responsable opérationnel ou le gestionnaire directement chargé du traitement de l'opération. Cette étape consiste à vérifier l'exactitude des

informations, la complétude du dossier, la conformité des documents justificatifs, le respect des procédures internes, la disponibilité des autorisations requises ainsi que la cohérence financière, administrative et réglementaire de l'opération concernée.

La seconde validation est effectuée par une autorité distincte disposant d'un niveau d'habilitation approprié et indépendante de l'auteur de la première validation. Ce contrôle complémentaire permet de confirmer la régularité de l'opération, de détecter d'éventuelles erreurs, incohérences ou anomalies, d'apprécier le niveau de risque résiduel et de s'assurer que la décision respecte les exigences de la présente Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT), les procédures internes de gouvernance ainsi que les obligations légales et réglementaires applicables.

Les personnes intervenant dans le processus de double validation doivent exercer leurs responsabilités avec impartialité, indépendance, diligence et confidentialité. Elles ne peuvent participer à la validation d'une opération lorsqu'elles présentent un intérêt personnel direct ou indirect susceptible de compromettre leur objectivité. En cas de conflit d'intérêts réel, apparent ou potentiel, la personne concernée est tenue de se récuser et d'en informer immédiatement sa hiérarchie afin qu'un autre responsable habilité soit désigné.

Lorsque des divergences apparaissent entre les deux niveaux de validation, l'opération est suspendue jusqu'à ce que les vérifications complémentaires nécessaires soient réalisées. Selon la nature de l'opération et le niveau de risque identifié, le dossier peut être transmis au Responsable de la Conformité, au Responsable Financier, au Président Général, au Comité de Gouvernance ou à toute autre autorité compétente désignée par l'Organisation pour décision. Aucune opération ne peut être exécutée tant que les désaccords n'ont pas été résolus et que toutes les validations requises n'ont pas été obtenues.

L'ensemble du processus de double validation fait l'objet d'une traçabilité complète. Les identités des validateurs, les dates et heures de validation, les observations formulées, les documents examinés, les décisions prises ainsi que les éventuelles réserves ou recommandations sont enregistrés dans les systèmes administratifs, financiers ou numériques de l'Organisation. Ces informations sont conservées conformément aux règles de conservation documentaire et demeurent disponibles pour les besoins des audits internes, des contrôles externes et des inspections des autorités compétentes.

Afin de renforcer l'efficacité de ce dispositif, AGCE International peut recourir à des mécanismes de validation électronique sécurisée intégrant l'authentification multifacteur, la signature électronique, la journalisation des actions, le contrôle des habilitations et la conservation horodatée des preuves de validation. Ces outils garantissent l'intégrité des décisions, limitent les risques de falsification et améliorent la traçabilité des processus de contrôle.

La procédure de double validation est régulièrement évaluée dans le cadre des audits internes, des revues de conformité et des contrôles de gouvernance. Les résultats de ces évaluations permettent d'identifier les éventuelles insuffisances du dispositif, d'adapter les

niveaux d'autorisation, de renforcer les procédures opérationnelles et de prendre en compte les évolutions réglementaires, technologiques et organisationnelles.

Par l'application systématique du principe de la double validation, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme son engagement en faveur d'une gouvernance rigoureuse, d'une transparence financière exemplaire, d'une gestion prudente des risques et d'une conformité permanente aux meilleures pratiques nationales et internationales en matière de contrôle interne, de lutte contre le blanchiment de capitaux, de prévention du financement du terrorisme et de protection des ressources destinées à ses missions humanitaires, sociales, éducatives, sanitaires, environnementales, économiques et numériques.

8.20 Séparation des responsabilités

La **séparation des responsabilités** constitue un principe fondamental du dispositif de contrôle interne de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle vise à garantir qu'aucune personne ne puisse, à elle seule, initier, autoriser, exécuter, enregistrer, contrôler et clôturer une même opération financière, administrative, informatique ou institutionnelle. Ce principe constitue un rempart essentiel contre les risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de ressources, de manipulation comptable, d'erreur opérationnelle et de conflit d'intérêts.

L'Organisation organise ses processus de manière à répartir les responsabilités entre plusieurs intervenants disposant de compétences et d'habilitations distinctes. Chaque acteur intervient dans la limite de ses fonctions, selon des procédures clairement définies et documentées. Cette organisation favorise la transparence, la redevabilité, la fiabilité des décisions et la prévention des abus de pouvoir.

Les fonctions d'initiation, de vérification, d'autorisation, d'exécution, d'enregistrement comptable, de contrôle, de supervision et d'audit sont attribuées à des personnes différentes lorsque la nature ou le niveau de risque de l'opération le justifie. Cette séparation s'applique notamment aux paiements, aux transferts internationaux, aux remboursements, aux opérations de trésorerie, aux contrats, aux achats, aux conventions de partenariat, aux subventions, aux dons, aux mouvements bancaires, aux modifications de données sensibles ainsi qu'aux accès aux systèmes d'information.

Les responsabilités sont définies dans les fiches de poste, les délégations de pouvoir, les procédures internes et les matrices d'habilitation de l'Organisation. Chaque collaborateur connaît précisément l'étendue de ses attributions, ses limites décisionnelles ainsi que les contrôles auxquels il est soumis. Toute délégation de compétence est formalisée par écrit, limitée dans son objet et sa durée, et régulièrement réexaminée afin de garantir son adéquation avec les besoins de l'Organisation.

Afin d'éviter toute situation de conflit d'intérêts, les personnes exerçant une responsabilité décisionnelle sont tenues de déclarer toute situation susceptible d'affecter leur indépendance ou leur impartialité. Lorsqu'un conflit d'intérêts réel, apparent ou potentiel est identifié, la personne concernée s'abstient de participer au traitement de l'opération et informe immédiatement son supérieur hiérarchique afin qu'une autre personne habilitée soit désignée.

Les systèmes d'information de l'Organisation intègrent également ce principe en limitant les droits d'accès selon les fonctions exercées. Les habilitations informatiques sont attribuées sur le principe du moindre privilège, régulièrement révisées et supprimées dès qu'elles ne sont plus justifiées. Toute création, modification ou suppression de droits d'accès est soumise à une procédure d'autorisation et à une traçabilité complète.

La séparation des responsabilités fait l'objet de contrôles réguliers dans le cadre des audits internes, des revues de conformité et des évaluations des risques. Toute dérogation exceptionnelle doit être dûment justifiée, approuvée par l'autorité compétente et accompagnée de mesures compensatoires destinées à maintenir un niveau de contrôle suffisant.

Par l'application rigoureuse de ce principe, AGCE International renforce la sécurité de ses opérations, protège les ressources qui lui sont confiées, améliore la qualité de sa gouvernance et garantit une conformité permanente aux exigences nationales et internationales applicables aux organisations à but non lucratif.

8.21 Contrôle hiérarchique

Le **contrôle hiérarchique** constitue un mécanisme permanent de supervision permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** d'assurer le respect des procédures internes, des obligations réglementaires et des principes de bonne gouvernance dans l'ensemble de ses activités. Il garantit que chaque niveau de responsabilité exerce une surveillance effective des opérations réalisées sous son autorité et contribue à la prévention des risques financiers, administratifs, opérationnels et technologiques.

Le contrôle hiérarchique repose sur une chaîne claire de responsabilités dans laquelle chaque supérieur est chargé de superviser les activités de ses collaborateurs, de vérifier la conformité des opérations, d'apprécier les risques associés et de s'assurer du respect des politiques, procédures et délégations de pouvoir en vigueur. Cette supervision s'exerce de manière continue et proportionnée au niveau de risque des activités concernées.

Les responsables hiérarchiques vérifient notamment la qualité des dossiers, la régularité des pièces justificatives, la conformité des autorisations, la cohérence des écritures comptables, l'exécution correcte des paiements, le respect des budgets, l'application des procédures de connaissance des membres et partenaires (KYC), ainsi que la mise en œuvre des mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Le contrôle hiérarchique comprend également l'examen régulier des indicateurs de performance, des rapports financiers, des tableaux de bord de conformité, des journaux d'événements, des alertes générées par les systèmes d'information et des recommandations formulées à l'issue des audits internes ou externes. Ces éléments permettent d'identifier rapidement les anomalies, les insuffisances organisationnelles ou les risques émergents nécessitant une intervention.

Lorsqu'une irrégularité est constatée, le responsable hiérarchique prend les mesures appropriées en fonction de la nature et de la gravité des faits. Il peut demander des explications complémentaires, suspendre temporairement une opération, renforcer les contrôles, prescrire des actions correctives, saisir le Responsable de la Conformité ou transmettre le dossier aux instances compétentes lorsque la situation l'exige. Toutes les décisions prises dans ce cadre sont documentées et conservées afin d'assurer leur traçabilité.

Les responsables hiérarchiques ont également pour mission d'accompagner leurs équipes dans l'application des règles de conformité, de promouvoir une culture de transparence et d'intégrité, d'organiser la diffusion des procédures internes et de veiller au maintien des compétences professionnelles grâce à des actions régulières de formation et de sensibilisation.

Le dispositif de contrôle hiérarchique fait l'objet d'une évaluation périodique afin de mesurer son efficacité, d'identifier les axes d'amélioration et d'adapter les modalités de supervision aux évolutions réglementaires, organisationnelles et technologiques. Les résultats de ces évaluations alimentent le système d'amélioration continue de l'Organisation et contribuent au renforcement de son dispositif global de gouvernance.

Par la mise en œuvre d'un contrôle hiérarchique structuré, documenté et permanent, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** assure une surveillance efficace de ses activités, favorise une prise de décision responsable, réduit les risques de non-conformité et consolide la confiance de ses membres, partenaires, donateurs, bailleurs de fonds et autorités de contrôle dans la qualité de sa gouvernance institutionnelle.

8.22 Revue périodique

La **revue périodique** constitue un mécanisme essentiel du dispositif de contrôle interne de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle permet d'évaluer de manière régulière l'efficacité, la pertinence et la conformité des procédures administratives, financières, comptables, opérationnelles, numériques et institutionnelles mises en œuvre dans le cadre de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**. Son objectif est de garantir que les dispositifs de prévention, de détection, de contrôle et de surveillance demeurent adaptés à l'évolution des risques, des activités de l'Organisation et des exigences réglementaires nationales et internationales.

La revue périodique repose sur une approche systématique et documentée couvrant l'ensemble des processus sensibles de l'Organisation. Elle porte notamment sur les adhésions, les cotisations, les abonnements, les dons, les paiements, les remboursements, les transferts internationaux, les conventions de partenariat, les achats, les opérations de trésorerie, les systèmes d'information, les procédures de connaissance des membres et partenaires (KYC), les dispositifs de sécurité informatique ainsi que les mécanismes de contrôle interne.

Chaque revue consiste à examiner la conformité des opérations réalisées, la qualité des pièces justificatives, le respect des procédures internes, l'efficacité des contrôles mis en œuvre, la pertinence des niveaux d'autorisation, la fiabilité des données financières, la cohérence des enregistrements comptables ainsi que le fonctionnement des systèmes de surveillance automatisés. Les responsables compétents évaluent également les écarts constatés, les incidents enregistrés, les alertes générées, les recommandations formulées lors des audits précédents et les actions correctives effectivement mises en œuvre.

Les revues sont réalisées selon une fréquence adaptée à la nature des activités, au niveau de risque des opérations et aux exigences de gouvernance de l'Organisation. Elles peuvent être mensuelles, trimestrielles, semestrielles ou annuelles, sans préjudice des revues exceptionnelles pouvant être décidées à la suite d'un incident majeur, d'une évolution réglementaire, d'un changement organisationnel ou d'un signalement particulier.

À l'issue de chaque revue, un rapport est établi précisant les contrôles réalisés, les constats effectués, les non-conformités identifiées, les risques résiduels, les recommandations proposées ainsi que les mesures correctives à engager. Ces rapports sont transmis aux responsables concernés, au Responsable de la Conformité, au Responsable Financier, à la Direction Générale ou aux organes de gouvernance compétents selon la nature des observations formulées.

Les résultats des revues périodiques alimentent le processus d'amélioration continue de l'Organisation. Ils permettent de mettre à jour les cartographies des risques, d'adapter les procédures internes, de renforcer les contrôles, d'améliorer les outils numériques, d'actualiser les programmes de formation et de consolider la culture de conformité au sein de l'ensemble des structures d'AGCE International.

Par ce mécanisme de revue périodique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** s'assure que son système de contrôle interne demeure performant, évolutif et pleinement conforme aux meilleures pratiques internationales de gouvernance, de transparence, de gestion des risques et de lutte contre le blanchiment de capitaux ainsi que le financement du terrorisme.

8.23 Contrôle permanent

Le **contrôle permanent** constitue le premier niveau de maîtrise des risques au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International –**

AGCE Canada). Il repose sur une surveillance continue des activités, des opérations financières, des processus administratifs, des systèmes d'information et des décisions institutionnelles afin de garantir le respect permanent des règles de gouvernance, des obligations réglementaires et des exigences de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**.

Contrairement aux contrôles ponctuels ou aux audits périodiques, le contrôle permanent est intégré aux activités quotidiennes de l'Organisation. Chaque responsable opérationnel est tenu d'exercer une vigilance constante sur les opérations relevant de son domaine de compétence et de vérifier, en temps réel, leur conformité aux procédures internes, aux délégations de pouvoir, aux budgets autorisés, aux règles comptables et aux dispositifs de sécurité en vigueur.

Le contrôle permanent couvre notamment la réception et la validation des paiements, les cotisations, les adhésions, les abonnements, les dons, les remboursements, les transferts internationaux, les achats, les engagements financiers, les conventions de partenariat, les opérations bancaires, les accès aux systèmes d'information, la gestion documentaire ainsi que les procédures de connaissance des membres, partenaires et bénéficiaires.

Ce dispositif s'appuie sur des contrôles manuels et automatisés, des tableaux de bord de suivi, des rapprochements comptables, des systèmes d'alertes, des indicateurs de performance, des journaux d'événements, des vérifications documentaires, des contrôles de cohérence et des mécanismes de surveillance numérique permettant d'identifier rapidement toute anomalie ou tout risque émergent.

Lorsqu'une irrégularité est détectée, les responsables compétents prennent immédiatement les mesures nécessaires afin de limiter les conséquences de l'incident. Selon la gravité des faits, ces mesures peuvent comprendre la suspension d'une opération, la réalisation de contrôles complémentaires, la correction des erreurs constatées, la mise en œuvre d'actions préventives, le renforcement des procédures ou la transmission du dossier au Responsable de la Conformité ou aux organes compétents de gouvernance.

Le contrôle permanent repose également sur une documentation continue des opérations réalisées. Chaque contrôle effectué, chaque anomalie identifiée, chaque décision prise et chaque action corrective mise en œuvre est enregistrée dans les systèmes de gestion de l'Organisation afin de garantir une traçabilité complète et de faciliter les contrôles hiérarchiques, les audits internes, les audits externes et les inspections des autorités compétentes.

Afin d'assurer son efficacité, le dispositif de contrôle permanent fait l'objet d'une évaluation régulière. Les enseignements tirés des incidents, des audits, des revues périodiques, des signalements internes, des évolutions réglementaires et des nouvelles menaces permettent d'améliorer continuellement les procédures de surveillance, les outils numériques, les indicateurs de risque et les mécanismes de prévention.

Par la mise en œuvre d'un contrôle permanent, structuré, documenté et fondé sur une approche basée sur les risques, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit une surveillance quotidienne de ses activités, protège les ressources qui lui sont confiées, renforce la fiabilité de ses opérations et consolide une gouvernance exemplaire reposant sur la transparence, la responsabilité, l'intégrité et la conformité aux meilleures pratiques internationales.

8.24 Journal des opérations

Le **journal des opérations** constitue un instrument essentiel de traçabilité, de transparence et de gouvernance au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il représente le registre officiel dans lequel sont consignées, de manière chronologique, exhaustive, sécurisée et inaltérable, toutes les opérations financières, administratives, comptables, numériques et institutionnelles réalisées dans le cadre des activités de l'Organisation. Ce dispositif permet de garantir la reconstitution fidèle des événements, de faciliter les contrôles internes et externes, de renforcer la prévention des risques et de démontrer le respect des exigences de la présente **Politique de Lutte contre le Blanchiment de Capitaux et le Financement du Terrorisme (LBC/FT)**.

Le journal des opérations couvre l'ensemble des transactions et événements présentant un intérêt pour la gouvernance et la conformité. Il comprend notamment les adhésions, les cotisations, les abonnements, les dons, les paiements, les remboursements, les transferts nationaux et internationaux, les opérations bancaires, les achats, les conventions, les engagements financiers, les modifications des données sensibles, les créations ou suppressions de comptes utilisateurs, les validations hiérarchiques, les alertes de conformité, les investigations, les décisions prises ainsi que les interventions techniques effectuées sur les systèmes d'information.

Chaque enregistrement comporte des informations précises permettant d'assurer une parfaite traçabilité des opérations. Sont notamment consignés la date et l'heure de l'événement, l'identité de l'utilisateur ou du responsable ayant initié ou validé l'opération, la nature de l'action réalisée, les montants concernés, les références des documents justificatifs, les systèmes utilisés, les autorisations obtenues, les observations éventuelles ainsi que le résultat final de l'opération. Les journaux électroniques doivent intégrer des mécanismes d'horodatage sécurisé, d'authentification des utilisateurs et de conservation des preuves numériques.

Les journaux des opérations sont protégés contre toute modification, suppression ou altération non autorisée. Ils sont conservés dans des environnements sécurisés bénéficiant de dispositifs de sauvegarde régulière, de chiffrement, de contrôle des accès, de journalisation des consultations et de protection contre les cyberattaques. Les droits d'accès sont limités aux seules personnes habilitées dans le cadre de leurs fonctions, conformément aux principes de confidentialité, de protection des données personnelles et de séparation des responsabilités.

Le journal des opérations constitue un outil permanent d'analyse et de supervision. Les responsables de la conformité, les responsables financiers, les auditeurs internes et les organes de gouvernance procèdent à des examens réguliers des journaux afin d'identifier les anomalies, les comportements inhabituels, les tentatives d'accès non autorisées, les erreurs opérationnelles ou toute situation susceptible de présenter un risque pour l'Organisation. Les informations issues de ces analyses alimentent les cartographies des risques, les dispositifs de contrôle permanent, les audits et les programmes d'amélioration continue.

Les journaux sont conservés pendant la durée prévue par les politiques de conservation documentaire de l'Organisation et par les réglementations applicables. Ils demeurent disponibles pour les besoins des contrôles internes, des audits externes, des inspections réglementaires et des investigations judiciaires ou administratives lorsque celles-ci sont légalement requises.

Par la mise en œuvre d'un système rigoureux de journalisation, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit la fiabilité de ses opérations, renforce la transparence de sa gouvernance, facilite la détection des risques et assure une conformité permanente aux meilleures pratiques internationales en matière de contrôle interne et de lutte contre la criminalité financière.

8.25 Audit interne

L'**audit interne** constitue un mécanisme indépendant et permanent d'évaluation du dispositif de gouvernance, de gestion des risques, de contrôle interne et de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour mission de fournir aux organes dirigeants une assurance raisonnable sur l'efficacité des procédures mises en œuvre afin de prévenir le blanchiment de capitaux, le financement du terrorisme, la fraude, la corruption, les erreurs de gestion, les cybermenaces et toute autre situation susceptible d'affecter les intérêts de l'Organisation.

L'audit interne est exercé en toute indépendance fonctionnelle, dans le respect des principes d'objectivité, d'impartialité, de confidentialité, d'intégrité et de compétence professionnelle. Les auditeurs internes disposent d'un accès aux informations, documents, systèmes et responsables nécessaires à l'accomplissement de leurs missions, sous réserve des règles relatives à la protection des données et au secret professionnel.

Les missions d'audit portent sur l'ensemble des activités de l'Organisation, notamment les procédures d'adhésion, les cotisations, les abonnements, les dons, les paiements, les remboursements, les transferts internationaux, la gestion des projets, la trésorerie, les achats, les contrats, les partenariats, les systèmes d'information, les dispositifs de sécurité informatique, les procédures KYC, les contrôles LBC/FT, la gestion documentaire ainsi que les mécanismes de gouvernance institutionnelle.

Les auditeurs évaluent la conformité des opérations aux politiques internes, aux délégations de pouvoir, aux obligations légales, aux procédures comptables et financières ainsi qu'aux exigences de la présente politique. Ils vérifient également l'efficacité des contrôles permanents, la pertinence des dispositifs de surveillance, la qualité des informations financières, la fiabilité des systèmes de gestion, le respect de la séparation des responsabilités et l'application des recommandations formulées lors des audits précédents.

Chaque mission donne lieu à un rapport d'audit détaillé présentant les objectifs de la mission, la méthodologie utilisée, les constats réalisés, les risques identifiés, leur niveau de criticité, les non-conformités observées, les recommandations d'amélioration ainsi que les plans d'actions correctifs proposés. Ces rapports sont transmis aux responsables concernés, au Responsable de la Conformité, au Responsable Financier, à la Direction Générale et aux organes de gouvernance compétents pour examen et suivi.

L'Organisation assure un suivi systématique de la mise en œuvre des recommandations issues des audits internes. Des revues de suivi sont réalisées afin de vérifier l'exécution effective des mesures correctives, d'évaluer leur efficacité et d'identifier les actions complémentaires éventuellement nécessaires. Les résultats de ces suivis alimentent le processus d'amélioration continue et contribuent au renforcement permanent du dispositif de contrôle interne.

Par son caractère indépendant, méthodique et fondé sur une approche basée sur les risques, l'audit interne constitue un levier stratégique de bonne gouvernance pour **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il favorise une gestion responsable des ressources, améliore la qualité des décisions, renforce la confiance des membres, partenaires, donateurs, bailleurs de fonds et autorités publiques, et contribue durablement à la transparence, à la performance institutionnelle et à la conformité de l'Organisation avec les meilleures pratiques internationales.

8.26 Audit externe

L'**audit externe** constitue un mécanisme indépendant de contrôle, d'évaluation et de vérification destiné à apprécier la conformité, la transparence, la sincérité et l'efficacité des dispositifs de gouvernance, de gestion financière, de contrôle interne et de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il complète les dispositifs de contrôle interne et d'audit interne en apportant une appréciation impartiale réalisée par des professionnels ou organismes indépendants de l'Organisation. Son objectif est de renforcer la confiance des membres, partenaires, bailleurs de fonds, donateurs, institutions financières, autorités publiques et autres parties prenantes dans la qualité de la gestion institutionnelle et financière de l'Organisation.

L'audit externe est réalisé par des cabinets d'audit, des commissaires aux comptes, des experts indépendants, des organismes de certification, des autorités de contrôle ou toute autre entité légalement habilitée à exercer des missions de vérification. Les auditeurs externes

interviennent dans le respect des principes d'indépendance, d'impartialité, d'intégrité, de confidentialité, de compétence professionnelle et d'objectivité, conformément aux normes professionnelles, aux dispositions légales applicables et aux exigences des partenaires institutionnels ou des bailleurs de fonds.

Les missions d'audit externe peuvent être programmées de manière périodique, exigées par une disposition réglementaire, sollicitées par les organes dirigeants de l'Organisation ou demandées dans le cadre d'une convention de financement, d'un partenariat stratégique, d'un projet spécifique ou d'une procédure de certification. Des audits extraordinaires peuvent également être organisés lorsqu'un événement exceptionnel, une suspicion de fraude, une alerte de conformité, une évolution réglementaire ou un risque majeur le justifie.

L'audit externe couvre l'ensemble des activités, des ressources et des dispositifs de gouvernance de l'Organisation. Il porte notamment sur la gestion financière et comptable, les états financiers, les procédures budgétaires, les mécanismes de contrôle interne, les opérations bancaires, les adhésions, les cotisations, les abonnements, les dons, les paiements, les remboursements, les transferts internationaux, les achats, les conventions de partenariat, les systèmes d'information, la cybersécurité, les procédures de connaissance des membres, partenaires et bénéficiaires (KYC), les mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), la protection des données personnelles ainsi que le respect des politiques institutionnelles et des obligations légales.

Les auditeurs externes disposent, dans le respect des lois applicables et des engagements de confidentialité, d'un accès aux documents, registres, pièces justificatives, systèmes d'information, rapports, contrats et informations nécessaires à l'accomplissement de leur mission. L'ensemble des responsables, collaborateurs, bénévoles et représentants de l'Organisation est tenu de coopérer pleinement avec les auditeurs, de fournir des informations exactes, complètes et sincères, et de faciliter l'exécution des travaux de vérification.

À l'issue de chaque mission, les auditeurs établissent un rapport détaillé présentant les objectifs de l'audit, la méthodologie employée, les travaux réalisés, les constats observés, les risques identifiés, les éventuelles non-conformités relevées, les recommandations formulées ainsi que, le cas échéant, une opinion sur la fiabilité des informations financières, l'efficacité du dispositif de contrôle interne et le niveau de conformité de l'Organisation. Ces rapports sont examinés par les organes de gouvernance compétents afin de déterminer les actions correctives, préventives ou organisationnelles à mettre en œuvre.

AGCE International assure un suivi rigoureux de l'ensemble des recommandations formulées à l'occasion des audits externes. Chaque observation fait l'objet d'un plan d'action précisant les mesures correctives retenues, les responsables désignés, les ressources nécessaires, les échéances de mise en œuvre ainsi que les modalités de suivi et d'évaluation. L'état d'avancement de ces actions est régulièrement présenté aux instances dirigeantes afin de garantir leur exécution effective et d'améliorer en permanence le niveau de maîtrise des risques.

Les résultats des audits externes alimentent le processus d'amélioration continue de l'Organisation. Ils contribuent à l'actualisation des politiques internes, au renforcement des procédures de contrôle, à l'amélioration des systèmes d'information, au développement des compétences des collaborateurs, à l'évolution des dispositifs de gestion des risques et à l'adaptation des mécanismes de conformité aux évolutions législatives, réglementaires, technologiques et institutionnelles.

L'Organisation veille également à préserver l'indépendance des auditeurs externes en évitant toute situation susceptible de compromettre leur objectivité. Aucune pression, influence ou intervention ne peut être exercée sur les travaux d'audit, leurs conclusions ou leurs recommandations. Les auditeurs bénéficient de toutes les garanties nécessaires à l'accomplissement de leur mission dans le respect des règles déontologiques applicables à leur profession.

Par la mise en œuvre d'un dispositif d'audit externe régulier, transparent et indépendant, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce la crédibilité de sa gouvernance, garantit une utilisation responsable des ressources qui lui sont confiées, consolide la confiance de ses partenaires institutionnels et financiers, démontre son engagement permanent en faveur de la transparence, de la redevabilité et de la bonne gouvernance, et confirme sa conformité aux meilleures pratiques internationales en matière de gestion des organisations à but non lucratif, de lutte contre le blanchiment de capitaux, de prévention du financement du terrorisme et de protection de l'intégrité financière.

SECTION IV

SÉCURITÉ DES PAIEMENTS

8.27 Politique de sécurité des paiements

La **Politique de sécurité des paiements** constitue l'un des piliers fondamentaux du dispositif de gouvernance financière de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif d'assurer la protection, l'intégrité, la confidentialité, la disponibilité et la traçabilité de l'ensemble des opérations de paiement réalisées par ou au bénéfice de l'Organisation. Cette politique vise à prévenir les risques de blanchiment de capitaux, de financement du terrorisme, de fraude financière, d'usurpation d'identité, de cybercriminalité, de corruption, de détournement de fonds, d'accès non autorisé aux systèmes de paiement et de toute autre atteinte susceptible de compromettre la sécurité des ressources financières confiées à l'Organisation.

La présente politique s'applique à l'ensemble des moyens de paiement utilisés par AGCE International, notamment les virements bancaires nationaux et internationaux, les cartes bancaires, les plateformes de paiement électronique, les portefeuilles numériques, les

paiements mobiles, les passerelles de paiement sécurisées, les solutions de collecte de dons en ligne, les paiements par codes QR ainsi que tout autre instrument financier autorisé par l'Organisation. Elle couvre également les paiements effectués par les membres, partenaires, donateurs, bailleurs de fonds, bénéficiaires, fournisseurs, prestataires et représentants habilités.

Toutes les opérations de paiement doivent être réalisées conformément aux procédures internes de gouvernance financière, aux politiques de contrôle interne, aux règles de séparation des responsabilités, aux mécanismes de double validation, aux exigences de connaissance des membres et partenaires (KYC), aux mesures de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) ainsi qu'aux lois et réglementations applicables dans les pays où l'Organisation exerce ses activités.

Avant toute exécution d'un paiement, une vérification préalable est réalisée afin de confirmer l'identité des parties concernées, la validité des coordonnées bancaires ou des comptes de paiement, la légitimité de l'opération, la disponibilité des autorisations nécessaires, l'existence des pièces justificatives requises ainsi que la conformité du paiement avec les objectifs institutionnels de l'Organisation. Toute anomalie, incohérence ou suspicion de fraude entraîne la suspension immédiate de l'opération jusqu'à la réalisation des vérifications complémentaires.

L'Organisation met en œuvre des mesures techniques et organisationnelles destinées à garantir un niveau élevé de sécurité des paiements. Ces mesures comprennent notamment le chiffrement des données financières, l'authentification multifacteur, la signature électronique sécurisée, la gestion rigoureuse des habilitations, la segmentation des accès, la journalisation des opérations, les sauvegardes régulières, les mécanismes de détection des comportements anormaux, les dispositifs de surveillance en temps réel ainsi que les protections contre les cyberattaques, les logiciels malveillants, le hameçonnage (phishing) et les tentatives d'intrusion.

Les plateformes et prestataires de paiement sélectionnés par AGCE International doivent répondre à des exigences élevées de sécurité, de conformité réglementaire et de protection des données. L'Organisation privilégie des partenaires financiers reconnus disposant de mécanismes robustes de prévention de la fraude, de gestion des risques, de surveillance des transactions et de conformité aux normes internationales applicables aux services de paiement électronique. Une évaluation régulière de ces prestataires est réalisée afin de vérifier le maintien de leur niveau de sécurité et de fiabilité.

Chaque opération de paiement fait l'objet d'une traçabilité complète. Les informations relatives aux montants, aux bénéficiaires, aux références des transactions, aux validations obtenues, aux justificatifs associés, aux dates d'exécution et aux responsables ayant participé au processus sont enregistrées dans les systèmes d'information sécurisés de l'Organisation. Ces données sont conservées conformément aux politiques d'archivage documentaire et peuvent être consultées dans le cadre des contrôles internes, des audits ou des demandes légalement formulées par les autorités compétentes.

En cas d'incident de sécurité, de tentative de fraude, d'accès non autorisé, de compromission des systèmes de paiement ou de suspicion d'opération illicite, des procédures d'urgence sont immédiatement déclenchées. Elles peuvent comprendre la suspension des paiements concernés, le blocage des accès, la sécurisation des comptes, l'ouverture d'une enquête interne, la notification des prestataires concernés, la conservation des preuves numériques ainsi que, lorsque la réglementation l'impose, le signalement aux autorités compétentes.

La sensibilisation des collaborateurs, bénévoles, représentants, membres et partenaires constitue un élément essentiel de cette politique. Des actions régulières d'information et de formation sont organisées afin de promouvoir les bonnes pratiques en matière de sécurité des paiements, de prévention de la fraude, de cybersécurité, de protection des données financières et de conformité aux obligations légales et réglementaires.

La Politique de sécurité des paiements fait l'objet d'une révision périodique afin de tenir compte des évolutions technologiques, des nouvelles menaces, des exigences réglementaires, des recommandations des auditeurs et des meilleures pratiques internationales. Les procédures, outils et contrôles sont adaptés en permanence afin de maintenir un niveau élevé de protection des actifs financiers de l'Organisation.

Par la mise en œuvre de cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme son engagement à garantir des paiements fiables, transparents et sécurisés, à protéger les ressources confiées par ses membres, partenaires, donateurs et bailleurs de fonds, à renforcer la confiance de l'ensemble de ses parties prenantes et à assurer une conformité permanente avec les meilleures pratiques internationales en matière de sécurité financière, de gestion des risques, de gouvernance institutionnelle et de lutte contre le blanchiment de capitaux ainsi que le financement du terrorisme.

8.28 Paiements PayPal

Les **paiements effectués par l'intermédiaire de la plateforme PayPal** constituent l'un des moyens de collecte et de règlement autorisés par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** pour recevoir les cotisations, adhésions, abonnements, dons, contributions volontaires, paiements de services, inscriptions aux événements, achats de produits numériques ainsi que toute autre opération financière approuvée par l'Organisation. L'utilisation de cette plateforme s'inscrit dans le respect des principes de transparence, de sécurité financière, de conformité réglementaire et de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

L'Organisation veille à ce que tous les comptes PayPal utilisés soient officiellement enregistrés, administrés par des personnes dûment habilitées et protégés par des mécanismes de sécurité renforcés. Les accès aux comptes sont strictement limités aux responsables autorisés selon le principe du moindre privilège. L'authentification multifacteur, les mots de

passes robustes, la gestion sécurisée des identifiants et la révision régulière des habilitations sont obligatoires afin de prévenir tout accès frauduleux ou non autorisé.

Avant l'acceptation d'un paiement réalisé via PayPal, AGCE International met en œuvre les procédures nécessaires de vérification de l'identité du payeur lorsque la réglementation, le niveau de risque ou la nature de l'opération l'exigent. Les informations relatives au titulaire du paiement, au montant, à la devise, au motif de la transaction, à la date, au numéro de référence ainsi qu'aux justificatifs associés sont enregistrées dans les systèmes de gestion de l'Organisation afin d'assurer une traçabilité complète.

Les paiements PayPal font l'objet d'une surveillance permanente destinée à détecter toute anomalie, opération inhabituelle, tentative de fraude, paiement fractionné, utilisation abusive d'un compte, activité suspecte ou transaction incompatible avec les objectifs institutionnels de l'Organisation. Les alertes générées par les systèmes de contrôle ou signalées par PayPal sont immédiatement analysées par les responsables compétents. Lorsque cela est nécessaire, les opérations peuvent être suspendues, vérifiées, refusées ou signalées conformément aux procédures internes et aux obligations légales applicables.

Toutes les opérations réalisées par l'intermédiaire de PayPal sont rapprochées périodiquement avec les relevés financiers, les registres comptables et les justificatifs de paiement afin de garantir leur exactitude, leur exhaustivité et leur conformité. Les éventuels écarts constatés donnent lieu à des investigations documentées et à la mise en œuvre des mesures correctives appropriées.

Les données issues des transactions PayPal sont protégées conformément aux politiques de sécurité de l'information, de protection des données personnelles et d'archivage documentaire de l'Organisation. Elles sont conservées pendant les délais prévus par les réglementations applicables et demeurent accessibles aux seules personnes habilitées dans le cadre des contrôles internes, des audits ou des demandes formulées par les autorités compétentes.

En cas de litige, de contestation, de remboursement, de rétrofacturation (chargeback), de tentative d'usurpation d'identité ou de compromission d'un compte, AGCE International applique les procédures prévues par la plateforme PayPal ainsi que ses propres procédures internes de gestion des incidents. Chaque situation est analysée individuellement afin de protéger les intérêts de l'Organisation, de ses membres, partenaires, donateurs et bénéficiaires tout en respectant les droits des utilisateurs et les exigences réglementaires.

Par l'encadrement rigoureux des paiements réalisés via PayPal, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce la sécurité de ses opérations financières internationales, garantit la transparence de ses flux financiers et consolide la confiance de l'ensemble de ses parties prenantes dans ses mécanismes de collecte et de gestion des ressources.

8.29 Paiements SeerBit

Les **paiements effectués au moyen de la plateforme SeerBit** constituent un dispositif stratégique permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de recevoir des paiements électroniques provenant de différents pays et de multiples moyens de règlement. Cette solution favorise l'inclusion financière, facilite les transactions internationales et contribue au développement des activités humanitaires, sociales, éducatives, sanitaires, environnementales, économiques et numériques de l'Organisation, tout en garantissant un niveau élevé de sécurité et de conformité.

Les paiements réalisés par l'intermédiaire de SeerBit peuvent concerner les adhésions, cotisations, abonnements, dons, paiements de prestations, achats de produits numériques, inscriptions aux formations, événements institutionnels et toute autre opération autorisée par les politiques financières de l'Organisation. Toutes ces transactions sont soumises aux règles internes de contrôle financier, de gouvernance, de double validation, de séparation des responsabilités et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Les comptes SeerBit utilisés par AGCE International sont administrés exclusivement par des responsables autorisés disposant d'habilitations spécifiques. Les accès sont protégés par des mécanismes de sécurité avancés comprenant notamment l'authentification multifacteur, le chiffrement des communications, la surveillance des connexions, la gestion sécurisée des identifiants ainsi que la journalisation des opérations réalisées sur la plateforme.

Chaque transaction enregistrée via SeerBit fait l'objet d'une vérification destinée à confirmer la cohérence des informations relatives au payeur, au bénéficiaire, au montant, à la devise utilisée, au motif du paiement et aux références de la transaction. Les données sont rapprochées avec les systèmes comptables et administratifs de l'Organisation afin d'assurer une parfaite concordance entre les paiements reçus et les opérations enregistrées.

L'Organisation met en œuvre un dispositif permanent de surveillance des transactions SeerBit afin de détecter toute opération inhabituelle, tout comportement anormal, toute tentative de fraude, de blanchiment de capitaux, de financement du terrorisme, de cyberattaque ou d'utilisation abusive des services de paiement. Les alertes générées par la plateforme ou par les systèmes internes sont analysées sans délai et peuvent conduire à la suspension de la transaction, à des vérifications complémentaires ou au signalement des opérations suspectes conformément aux exigences réglementaires.

Les informations relatives aux paiements SeerBit sont conservées dans des systèmes d'information sécurisés garantissant leur intégrité, leur confidentialité, leur disponibilité et leur traçabilité. Elles sont protégées contre tout accès non autorisé et demeurent accessibles uniquement aux personnes habilitées dans le cadre des activités de gestion financière, de conformité, d'audit ou des contrôles exercés par les autorités compétentes.

L'Organisation procède régulièrement à des rapprochements comptables, à des contrôles de cohérence, à des revues de sécurité et à des audits des opérations réalisées via SeerBit afin d'évaluer l'efficacité des dispositifs de contrôle, d'identifier les risques émergents et de renforcer les mesures de protection contre les menaces financières et technologiques.

Par l'utilisation encadrée de la plateforme SeerBit, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme sa volonté de proposer des solutions de paiement électroniques modernes, fiables, inclusives et sécurisées, conformes aux meilleures pratiques internationales en matière de gouvernance financière, de cybersécurité, de protection des données, de gestion des risques et de lutte contre le blanchiment de capitaux ainsi que le financement du terrorisme.

8.30 Paiements Moneris

Les **paiements effectués par l'intermédiaire de la plateforme Moneris** constituent un moyen de paiement électronique autorisé par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** pour la perception des adhésions, cotisations, abonnements, dons, contributions volontaires, paiements de prestations, inscriptions aux activités, achats de produits et services numériques ainsi que toute autre transaction financière approuvée par l'Organisation. L'utilisation de cette solution de paiement s'inscrit dans le respect des principes de sécurité financière, de transparence, de traçabilité, de protection des données et de conformité aux exigences de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

AGCE International veille à ce que les comptes Moneris utilisés soient ouverts au nom de l'Organisation, administrés exclusivement par des personnes dûment habilitées et protégés par des dispositifs de sécurité renforcés. Les accès sont limités selon le principe du moindre privilège et reposent sur des mécanismes d'authentification forte, de gestion sécurisée des mots de passe, de contrôle des habilitations, de journalisation des connexions et de surveillance continue des activités réalisées sur la plateforme.

Chaque paiement traité via Moneris fait l'objet d'un processus de vérification destiné à confirmer l'identité du payeur lorsque cela est requis, la cohérence des informations relatives à la transaction, la validité des autorisations, la conformité des justificatifs et la légitimité de l'opération. Les données essentielles, notamment le montant, la devise, le moyen de paiement utilisé, la référence de transaction, la date, l'heure et le bénéficiaire, sont enregistrées dans les systèmes de gestion financière de l'Organisation afin d'assurer une traçabilité complète.

Les transactions Moneris sont soumises à un dispositif permanent de surveillance permettant d'identifier les opérations inhabituelles, les paiements répétitifs, les anomalies de comportement, les tentatives de fraude, les contestations de paiement, les rétrofacturations (chargebacks), les accès non autorisés et toute autre situation susceptible de présenter un risque financier ou réglementaire. Toute alerte déclenche une analyse approfondie par les responsables compétents, pouvant conduire à la suspension temporaire de la transaction, à

des vérifications complémentaires ou au signalement des opérations suspectes conformément aux procédures internes.

L'Organisation procède régulièrement à des rapprochements entre les relevés Moneris, les écritures comptables, les justificatifs financiers et les données enregistrées dans ses systèmes d'information afin de garantir l'exactitude des opérations et la fiabilité des informations financières. Les écarts constatés sont documentés, analysés et corrigés dans les meilleurs délais.

Les informations relatives aux paiements Moneris sont conservées dans des environnements numériques sécurisés garantissant leur confidentialité, leur intégrité, leur disponibilité et leur conservation conformément aux politiques d'archivage documentaire, de protection des données personnelles et aux obligations légales applicables. L'accès à ces informations est réservé aux seules personnes habilitées dans le cadre de leurs missions.

En cas d'incident technique, de fraude, de compromission d'un compte, de tentative d'intrusion ou de litige relatif à une transaction, AGCE International applique sans délai les procédures de gestion des incidents prévues par ses politiques internes ainsi que les mécanismes de sécurité mis à disposition par Moneris. Les mesures appropriées sont prises afin de limiter les risques, protéger les intérêts des parties concernées et assurer la continuité des opérations.

Par l'utilisation encadrée de Moneris, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce la sécurité de ses paiements électroniques, améliore la fiabilité de ses opérations financières et garantit à ses membres, partenaires, donateurs et bailleurs de fonds un environnement de paiement conforme aux meilleures pratiques internationales de gouvernance financière, de cybersécurité et de conformité réglementaire.

8.31 Paiements Orange Money

Les **paiements réalisés au moyen du service Orange Money** constituent une solution de paiement mobile autorisée par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** afin de faciliter la réception des adhésions, cotisations, dons, abonnements, contributions volontaires, paiements de services, inscriptions aux activités et autres opérations financières autorisées. Cette solution favorise l'inclusion financière, améliore l'accessibilité des services de l'Organisation et permet aux membres, partenaires, bénéficiaires et donateurs d'effectuer des transactions rapides, sécurisées et adaptées aux réalités locales.

L'utilisation d'Orange Money est encadrée par les procédures internes de gouvernance financière, de contrôle interne et de lutte contre le blanchiment de capitaux et le financement du terrorisme. Les comptes Orange Money utilisés par AGCE International sont ouverts au nom de l'Organisation ou de structures officiellement autorisées, administrés uniquement par

des personnes habilitées et protégées par des mesures de sécurité appropriées garantissant la confidentialité des identifiants, la protection des codes d'accès et la limitation des droits d'utilisation.

Chaque paiement reçu ou effectué via Orange Money est enregistré dans les systèmes de gestion financière de l'Organisation avec l'ensemble des informations nécessaires à son identification. Les références de transaction, les montants, les dates, les heures, les numéros de transaction, les justificatifs, les bénéficiaires, les motifs des paiements ainsi que les validations internes sont conservés afin d'assurer une traçabilité complète des opérations.

Les transactions Orange Money font l'objet d'un contrôle permanent destiné à détecter les paiements inhabituels, les opérations fractionnées, les montants anormalement élevés, les tentatives de fraude, les erreurs de destinataire, les transactions répétitives ou tout comportement susceptible de révéler un risque de blanchiment de capitaux, de financement du terrorisme ou d'utilisation abusive des services financiers mobiles. Les opérations présentant un caractère suspect sont immédiatement soumises à une analyse approfondie et peuvent être suspendues jusqu'à la fin des vérifications nécessaires.

Les rapprochements entre les relevés Orange Money, les registres comptables et les systèmes de gestion de l'Organisation sont réalisés de manière régulière afin de garantir l'exactitude des informations financières, d'identifier les éventuels écarts et de mettre en œuvre les actions correctives appropriées. Toute anomalie significative fait l'objet d'une documentation complète et, le cas échéant, d'une procédure d'investigation ou de signalement conformément aux obligations réglementaires applicables.

Les données relatives aux paiements Orange Money sont protégées par des mesures techniques et organisationnelles garantissant leur confidentialité, leur intégrité, leur disponibilité et leur conservation pendant les délais prévus par les politiques internes et les réglementations en vigueur. L'accès à ces informations est limité aux personnes autorisées dans le cadre de leurs fonctions de gestion financière, de conformité, d'audit ou de contrôle.

En cas de perte d'accès, de fraude, d'usurpation d'identité, de paiement erroné, de compromission d'un compte ou de tout autre incident de sécurité, AGCE International applique immédiatement son dispositif de gestion des incidents. Celui-ci prévoit notamment la suspension des opérations concernées, la sécurisation des comptes, la notification des opérateurs de paiement, la conservation des éléments de preuve, la conduite d'investigations internes et, lorsque les circonstances l'exigent, le signalement aux autorités compétentes.

Par l'encadrement rigoureux des paiements effectués via Orange Money, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** favorise un accès sécurisé aux services financiers mobiles, renforce l'inclusion des populations, protège les ressources confiées à l'Organisation et garantit une gestion financière conforme aux principes de transparence, de responsabilité, de sécurité et aux meilleures pratiques internationales en matière de lutte contre le blanchiment de capitaux, de prévention du financement du terrorisme et de bonne gouvernance institutionnelle.

8.32 Paiements MTN Mobile Money

Les **paiements réalisés par l'intermédiaire du service MTN Mobile Money** constituent un moyen de paiement électronique autorisé par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** afin de faciliter la réception et, lorsque cela est autorisé, l'exécution de certaines opérations financières liées à ses activités institutionnelles. Ce service permet notamment le règlement des droits d'adhésion, des cotisations annuelles, des abonnements, des dons, des contributions volontaires, des frais d'inscription aux formations et événements, ainsi que des paiements relatifs aux services proposés par l'Organisation. Son utilisation s'inscrit dans le respect des principes de transparence, de sécurité financière, de traçabilité et de conformité aux exigences de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

Tous les comptes MTN Mobile Money utilisés par AGCE International sont ouverts conformément aux dispositions réglementaires applicables et sont exclusivement administrés par des responsables officiellement désignés. Les accès aux comptes sont protégés par des mesures de sécurité renforcées comprenant notamment des codes confidentiels robustes, une authentification adaptée, une gestion rigoureuse des habilitations et une surveillance permanente des accès. Toute modification des droits d'utilisation fait l'objet d'une autorisation préalable et d'une traçabilité complète.

Chaque paiement reçu ou effectué via MTN Mobile Money est soumis à une procédure de vérification permettant de confirmer l'identité du payeur ou du bénéficiaire lorsque cela est requis, la conformité du montant, la cohérence des références de transaction, la justification de l'opération ainsi que le respect des procédures internes de validation. Les informations relatives aux transactions sont enregistrées dans les systèmes comptables et administratifs de l'Organisation afin de garantir une parfaite traçabilité des flux financiers.

L'Organisation met en œuvre un dispositif permanent de surveillance des opérations réalisées via MTN Mobile Money. Les transactions sont analysées afin de détecter les paiements inhabituels, les opérations répétitives ou fractionnées, les montants anormalement élevés, les anomalies de comportement, les erreurs de destinataire, les tentatives de fraude, les usurpations d'identité ou tout autre événement susceptible de présenter un risque de blanchiment de capitaux, de financement du terrorisme ou de détournement de ressources. Les alertes générées sont examinées sans délai par les responsables compétents.

Les rapprochements entre les relevés MTN Mobile Money, les pièces justificatives, les registres comptables et les systèmes financiers de l'Organisation sont réalisés de manière régulière afin d'assurer la concordance des informations, d'identifier les éventuels écarts et de mettre en œuvre les mesures correctives appropriées. Toute irrégularité fait l'objet d'une analyse documentée et, lorsque cela est nécessaire, d'une procédure d'investigation ou de signalement conformément aux dispositions légales applicables.

Les données relatives aux paiements sont conservées dans des environnements sécurisés garantissant leur confidentialité, leur intégrité, leur disponibilité et leur conservation conformément aux politiques d'archivage documentaire de l'Organisation. L'accès à ces informations est limité aux personnes dûment habilitées dans le cadre de leurs missions de gestion financière, de conformité, d'audit ou de contrôle.

En cas de fraude, de perte d'accès, de compromission d'un compte, d'erreur de transaction ou d'incident de sécurité, AGCE International déclenche immédiatement les procédures prévues par son dispositif de gestion des incidents. Ces mesures comprennent notamment la suspension des opérations concernées, la sécurisation des comptes, la notification de l'opérateur de paiement, la conservation des éléments de preuve, la réalisation d'investigations internes et, lorsque les circonstances l'exigent, la transmission des informations aux autorités compétentes.

Par l'encadrement rigoureux des paiements effectués via MTN Mobile Money, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit un environnement de paiement mobile fiable, sécurisé et transparent, favorise l'inclusion financière de ses membres et partenaires, protège les ressources qui lui sont confiées et renforce sa conformité aux meilleures pratiques internationales en matière de gouvernance financière et de lutte contre la criminalité financière.

8.33 Virements bancaires

Les **virements bancaires** constituent l'un des principaux moyens de paiement utilisés par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** pour la réception et l'exécution de transactions financières nationales et internationales. Ils permettent notamment le versement des adhésions, cotisations, dons, subventions, contributions institutionnelles, financements de projets, paiements de fournisseurs, règlements contractuels et toute autre opération financière autorisée dans le cadre des activités de l'Organisation. Leur utilisation est soumise à des règles strictes de gouvernance, de sécurité, de traçabilité et de conformité aux exigences relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

Tous les comptes bancaires utilisés par l'Organisation sont ouverts au nom de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** auprès d'établissements financiers légalement agréés et sélectionnés selon des critères de solidité, de conformité réglementaire, de sécurité opérationnelle et de fiabilité. L'ouverture, la modification ou la clôture d'un compte bancaire sont soumises à l'autorisation des instances compétentes de gouvernance et font l'objet d'une documentation complète.

Avant l'exécution d'un virement bancaire, une vérification préalable est réalisée afin de confirmer l'identité du donneur d'ordre et du bénéficiaire, l'exactitude des coordonnées bancaires, la disponibilité des autorisations internes, la présence des pièces justificatives, la conformité budgétaire ainsi que la légitimité de l'opération. Les paiements présentant un niveau

de risque élevé ou dépassant les seuils internes peuvent être soumis à une procédure renforcée comprenant une double validation et des contrôles complémentaires.

Chaque virement bancaire est enregistré dans les systèmes financiers de l'Organisation avec l'ensemble des informations nécessaires à sa traçabilité. Sont notamment conservés les références bancaires, les numéros de transaction, les montants, les devises, les dates d'exécution, les justificatifs, les validations internes, les correspondances éventuelles ainsi que les documents attestant de la réalisation effective de l'opération. Ces informations sont archivées conformément aux politiques documentaires de l'Organisation et aux obligations réglementaires applicables.

Les virements bancaires font l'objet d'une surveillance permanente destinée à détecter toute anomalie susceptible de révéler une fraude, une erreur de saisie, une tentative de détournement, une falsification de coordonnées bancaires, un paiement inhabituel, une opération sans justification économique ou tout autre comportement présentant un risque de blanchiment de capitaux ou de financement du terrorisme. Toute opération suspecte est immédiatement suspendue lorsque cela est possible, analysée par les responsables compétents et traitée conformément aux procédures de gestion des alertes et des signalements.

L'Organisation effectue des rapprochements bancaires réguliers entre les relevés des établissements financiers, les écritures comptables, les justificatifs de paiement et les registres financiers internes. Ces contrôles permettent de garantir l'exactitude des opérations, d'identifier rapidement les écarts éventuels et de mettre en œuvre les actions correctives nécessaires afin d'assurer la fiabilité des informations financières.

Les données bancaires sont protégées par des mesures de sécurité techniques et organisationnelles comprenant notamment le chiffrement des informations sensibles, la limitation des accès selon les habilitations, la journalisation des opérations, les sauvegardes régulières, la surveillance des systèmes d'information et des procédures de continuité d'activité destinées à préserver la disponibilité des services financiers.

En cas d'incident, de fraude bancaire, de compromission des coordonnées de paiement, de tentative de cyberattaque ou de litige relatif à un virement, AGCE International met immédiatement en œuvre son dispositif de gestion des incidents financiers. Celui-ci prévoit la suspension des opérations concernées, l'information de l'établissement bancaire, la sécurisation des comptes, l'ouverture d'une enquête interne, la conservation des preuves et, lorsque les circonstances l'imposent, le signalement aux autorités compétentes.

Par l'application de ces règles, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que l'ensemble des virements bancaires est exécuté dans des conditions optimales de sécurité, de transparence, de responsabilité et de conformité, assurant ainsi une gestion rigoureuse des ressources qui lui sont confiées et le respect des meilleures pratiques internationales en matière de gouvernance financière et de prévention de la criminalité financière.

8.34 Paiements par cartes Visa

Les **paiements effectués au moyen des cartes Visa** constituent un mode de règlement électronique autorisé par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** pour la réception des adhésions, cotisations, abonnements, dons, contributions volontaires, paiements de services, inscriptions aux programmes, formations, événements institutionnels, acquisitions de produits numériques ainsi que toute autre opération financière approuvée par l'Organisation. L'utilisation des cartes Visa s'inscrit dans le respect des principes de transparence, de sécurité financière, de protection des données, de traçabilité et de conformité aux dispositions relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

L'Organisation veille à ce que tous les paiements effectués par carte Visa transitent exclusivement par des passerelles de paiement sécurisées, conformes aux normes internationales de sécurité applicables aux paiements électroniques. Les plateformes retenues doivent garantir la confidentialité des données financières, la protection contre les accès non autorisés, le chiffrement des échanges de données, la détection des activités frauduleuses ainsi que l'authentification renforcée des transactions lorsque celle-ci est requise.

Avant la validation d'un paiement par carte Visa, les systèmes de l'Organisation procèdent aux contrôles nécessaires afin de vérifier la cohérence des informations de transaction, la conformité du montant, la devise utilisée, la validité de l'autorisation bancaire ainsi que la compatibilité de l'opération avec les politiques financières et les procédures de conformité en vigueur. Lorsque la nature, le montant ou les caractéristiques d'une transaction présentent un niveau de risque élevé, des contrôles renforcés peuvent être mis en œuvre avant toute validation définitive.

Toutes les transactions Visa sont automatiquement enregistrées dans les systèmes d'information de l'Organisation avec l'ensemble des informations nécessaires à leur traçabilité. Ces données comprennent notamment la référence de la transaction, la date et l'heure du paiement, le montant, la devise, l'identifiant de la plateforme de paiement, les autorisations obtenues ainsi que les justificatifs associés. Les informations sensibles relatives aux cartes bancaires ne sont jamais conservées au-delà de ce qui est strictement nécessaire et conformément aux exigences légales et aux règles de sécurité applicables.

Les paiements Visa font l'objet d'une surveillance permanente destinée à détecter les comportements inhabituels, les paiements multiples, les tentatives de fraude, les rétrofacturations (chargebacks), les contestations, les usurpations d'identité, les anomalies techniques ainsi que toute opération susceptible de constituer un risque de blanchiment de capitaux ou de financement du terrorisme. Les alertes générées par les systèmes internes ou par les prestataires de paiement sont analysées sans délai par les responsables compétents.

L'Organisation réalise régulièrement des rapprochements entre les relevés des prestataires de paiement, les enregistrements comptables, les justificatifs financiers et les

opérations effectivement réalisées. Toute différence constatée fait l'objet d'une analyse documentée, de mesures correctives adaptées et, si nécessaire, d'une procédure d'investigation conformément aux politiques internes de contrôle et de conformité.

En cas de fraude présumée, de contestation de paiement, de compromission d'une transaction, de tentative d'utilisation frauduleuse d'une carte ou d'incident de sécurité, AGCE International met immédiatement en œuvre son dispositif de gestion des incidents. Celui-ci prévoit notamment la suspension des opérations concernées lorsque cela est possible, la notification du prestataire de paiement, la sécurisation des systèmes, la conservation des preuves, l'ouverture d'une enquête interne et, lorsque les circonstances l'imposent, le signalement aux autorités compétentes.

Par l'application de ces mesures, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que les paiements réalisés au moyen des cartes Visa sont traités dans un environnement sécurisé, transparent et conforme aux meilleures pratiques internationales de gouvernance financière, de cybersécurité, de protection des données personnelles et de prévention de la criminalité financière.

8.35 Paiements par cartes Mastercard

Les paiements effectués au moyen des cartes Mastercard constituent un instrument de paiement électronique reconnu par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** pour faciliter les transactions financières nationales et internationales réalisées dans le cadre de ses activités institutionnelles. Ils permettent notamment le règlement des adhésions, cotisations, abonnements, dons, contributions volontaires, achats de services, inscriptions aux formations et événements, financements de projets ainsi que toute autre opération autorisée conformément aux politiques financières de l'Organisation.

L'utilisation des cartes Mastercard est encadrée par les principes de sécurité financière, de transparence, de protection des données, de maîtrise des risques et de conformité réglementaire. Toutes les opérations sont exécutées exclusivement par l'intermédiaire de prestataires de paiement répondant aux normes internationales de sécurité des transactions électroniques et disposant de mécanismes robustes de prévention de la fraude, de gestion des risques et de surveillance des paiements.

Avant toute validation d'une transaction Mastercard, des contrôles sont effectués afin de vérifier l'authenticité de la demande de paiement, la conformité des informations de transaction, la disponibilité des autorisations requises, la cohérence des montants et la compatibilité de l'opération avec les politiques financières, budgétaires et de conformité de l'Organisation. Les opérations présentant des caractéristiques inhabituelles peuvent être soumises à des contrôles renforcés avant leur exécution.

Chaque transaction Mastercard fait l'objet d'une traçabilité complète. Les systèmes de gestion enregistrent notamment la référence de la transaction, le montant, la devise, la date, l'heure, le canal de paiement, les validations obtenues, les justificatifs disponibles ainsi que les informations nécessaires au suivi comptable et aux contrôles de conformité. Les données relatives aux titulaires des cartes sont protégées conformément aux exigences légales applicables et aux politiques internes de sécurité de l'information.

Les paiements Mastercard sont surveillés en permanence afin d'identifier les opérations inhabituelles, les tentatives de fraude, les paiements répétitifs, les contestations, les remboursements anormaux, les rétrofacturations, les anomalies techniques et toute activité susceptible de présenter un risque de blanchiment de capitaux, de financement du terrorisme ou d'atteinte aux intérêts financiers de l'Organisation. Toute alerte déclenche une analyse immédiate pouvant conduire à des vérifications complémentaires, à la suspension de l'opération ou à l'application des procédures internes de gestion des incidents.

Des rapprochements réguliers sont réalisés entre les données des prestataires de paiement, les relevés bancaires, les écritures comptables et les justificatifs financiers afin de garantir l'exactitude des opérations enregistrées. Les écarts éventuels sont analysés, documentés et corrigés selon les procédures internes de contrôle financier.

En cas de fraude, de cyberattaque, de compromission d'une transaction, de contestation de paiement ou de toute autre anomalie affectant une opération Mastercard, AGCE International applique immédiatement les mesures prévues par son dispositif de gestion des incidents. Celui-ci comprend la sécurisation des systèmes concernés, la coopération avec les prestataires de paiement, la conservation des éléments de preuve, la conduite d'investigations internes, la mise en œuvre d'actions correctives et, le cas échéant, le signalement des faits aux autorités compétentes.

Par la mise en œuvre de cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** assure que les paiements réalisés au moyen des cartes Mastercard sont exécutés dans des conditions optimales de sécurité, de fiabilité et de conformité. L'Organisation renforce ainsi la confiance de ses membres, partenaires, donateurs, bailleurs de fonds et bénéficiaires tout en garantissant une gestion financière responsable, transparente et conforme aux meilleures pratiques internationales en matière de sécurité des paiements électroniques et de lutte contre le blanchiment de capitaux ainsi que le financement du terrorisme.

8.36 Paiements American Express

Les **paiements effectués au moyen des cartes American Express** constituent un mode de règlement électronique reconnu par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** pour la perception des adhésions, cotisations, abonnements, dons, contributions volontaires, financements de projets, inscriptions aux activités, acquisitions de produits ou services numériques ainsi que toute autre

transaction financière autorisée par l'Organisation. Leur utilisation s'inscrit dans le respect des principes de bonne gouvernance, de transparence financière, de sécurité des paiements et de conformité aux exigences de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

L'ensemble des transactions réalisées au moyen des cartes American Express est traité exclusivement par des passerelles de paiement sécurisées et des prestataires agréés répondant aux normes internationales de sécurité des paiements électroniques. AGCE International veille à ce que ces partenaires disposent de mécanismes robustes de protection contre la fraude, de gestion des risques, de surveillance des transactions, de chiffrement des données et de protection des informations financières conformément aux meilleures pratiques internationales.

Avant toute validation d'un paiement, une série de contrôles est effectuée afin de vérifier la conformité de l'opération, l'autorisation bancaire, la cohérence du montant, la devise utilisée, le respect des procédures internes ainsi que la légitimité de la transaction. Les opérations présentant un profil de risque élevé, un montant inhabituel, un comportement atypique ou des incohérences techniques peuvent faire l'objet de contrôles renforcés, de validations complémentaires ou d'une suspension temporaire jusqu'à l'achèvement des vérifications nécessaires.

Chaque transaction American Express est enregistrée dans les systèmes d'information de l'Organisation avec l'ensemble des informations nécessaires à sa traçabilité. Les données conservées comprennent notamment la référence de la transaction, la date, l'heure, le montant, la devise, le canal de paiement, les justificatifs associés, les validations internes et les éléments nécessaires aux rapprochements comptables et aux audits. Les informations confidentielles relatives aux cartes de paiement ne sont ni stockées ni exploitées au-delà des exigences strictement nécessaires au traitement sécurisé des opérations et dans le respect des réglementations applicables.

L'Organisation met en œuvre un dispositif permanent de surveillance des transactions American Express afin d'identifier rapidement toute tentative de fraude, d'usurpation d'identité, de paiement répété, de rétrofacturation (chargeback), de contestation abusive, de comportement inhabituel ou de toute opération susceptible de révéler un risque de blanchiment de capitaux, de financement du terrorisme ou de cybercriminalité. Les alertes générées par les systèmes de surveillance sont immédiatement analysées par les responsables compétents et donnent lieu, le cas échéant, à des investigations approfondies.

Des rapprochements réguliers sont réalisés entre les données issues des prestataires de paiement, les relevés bancaires, les écritures comptables, les justificatifs financiers et les registres institutionnels afin de garantir l'exactitude des informations enregistrées et la parfaite concordance des opérations financières. Toute anomalie constatée est documentée, analysée et traitée conformément aux procédures internes de contrôle, de conformité et de gestion des incidents.

En cas de fraude, de compromission d'une transaction, de tentative d'accès non autorisé, de contestation de paiement ou de tout autre incident de sécurité, AGCE International applique immédiatement son dispositif de gestion des incidents financiers. Celui-ci prévoit notamment la suspension des opérations concernées, la sécurisation des systèmes, la coopération avec le prestataire de paiement, la conservation des preuves, l'ouverture d'une enquête interne, la mise en œuvre d'actions correctives et, lorsque les circonstances l'exigent, la transmission des informations aux autorités compétentes.

Par l'encadrement rigoureux des paiements effectués au moyen des cartes American Express, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit un environnement de paiement électronique sécurisé, fiable et conforme aux meilleures pratiques internationales de gouvernance financière, de cybersécurité, de protection des données personnelles et de prévention de la criminalité financière.

8.37 Authentification forte (MFA)

L'**authentification forte (Multi-Factor Authentication – MFA)** constitue une mesure essentielle de sécurité mise en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** afin de protéger l'accès à ses systèmes d'information, à ses plateformes de paiement, à ses applications numériques, à ses services financiers, à ses espaces administratifs ainsi qu'à l'ensemble des données sensibles relatives à ses activités institutionnelles. Elle contribue à prévenir les accès non autorisés, les usurpations d'identité, les compromissions de comptes, les cyberattaques et les opérations frauduleuses susceptibles de porter atteinte à l'intégrité des ressources de l'Organisation.

Le principe de l'authentification forte repose sur la combinaison d'au moins deux facteurs d'authentification indépendants appartenant à des catégories différentes, notamment un élément connu uniquement de l'utilisateur (mot de passe ou code confidentiel), un élément détenu par celui-ci (téléphone mobile, jeton de sécurité ou clé matérielle) et, lorsque cela est approprié, un élément biométrique (empreinte digitale, reconnaissance faciale ou autre procédé reconnu). Cette combinaison permet de réduire significativement les risques d'accès frauduleux aux systèmes de l'Organisation.

L'authentification forte est obligatoire pour tous les comptes disposant de privilèges administratifs, les responsables financiers, les gestionnaires des plateformes de paiement, les administrateurs des systèmes d'information, les responsables de la conformité, les membres des organes de gouvernance ainsi que toute personne ayant accès à des informations confidentielles ou à des fonctions sensibles. Elle est également exigée pour les opérations présentant un niveau élevé de risque, notamment les validations de paiements, les virements bancaires, les modifications des coordonnées financières, les changements d'habilitation et les accès à distance aux infrastructures numériques.

L'Organisation met en œuvre des solutions d'authentification conformes aux standards internationaux de cybersécurité et veille à leur mise à jour régulière afin de tenir compte de l'évolution des menaces. Les mécanismes d'authentification sont intégrés aux plateformes numériques utilisées par AGCE International, notamment les systèmes de gestion financière, les espaces membres, les outils collaboratifs, les applications administratives et les services de paiement en ligne.

Toutes les tentatives d'authentification sont enregistrées dans des journaux sécurisés permettant d'assurer une traçabilité complète des accès. Les connexions inhabituelles, les tentatives répétées d'échec, les connexions depuis des zones géographiques anormales, les appareils non reconnus ou tout comportement suspect génèrent automatiquement des alertes pouvant entraîner le blocage temporaire du compte, la demande d'une vérification complémentaire ou l'ouverture d'une procédure d'investigation.

Les utilisateurs sont tenus de préserver la confidentialité de leurs moyens d'authentification, de ne jamais partager leurs identifiants ou leurs codes de validation et de signaler immédiatement toute suspicion de compromission, de perte d'appareil, de tentative de phishing ou d'utilisation frauduleuse de leur compte. L'Organisation organise régulièrement des actions de sensibilisation afin de promouvoir les bonnes pratiques en matière de cybersécurité, de protection des identifiants et de gestion des accès.

Les dispositifs d'authentification forte font l'objet d'évaluations régulières dans le cadre des audits de sécurité, des contrôles internes et des revues de conformité. Les enseignements tirés des incidents, des évolutions technologiques et des nouvelles menaces permettent d'améliorer en permanence les mécanismes de protection et de renforcer la résilience des systèmes numériques.

Par l'application systématique de l'authentification forte, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** protège efficacement ses ressources numériques, sécurise l'ensemble de ses opérations financières et administratives, renforce la confiance de ses membres, partenaires, donateurs et bailleurs de fonds, et confirme son engagement permanent en faveur de la cybersécurité, de la protection des données, de la bonne gouvernance et de la conformité aux meilleures pratiques internationales en matière de sécurité des systèmes d'information et de lutte contre le blanchiment de capitaux ainsi que le financement du terrorisme.

8.38 Signature électronique

La **signature électronique** constitue un mécanisme essentiel de sécurisation, d'authentification et de validation des opérations numériques au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle permet d'assurer l'intégrité, l'authenticité, la traçabilité et la valeur probante des documents, contrats, autorisations, conventions, opérations financières et décisions institutionnelles traités sous format électronique. Son utilisation contribue au renforcement de la gouvernance

numérique, de la sécurité juridique et de la conformité de l'Organisation aux exigences nationales et internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

La signature électronique est utilisée pour l'ensemble des actes nécessitant une validation officielle, notamment les contrats, conventions de partenariat, bons de commande, validations de paiements, ordres de virement, autorisations administratives, rapports d'audit, procès-verbaux, décisions des organes de gouvernance, documents comptables, formulaires institutionnels, attestations, certificats ainsi que tout document dont l'authenticité doit être garantie.

AGCE International met en œuvre des solutions de signature électronique répondant à des exigences élevées de sécurité, de fiabilité et de conformité. Les dispositifs retenus doivent garantir l'identification du signataire, l'intégrité du document signé, la protection contre toute modification postérieure, l'horodatage sécurisé de l'opération ainsi que la conservation des preuves numériques permettant de démontrer la validité de la signature en cas de contrôle, d'audit ou de procédure judiciaire.

Chaque signature électronique est associée à un utilisateur identifié et authentifié au moyen de mécanismes de sécurité adaptés, notamment l'authentification forte (MFA), des certificats numériques, des clés cryptographiques ou tout autre procédé reconnu garantissant un niveau de sécurité approprié. Les certificats utilisés doivent être protégés contre toute utilisation frauduleuse et faire l'objet d'une gestion rigoureuse tout au long de leur cycle de vie.

L'Organisation applique une politique stricte de gestion des habilitations afin de déterminer les personnes autorisées à signer électroniquement des documents. Les droits de signature sont attribués en fonction des responsabilités exercées, des délégations de pouvoir, des niveaux d'autorisation et des procédures internes de gouvernance. Toute création, modification, suspension ou suppression d'un droit de signature est formalisée, validée et enregistrée dans les systèmes de gestion de l'Organisation.

Toutes les opérations de signature électronique sont automatiquement enregistrées dans des journaux sécurisés comprenant notamment l'identité du signataire, la date et l'heure de signature, le document concerné, l'adresse technique de connexion lorsque cela est autorisé, le certificat utilisé ainsi que les validations complémentaires éventuellement réalisées. Cette traçabilité garantit la reconstitution complète des opérations et facilite les audits, les contrôles internes et les investigations en cas d'incident.

Les documents signés électroniquement sont conservés dans des environnements numériques sécurisés garantissant leur confidentialité, leur intégrité, leur disponibilité et leur conservation pendant les délais prévus par les politiques documentaires de l'Organisation et les réglementations applicables. Toute tentative d'altération, de suppression ou de falsification est détectée et traitée conformément aux procédures de sécurité de l'information.

En cas de compromission d'un certificat, de perte d'un dispositif d'authentification, de suspicion d'usurpation d'identité ou de fraude, AGCE International met immédiatement en œuvre les mesures nécessaires, notamment la révocation des certificats concernés, la suspension des droits de signature, l'ouverture d'une enquête interne, la conservation des preuves numériques et, lorsque les circonstances l'exigent, la notification des autorités compétentes.

Par l'intégration de la signature électronique dans ses processus institutionnels, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce la sécurité juridique de ses actes, accélère ses procédures administratives, protège l'intégrité de ses opérations numériques et confirme son engagement en faveur d'une gouvernance moderne, transparente, sécurisée et conforme aux meilleures pratiques internationales.

8.39 Webhooks sécurisés

Les **webhooks sécurisés** constituent un mécanisme technique permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de recevoir automatiquement, en temps réel et de manière sécurisée, les notifications provenant de ses plateformes de paiement, de ses systèmes financiers, de ses applications numériques, de ses partenaires technologiques et de ses services en ligne. Ils assurent la synchronisation fiable des informations relatives aux transactions, aux validations de paiement, aux remboursements, aux abonnements, aux dons, aux adhésions et à tout autre événement nécessitant une mise à jour automatique des systèmes d'information de l'Organisation.

L'utilisation des webhooks s'inscrit dans le cadre des politiques de cybersécurité, de protection des données, de sécurité des paiements et de lutte contre le blanchiment de capitaux et le financement du terrorisme. Chaque webhook est configuré selon le principe de sécurité dès la conception (« Security by Design ») et de protection des données dès la conception (« Privacy by Design »), afin de limiter les risques d'interception, d'altération, de falsification ou d'utilisation non autorisée des informations échangées.

Tous les échanges réalisés par webhooks sont protégés par des protocoles de communication sécurisés, des mécanismes de chiffrement, des certificats numériques, des signatures cryptographiques ou tout autre procédé permettant de vérifier l'authenticité de l'émetteur, l'intégrité des données transmises et la confidentialité des communications. Les systèmes de l'Organisation vérifient systématiquement l'origine des notifications avant toute prise en compte des informations reçues.

Chaque notification reçue est soumise à un processus automatique de validation comprenant notamment le contrôle des signatures numériques, la vérification des clés d'authentification, l'analyse des identifiants de transaction, la cohérence des données reçues, la prévention des doublons, la détection des tentatives de rejeu (« replay attacks ») ainsi que le respect des règles de conformité applicables aux opérations concernées. Toute notification ne

satisfaisant pas aux critères de sécurité est automatiquement rejetée, enregistrée et signalée pour analyse.

Les événements traités par les webhooks sont intégralement journalisés. Les systèmes enregistrent notamment la date et l'heure de réception, la source de la notification, les identifiants techniques, le contenu des contrôles réalisés, le résultat des validations, les actions exécutées ainsi que les éventuelles anomalies détectées. Ces informations sont conservées dans des environnements sécurisés afin de garantir leur disponibilité pour les audits, les contrôles internes, les investigations techniques et les demandes des autorités compétentes.

L'Organisation réalise des contrôles réguliers des configurations de ses webhooks afin de vérifier leur conformité, leur niveau de sécurité, leur disponibilité et leur efficacité opérationnelle. Les clés d'authentification, certificats et secrets techniques font l'objet d'une rotation périodique, d'un stockage sécurisé et d'une gestion conforme aux politiques de cybersécurité de l'Organisation.

En cas d'incident de sécurité, de tentative d'intrusion, de compromission d'un webhook, de détection d'un comportement anormal ou d'échec des mécanismes de validation, AGCE International déclenche immédiatement son dispositif de gestion des incidents. Celui-ci prévoit notamment la désactivation temporaire des webhooks concernés, la sécurisation des systèmes, la conservation des preuves numériques, l'analyse technique des événements, la mise en œuvre des actions correctives nécessaires ainsi que la notification des partenaires concernés lorsque cela est approprié.

Par l'adoption de webhooks sécurisés, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit la fiabilité, l'intégrité et la sécurité des échanges automatisés entre ses plateformes numériques, renforce la continuité de ses services, améliore la rapidité du traitement des opérations financières et confirme son engagement permanent en faveur de la cybersécurité, de la gouvernance numérique, de la protection des données et de la conformité aux meilleures pratiques internationales.

8.40 Chiffrement des échanges

Le **chiffrement des échanges** constitue un élément fondamental de la politique de cybersécurité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour finalité d'assurer la confidentialité, l'intégrité, l'authenticité et la protection des informations échangées entre les utilisateurs, les plateformes numériques, les systèmes d'information, les établissements financiers, les prestataires de paiement, les partenaires institutionnels et les services en ligne de l'Organisation. Cette mesure contribue directement à la prévention du blanchiment de capitaux, du financement du terrorisme, de la fraude informatique, des cyberattaques, de l'espionnage numérique, des interceptions illicites et des atteintes à la confidentialité des données.

L'ensemble des communications électroniques impliquant des données financières, des informations personnelles, des documents administratifs, des justificatifs comptables, des identifiants d'authentification ou des informations sensibles est protégé au moyen de mécanismes de chiffrement robustes conformes aux standards internationaux reconnus. Les échanges entre les navigateurs des utilisateurs, les applications mobiles, les plateformes de paiement, les interfaces d'administration, les serveurs et les services tiers autorisés sont systématiquement sécurisés afin d'empêcher toute interception ou modification non autorisée des informations transmises.

Le chiffrement s'applique notamment aux paiements électroniques, aux virements bancaires, aux transactions réalisées via PayPal, SeerBit, Moneris, Orange Money, MTN Mobile Money, aux paiements par cartes bancaires, aux signatures électroniques, aux webhooks, aux espaces membres, aux applications internes, aux bases de données, aux sauvegardes numériques ainsi qu'à toute communication contenant des informations confidentielles relatives aux activités de l'Organisation.

Les clés cryptographiques utilisées pour le chiffrement sont générées, conservées, renouvelées et détruites selon des procédures strictes garantissant leur confidentialité et leur intégrité. L'accès à ces clés est limité aux personnes ou aux systèmes expressément autorisés, dans le respect du principe du moindre privilège. Toute utilisation, modification ou révocation d'une clé de chiffrement fait l'objet d'une traçabilité complète et d'un contrôle approprié.

Les dispositifs de chiffrement sont régulièrement évalués afin de garantir leur efficacité face à l'évolution des menaces informatiques. AGCE International procède à des mises à jour de ses mécanismes de sécurité, remplace les protocoles devenus obsolètes, applique les correctifs de sécurité recommandés et veille à l'utilisation de technologies reconnues pour leur fiabilité et leur conformité aux meilleures pratiques internationales.

Les échanges avec les partenaires, les établissements financiers, les fournisseurs de services numériques et les prestataires de paiement sont soumis aux mêmes exigences de sécurité. L'Organisation privilégie des partenaires mettant en œuvre des dispositifs de chiffrement conformes aux normes internationales et capables de garantir un niveau élevé de protection des données échangées.

Les opérations de chiffrement et de déchiffrement sont intégrées aux mécanismes de supervision de la sécurité de l'information. Toute tentative d'interception, de compromission des communications, d'utilisation de certificats frauduleux ou de dégradation des mécanismes de chiffrement fait l'objet d'une détection immédiate, d'une analyse technique approfondie et, le cas échéant, de l'application des procédures de gestion des incidents et de notification prévues par les politiques internes.

Les collaborateurs, administrateurs, bénévoles et partenaires habilités sont régulièrement sensibilisés aux bonnes pratiques relatives à la protection des communications électroniques, à la gestion des certificats numériques, aux risques liés aux réseaux non sécurisés et aux menaces susceptibles d'affecter la confidentialité des échanges.

Par la mise en œuvre d'une politique rigoureuse de chiffrement des échanges, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit la sécurité de ses communications numériques, protège les informations confiées par ses membres, partenaires, donateurs et bailleurs de fonds, renforce la résilience de ses infrastructures informatiques et confirme son engagement permanent en faveur de la cybersécurité, de la protection des données et de la conformité aux meilleures pratiques internationales.

8.41 Journalisation informatique

La **journalisation informatique** constitue un dispositif stratégique de surveillance, de traçabilité et de contrôle permanent des systèmes d'information de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle permet d'enregistrer de manière automatique, chronologique, sécurisée et inaltérable les événements techniques, les opérations administratives, les accès aux systèmes, les activités des utilisateurs, les transactions financières et les événements de sécurité afin de garantir l'intégrité des infrastructures numériques et de renforcer les mécanismes de lutte contre le blanchiment de capitaux, le financement du terrorisme et la cybercriminalité.

Le système de journalisation couvre l'ensemble des plateformes numériques de l'Organisation, notamment les sites web, les espaces membres, les applications mobiles, les solutions de paiement électronique, les bases de données, les serveurs, les systèmes d'authentification, les interfaces d'administration, les outils collaboratifs, les solutions de sauvegarde, les équipements réseau ainsi que les services infonuagiques (cloud) utilisés dans le cadre des activités institutionnelles.

Les journaux enregistrent notamment les connexions et déconnexions des utilisateurs, les tentatives d'authentification réussies ou échouées, les modifications de droits d'accès, les créations et suppressions de comptes, les validations de paiements, les opérations bancaires, les changements de configuration, les téléchargements de documents, les transferts de fichiers, les alertes de sécurité, les erreurs systèmes, les incidents techniques ainsi que toute activité susceptible d'avoir un impact sur la sécurité, la disponibilité ou l'intégrité des systèmes d'information.

Chaque événement enregistré comporte les informations nécessaires à sa parfaite traçabilité, notamment la date et l'heure horodatées, l'identifiant de l'utilisateur ou du système concerné, la nature de l'opération, les ressources utilisées, les résultats obtenus, les adresses techniques pertinentes lorsque leur traitement est autorisé par la réglementation applicable, ainsi que toute information utile à l'analyse des incidents ou aux investigations de conformité.

Les journaux informatiques sont protégés contre toute modification, suppression ou consultation non autorisée. Ils sont conservés dans des environnements sécurisés bénéficiant de mécanismes de chiffrement, de sauvegarde, de redondance, de contrôle des accès et de surveillance continue. Seules les personnes expressément habilitées dans le cadre de leurs

fonctions de sécurité informatique, de conformité, d'audit ou de gouvernance peuvent accéder à ces informations.

Les données issues de la journalisation font l'objet d'une analyse permanente au moyen d'outils de supervision permettant d'identifier rapidement les comportements anormaux, les tentatives d'intrusion, les cyberattaques, les accès frauduleux, les anomalies techniques, les opérations suspectes, les défaillances systèmes ou tout autre événement présentant un risque pour les activités de l'Organisation. Les alertes générées sont immédiatement examinées par les responsables compétents afin de mettre en œuvre les mesures de protection, de correction ou d'investigation appropriées.

Les journaux sont conservés conformément aux politiques d'archivage documentaire, aux exigences de protection des données personnelles et aux obligations légales applicables. Ils peuvent être consultés dans le cadre des audits internes, des audits externes, des contrôles réglementaires, des investigations techniques, des procédures disciplinaires ou des demandes légalement formulées par les autorités compétentes.

Les mécanismes de journalisation informatique font l'objet de revues périodiques afin d'évaluer leur efficacité, leur couverture fonctionnelle, leur conformité aux politiques de cybersécurité et leur capacité à répondre à l'évolution des risques numériques. Les résultats de ces évaluations alimentent le processus d'amélioration continue des dispositifs de sécurité de l'Organisation.

Par l'application d'une politique complète de journalisation informatique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit une surveillance permanente de ses infrastructures numériques, renforce la détection des incidents de sécurité, facilite les investigations et les audits, protège les données sensibles de ses parties prenantes et consolide son engagement en faveur d'une gouvernance numérique sécurisée, transparente et conforme aux meilleures pratiques internationales en matière de cybersécurité et de conformité financière.

SECTION V

CONSERVATION DOCUMENTAIRE

8.42 Principes

La **conservation documentaire** constitue un pilier fondamental du dispositif de gouvernance, de conformité, de transparence et de sécurité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif d'assurer la conservation, l'intégrité, la disponibilité, la confidentialité, l'authenticité et la traçabilité de l'ensemble des documents produits, reçus ou traités dans le cadre des activités institutionnelles, administratives, financières, comptables, juridiques, opérationnelles et numériques de l'Organisation. Cette politique garantit la préservation du

patrimoine documentaire de l'Organisation tout en répondant aux exigences légales, réglementaires et contractuelles applicables, notamment celles relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

Le principe fondamental de la conservation documentaire repose sur l'obligation de préserver tout document présentant une valeur administrative, financière, comptable, juridique, opérationnelle, historique ou probatoire. Sont notamment concernés les statuts, règlements, procès-verbaux, conventions de partenariat, contrats, rapports financiers, pièces comptables, justificatifs de paiement, dossiers d'adhésion, dossiers de dons, dossiers de conformité, documents KYC, rapports d'audit, signalements, correspondances officielles, documents fiscaux, décisions des organes de gouvernance, journaux d'événements, registres institutionnels ainsi que l'ensemble des documents numériques produits dans le cadre des activités de l'Organisation.

Tous les documents sont classés selon une nomenclature documentaire normalisée permettant leur identification, leur localisation, leur consultation et leur archivage. Chaque document reçoit un identifiant unique, une catégorie documentaire, une date de création, un niveau de confidentialité, une durée de conservation, un responsable désigné ainsi que les informations nécessaires à son suivi tout au long de son cycle de vie. Cette organisation garantit une gestion documentaire cohérente, homogène et conforme aux exigences de gouvernance de l'Organisation.

La conservation documentaire s'applique aussi bien aux documents physiques qu'aux documents électroniques. Les archives papier sont conservées dans des espaces sécurisés, protégés contre les risques de détérioration, de perte, de vol, d'incendie, d'humidité, d'accès non autorisé ou de destruction accidentelle. Les archives numériques sont hébergées dans des infrastructures bénéficiant de mécanismes de chiffrement, de sauvegarde régulière, de redondance, de contrôle des accès, de surveillance permanente et de plans de continuité d'activité destinés à assurer leur disponibilité et leur intégrité.

L'accès aux documents est strictement limité aux personnes dûment habilitées dans l'exercice de leurs fonctions. Les niveaux d'autorisation sont définis en fonction des responsabilités exercées et du caractère sensible des informations concernées. Toute consultation, modification, reproduction, transmission, exportation ou destruction d'un document fait l'objet d'une traçabilité complète permettant d'identifier l'utilisateur concerné, la nature de l'opération réalisée, la date, l'heure et le motif de l'intervention.

Les documents contenant des données personnelles, des informations financières, des informations stratégiques ou tout autre élément confidentiel sont soumis à des mesures renforcées de protection conformément aux politiques internes de sécurité de l'information et de protection des données de l'Organisation. Leur traitement s'effectue dans le respect des principes de confidentialité, de proportionnalité, de limitation des accès et de minimisation des risques de divulgation non autorisée.

AGCE International applique également le principe de conservation proportionnée. Les documents sont conservés pendant la durée nécessaire à l'accomplissement de leurs finalités administratives, financières, juridiques, fiscales, contractuelles ou réglementaires, conformément aux délais de conservation prévus par les lois applicables, les exigences des partenaires institutionnels et les politiques internes de l'Organisation. À l'expiration de ces délais, les documents peuvent être détruits ou archivés définitivement selon leur valeur historique, patrimoniale ou institutionnelle, dans le respect des procédures de destruction sécurisée.

La politique de conservation documentaire fait l'objet de contrôles réguliers, de revues périodiques et d'audits internes ou externes afin de vérifier son efficacité, sa conformité réglementaire et son adéquation avec les évolutions technologiques, organisationnelles et législatives. Les recommandations issues de ces évaluations alimentent le processus d'amélioration continue et permettent d'adapter les procédures documentaires aux nouveaux risques et aux meilleures pratiques internationales.

Par l'application de ces principes, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit la préservation durable de son patrimoine documentaire, renforce la sécurité juridique et financière de ses activités, facilite les contrôles, les audits et les investigations, protège les droits de ses membres, partenaires, donateurs et bénéficiaires, et affirme son engagement permanent en faveur d'une gouvernance responsable, transparente et conforme aux meilleures pratiques internationales en matière de gestion documentaire, de conformité institutionnelle et de lutte contre le blanchiment de capitaux ainsi que le financement du terrorisme.

8.43 Durées de conservation

La **détermination des durées de conservation** constitue un élément essentiel de la politique de gestion documentaire de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle vise à garantir que l'ensemble des documents institutionnels, administratifs, financiers, comptables, juridiques, techniques et numériques est conservé pendant une période suffisante pour répondre aux exigences légales, réglementaires, contractuelles, fiscales, comptables et opérationnelles applicables, tout en assurant la protection des droits de l'Organisation, de ses membres, partenaires, donateurs, bénéficiaires et autres parties prenantes.

Les durées de conservation sont déterminées selon la nature du document, son utilité administrative, sa valeur probatoire, les obligations réglementaires applicables, les exigences des bailleurs de fonds, les conventions de partenariat ainsi que les impératifs liés à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). L'Organisation veille à ce que les délais retenus permettent de répondre efficacement aux demandes des autorités compétentes, aux contrôles réglementaires, aux audits internes et externes, aux procédures judiciaires ainsi qu'aux besoins de gestion institutionnelle.

Sont notamment soumis à des règles spécifiques de conservation les statuts, règlements intérieurs, procès-verbaux des organes de gouvernance, conventions de partenariat, contrats, rapports d'activités, états financiers, livres comptables, pièces justificatives, relevés bancaires, dossiers d'adhésion, dossiers de cotisation, dossiers de dons, dossiers KYC, rapports d'audit, déclarations réglementaires, registres des opérations, journaux informatiques, documents relatifs aux paiements électroniques, archives numériques ainsi que les documents liés aux investigations de conformité et aux opérations suspectes.

Pendant toute la durée de conservation, les documents doivent demeurer complets, lisibles, authentiques, accessibles et protégés contre toute altération, suppression, perte ou destruction non autorisée. AGCE International met en œuvre des mesures techniques, organisationnelles et physiques garantissant la pérennité des informations, notamment des systèmes de sauvegarde, de redondance, de chiffrement, de contrôle des accès, de surveillance continue et de vérification régulière de l'intégrité des archives.

Les durées de conservation font l'objet d'une revue périodique afin de tenir compte des évolutions législatives, réglementaires, technologiques et organisationnelles. Toute modification des délais est validée par les autorités compétentes de l'Organisation et intégrée aux politiques documentaires officielles. Les collaborateurs concernés sont informés des nouvelles exigences afin d'assurer une application uniforme des règles de conservation.

À l'expiration des délais applicables, les documents sont évalués afin de déterminer s'ils doivent être conservés à des fins historiques, patrimoniales, institutionnelles ou juridiques, ou s'ils peuvent faire l'objet d'une destruction sécurisée. Aucune destruction ne peut intervenir lorsqu'un document est nécessaire dans le cadre d'une procédure judiciaire, d'un audit, d'une enquête administrative, d'un contrôle fiscal ou d'une investigation de conformité. Toute opération de destruction est autorisée, documentée, tracée et réalisée selon des méthodes garantissant l'impossibilité de reconstituer les informations supprimées.

Par l'application d'une politique rigoureuse relative aux durées de conservation, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit la disponibilité permanente des informations nécessaires à la gestion de ses activités, renforce sa sécurité juridique et financière, facilite les contrôles institutionnels et démontre son engagement en faveur d'une gouvernance responsable, transparente et conforme aux meilleures pratiques internationales.

8.44 Archivage physique

L'**archivage physique** constitue une composante essentielle du dispositif de conservation documentaire de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour objectif d'assurer la conservation durable, l'intégrité, la confidentialité, la disponibilité et la protection de l'ensemble des documents papier présentant une valeur administrative, juridique, comptable, financière, institutionnelle ou historique. Ce dispositif complète les mécanismes d'archivage numérique et

garantit la préservation des documents originaux lorsque leur conservation sous format physique demeure nécessaire ou imposée par la réglementation applicable.

L'Organisation conserve sous format papier les documents originaux présentant une valeur probatoire ou nécessitant une conservation matérielle. Sont notamment concernés les statuts, règlements, procès-verbaux des réunions statutaires, conventions de partenariat, contrats signés, titres de propriété, pièces comptables originales, justificatifs de paiement, relevés bancaires, dossiers d'adhésion, documents KYC, rapports d'audit, correspondances officielles, autorisations administratives, certificats, documents fiscaux ainsi que tout autre document dont l'original est requis à des fins légales ou institutionnelles.

Les archives physiques sont classées selon une nomenclature documentaire normalisée permettant leur identification, leur localisation rapide et leur consultation contrôlée. Chaque dossier est référencé au moyen d'un identifiant unique comportant notamment sa catégorie documentaire, sa date de création, son niveau de confidentialité, sa durée de conservation et le service responsable de sa gestion. Cette organisation facilite les recherches documentaires et garantit une gestion cohérente de l'ensemble des archives.

Les locaux destinés à l'archivage physique sont aménagés de manière à assurer une protection optimale contre les risques de dégradation, d'incendie, d'inondation, d'humidité, de poussière, de nuisibles, de vol, de perte ou d'accès non autorisé. L'Organisation veille à maintenir des conditions de conservation appropriées afin de préserver durablement la qualité et la lisibilité des documents. Les espaces d'archives font l'objet de contrôles réguliers portant sur leur sécurité, leur état de conservation et leur conformité aux procédures internes.

L'accès aux archives physiques est strictement réservé aux personnes expressément habilitées dans le cadre de leurs fonctions. Toute consultation, emprunt, reproduction, transfert ou restitution d'un document est enregistrée dans un registre de suivi garantissant une traçabilité complète des mouvements d'archives. Les documents confidentiels bénéficient de mesures de protection renforcées et ne peuvent être communiqués qu'aux personnes légalement autorisées.

Afin de limiter les risques de perte d'information, AGCE International peut procéder à la numérisation sécurisée de certains documents physiques. Cette opération ne dispense pas de la conservation des originaux lorsque celle-ci demeure exigée par la réglementation, les engagements contractuels ou les besoins institutionnels. Les copies numériques sont intégrées au système d'archivage électronique de l'Organisation et bénéficient des mêmes mesures de sécurité que les autres documents numériques.

Les archives physiques font l'objet de revues périodiques permettant de vérifier le respect des durées de conservation, d'identifier les documents pouvant être transférés en archives définitives ou détruits conformément aux procédures applicables, et de garantir l'actualisation permanente des inventaires documentaires. Toute destruction est autorisée, documentée et réalisée selon des procédés garantissant la confidentialité des informations contenues dans les documents concernés.

Par la mise en œuvre d'un système d'archivage physique structuré, sécurisé et conforme aux exigences réglementaires, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** protège durablement son patrimoine documentaire, renforce la fiabilité de ses activités administratives et financières, facilite les contrôles et les audits, et affirme son engagement permanent en faveur de la transparence, de la bonne gouvernance, de la conformité institutionnelle et de la préservation de sa mémoire organisationnelle.

8.45 Archivage électronique

L'**archivage électronique** constitue le dispositif organisé par lequel **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** conserve, protège, classe et rend accessibles les documents numériques produits ou reçus dans le cadre de ses activités institutionnelles, administratives, financières, comptables, juridiques, opérationnelles et technologiques. Il vise à garantir la pérennité des informations, leur intégrité, leur authenticité, leur lisibilité et leur valeur probante pendant toute la durée de conservation applicable.

1. Périmètre des documents concernés. L'archivage électronique couvre notamment les contrats, conventions, procès-verbaux, rapports, pièces comptables, factures, relevés bancaires, justificatifs de paiement, dossiers d'adhésion, documents KYC, dossiers de dons, registres financiers, rapports d'audit, déclarations réglementaires, courriels officiels, signatures électroniques, journaux informatiques, notifications de paiement, webhooks, pièces justificatives numérisées et documents relatifs aux investigations de conformité.

2. Classement et identification. Chaque document numérique est classé selon une nomenclature documentaire harmonisée. Il reçoit une référence unique, une date de création ou de réception, une catégorie, un niveau de confidentialité, une durée de conservation, un service responsable et, lorsque cela est nécessaire, une indication de version. Cette méthode permet d'éviter les doublons, les pertes de documents et les confusions entre versions provisoires et définitives.

3. Authenticité et intégrité. Les documents archivés doivent demeurer conformes à leur version d'origine. AGCE International met en œuvre des mécanismes techniques permettant de détecter toute modification non autorisée, notamment l'horodatage, les empreintes numériques, les signatures électroniques, les contrôles d'intégrité et la conservation des historiques de modification. Toute altération constatée fait l'objet d'une alerte et d'une investigation.

4. Lisibilité et pérennité. Les formats de fichiers retenus doivent permettre une consultation durable, indépendamment de l'évolution des logiciels et des équipements. L'Organisation prévoit, lorsque cela est nécessaire, des opérations de migration, de conversion ou de renouvellement des supports afin d'éviter l'obsolescence technologique et de maintenir l'accessibilité des archives.

5. Sauvegarde et redondance. Les archives électroniques font l'objet de sauvegardes régulières sur des infrastructures distinctes et sécurisées. La redondance des données permet de prévenir les pertes liées à une panne, une erreur humaine, une cyberattaque, un sinistre ou une indisponibilité technique. Les procédures de restauration sont testées périodiquement afin de vérifier leur efficacité.

6. Contrôle des accès. L'accès aux archives est attribué selon les fonctions, les responsabilités et le niveau d'habilitation de chaque utilisateur. Le principe du moindre privilège s'applique systématiquement. Toute consultation, modification, extraction, transmission ou suppression est enregistrée afin de garantir la traçabilité des opérations.

7. Numérisation des documents physiques. Les documents papier peuvent être numérisés selon une procédure garantissant la qualité, la complétude, la lisibilité et la fidélité de la copie électronique. La numérisation ne dispense toutefois pas de conserver l'original physique lorsque la réglementation, la valeur probatoire ou les exigences contractuelles l'imposent.

8. Suspension de destruction. Aucun document électronique ne peut être supprimé lorsqu'il est lié à un audit, une enquête, un contentieux, un contrôle réglementaire, une investigation LBC/FT ou une demande formulée par une autorité compétente. Dans ce cas, une mesure de conservation exceptionnelle est appliquée jusqu'à la clôture formelle de la procédure.

Par ce dispositif, AGCE International assure la continuité de sa mémoire institutionnelle, la fiabilité de ses preuves numériques et la disponibilité des informations nécessaires à la gouvernance, aux audits, aux contrôles et aux obligations de conformité.

8.46 Sécurisation

La **sécurisation de la conservation documentaire** regroupe l'ensemble des mesures physiques, techniques, organisationnelles et humaines destinées à protéger les archives de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** contre la perte, l'altération, la destruction, le vol, l'accès non autorisé, la divulgation, l'utilisation frauduleuse et toute atteinte susceptible d'affecter leur confidentialité, leur intégrité, leur disponibilité ou leur authenticité.

1. Classification des informations. Les documents sont classés selon leur degré de sensibilité, notamment public, interne, confidentiel ou strictement confidentiel. Le niveau attribué détermine les conditions d'accès, de stockage, de transmission, de reproduction, de partage et de destruction applicables.

2. Gestion des habilitations. Les droits d'accès sont accordés uniquement aux personnes dont les fonctions justifient la consultation ou le traitement des documents concernés. Toute habilitation doit être autorisée, documentée, révisée périodiquement et supprimée sans délai en cas de changement de fonction, de suspension, de départ ou de perte de confiance.

3. Authentification renforcée. L'accès aux archives sensibles est protégé par des identifiants individuels, des mots de passe robustes et, lorsque cela est requis, une authentification multifacteur. Les comptes partagés sont évités, afin que chaque opération puisse être attribuée à un utilisateur déterminé.

4. Chiffrement et protection des supports. Les archives numériques sensibles sont chiffrées pendant leur stockage et leur transmission. Les supports amovibles, équipements mobiles et sauvegardes externes sont également protégés afin de limiter les risques de fuite, de copie illicite ou d'exploitation frauduleuse.

5. Surveillance et journalisation. Les accès, téléchargements, suppressions, modifications, exportations et tentatives de connexion sont enregistrés dans des journaux sécurisés. Ces données permettent d'identifier les comportements inhabituels, les accès excessifs, les extractions massives et les tentatives de contournement des mesures de sécurité.

6. Protection contre les sinistres. Les archives physiques et électroniques sont protégées contre les incendies, les inondations, les variations climatiques, les pannes électriques, les défaillances matérielles, les logiciels malveillants et les attaques informatiques. Des plans de continuité et de reprise d'activité sont établis afin d'assurer la restauration rapide des documents essentiels.

7. Sécurité des prestataires. Tout prestataire chargé de l'hébergement, du stockage, de la numérisation, de la maintenance ou de la destruction documentaire doit présenter des garanties suffisantes en matière de confidentialité, de cybersécurité, de traçabilité et de conformité. Ses obligations sont formalisées contractuellement et peuvent faire l'objet de contrôles.

8. Gestion des incidents. Toute perte, fuite, altération, destruction ou consultation non autorisée doit être signalée immédiatement. L'Organisation procède à la sécurisation des systèmes, à la conservation des preuves, à l'analyse de l'incident, à l'évaluation de ses conséquences et à la mise en œuvre de mesures correctives. Les autorités et parties concernées sont informées lorsque les obligations applicables l'exigent.

9. Destruction sécurisée. À l'expiration des durées de conservation, les documents sont détruits selon des méthodes empêchant toute reconstitution. Les supports physiques sont broyés ou rendus illisibles, tandis que les données numériques sont supprimées de manière contrôlée, y compris sur les sauvegardes lorsque cela est techniquement possible et juridiquement autorisé.

Par l'application de ces mesures, **AGCE International – AGCE Canada** protège durablement son patrimoine documentaire, sécurise les informations de ses membres, bénéficiaires, donateurs et partenaires, et renforce la conformité, la transparence et la résilience de son dispositif institutionnel.

8.47 Confidentialité

La **confidentialité** constitue un principe fondamental de la politique de conservation documentaire de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle vise à garantir que l'ensemble des informations, documents, archives et données institutionnelles conservés par l'Organisation ne soient accessibles, consultés, utilisés, reproduits, communiqués ou diffusés qu'aux seules personnes légalement autorisées, conformément à leurs fonctions, à leurs responsabilités et aux exigences de la réglementation applicable. Cette politique participe directement à la protection des données personnelles, des informations financières, des secrets d'affaires, des données stratégiques ainsi qu'à la prévention du blanchiment de capitaux, du financement du terrorisme et de toute autre activité illicite.

1. Principe général de confidentialité. Tous les documents produits, reçus ou conservés par l'Organisation sont présumés confidentiels, sauf disposition contraire ou publication officiellement autorisée. Chaque collaborateur, administrateur, bénévole, consultant, partenaire ou prestataire est tenu à une obligation permanente de discrétion professionnelle concernant les informations auxquelles il accède dans l'exercice de ses fonctions.

2. Classification des informations. Les documents sont classifiés selon leur niveau de sensibilité afin d'adapter les mesures de protection appropriées. Cette classification permet notamment de distinguer les informations publiques, internes, confidentielles et strictement confidentielles. Le niveau retenu détermine les modalités d'accès, de diffusion, de reproduction, de conservation et de destruction des documents.

3. Protection des données sensibles. Les dossiers contenant des données personnelles, des informations bancaires, des pièces d'identification, des documents KYC, des rapports financiers, des dossiers disciplinaires, des enquêtes internes, des rapports d'audit ou toute autre information sensible bénéficient de mesures renforcées de sécurité. Leur consultation est strictement limitée aux personnes dont les missions rendent cet accès indispensable.

4. Obligation de confidentialité des utilisateurs. Toute personne autorisée à consulter ou traiter des documents de l'Organisation s'engage à préserver leur confidentialité, à ne pas les divulguer sans autorisation préalable et à mettre en œuvre toutes les précautions nécessaires afin d'éviter leur perte, leur copie illicite ou leur communication à des tiers non autorisés. Cette obligation demeure applicable après la cessation des fonctions, du contrat ou de la collaboration avec AGCE International.

5. Transmission sécurisée des informations. Les échanges de documents confidentiels s'effectuent exclusivement au moyen de canaux sécurisés, utilisant des mécanismes appropriés de chiffrement, d'authentification, de contrôle des destinataires et de traçabilité. Les informations sensibles ne doivent jamais être transmises au moyen de supports ou de services ne présentant pas un niveau de sécurité suffisant.

6. Gestion des incidents de confidentialité. Toute suspicion de fuite d'information, de divulgation accidentelle, de perte documentaire, de consultation non autorisée ou de violation de la confidentialité doit être signalée immédiatement aux responsables compétents. L'Organisation procède sans délai à l'analyse de l'incident, à la mise en œuvre de mesures correctives, à la conservation des preuves et, lorsque la réglementation l'impose, à la notification des autorités compétentes et des personnes concernées.

7. Sensibilisation et engagement. AGCE International organise régulièrement des actions de sensibilisation destinées à renforcer la culture de confidentialité auprès de l'ensemble de ses collaborateurs et partenaires. Des engagements écrits de confidentialité peuvent être exigés selon les responsabilités exercées et la nature des informations traitées.

Par l'application de cette politique de confidentialité, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** protège efficacement les informations confiées par ses membres, partenaires, donateurs, bénéficiaires et bailleurs de fonds, renforce la confiance accordée à l'Organisation et garantit une gestion documentaire conforme aux meilleures pratiques internationales de gouvernance, de cybersécurité et de conformité réglementaire.

8.48 Gestion des accès

La **gestion des accès** constitue un mécanisme essentiel de sécurisation de la conservation documentaire au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif d'assurer que seules les personnes dûment autorisées puissent accéder aux documents, aux archives, aux bases de données et aux systèmes documentaires de l'Organisation, selon le principe du besoin d'en connaître (« Need to Know ») et du moindre privilège (« Least Privilege »). Cette approche contribue à préserver l'intégrité, la confidentialité et la disponibilité des informations institutionnelles.

1. Attribution des droits d'accès. Les autorisations d'accès sont accordées exclusivement en fonction des missions, des responsabilités et du niveau d'habilitation de chaque utilisateur. Toute demande d'accès fait l'objet d'une validation formelle par les responsables compétents et d'un enregistrement dans les systèmes de gestion documentaire.

2. Gestion des profils utilisateurs. Chaque utilisateur dispose d'un identifiant personnel unique. Les profils sont définis selon les catégories de fonctions exercées, notamment les administrateurs, responsables financiers, responsables de conformité, responsables informatiques, gestionnaires documentaires, collaborateurs, auditeurs ou partenaires autorisés. Les comptes génériques ou partagés sont limités aux situations exceptionnelles dûment justifiées.

3. Contrôle des habilitations. Les droits d'accès sont régulièrement réexaminés afin de vérifier leur adéquation avec les fonctions réellement exercées. Toute évolution des

responsabilités, mutation, suspension, départ ou cessation de collaboration entraîne une mise à jour immédiate des habilitations afin d'éviter tout accès injustifié aux informations de l'Organisation.

4. Authentification sécurisée. L'accès aux systèmes documentaires est protégé par des mécanismes d'authentification robustes, comprenant notamment des mots de passe complexes, une authentification multifacteur (MFA), des certificats numériques ou tout autre dispositif garantissant un niveau élevé de sécurité. Les paramètres d'authentification sont régulièrement renforcés afin de faire face à l'évolution des menaces.

5. Traçabilité des accès. Toutes les opérations d'accès, de consultation, de modification, de téléchargement, d'impression, de partage ou de suppression de documents sont automatiquement enregistrées dans des journaux sécurisés. Ces enregistrements permettent d'assurer une traçabilité complète des activités, de faciliter les audits et de détecter rapidement tout comportement anormal ou toute tentative d'accès non autorisée.

6. Contrôle des accès physiques. Les locaux d'archives, salles serveurs et espaces de conservation documentaire sont protégés par des dispositifs de contrôle physique adaptés, tels que badges d'accès, registres de visiteurs, vidéosurveillance lorsque cela est autorisé, serrures sécurisées ou autres moyens permettant de limiter les accès aux seules personnes habilitées.

7. Révision et amélioration continue. Les procédures de gestion des accès font l'objet de contrôles réguliers, d'audits de sécurité et d'évaluations périodiques afin d'identifier les risques, de corriger les éventuelles faiblesses et d'améliorer en permanence le dispositif de protection documentaire. Les enseignements tirés des incidents et des évolutions technologiques sont intégrés dans les procédures internes afin de maintenir un niveau de sécurité élevé.

Par l'application rigoureuse de cette politique de gestion des accès, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que son patrimoine documentaire demeure accessible uniquement aux personnes autorisées, protège efficacement les informations sensibles contre tout accès illicite ou abusif et consolide son engagement en faveur de la bonne gouvernance, de la sécurité de l'information, de la conformité réglementaire et de la confiance de l'ensemble de ses parties prenantes.

8.49 Destruction sécurisée

La **destruction sécurisée des documents et des données** constitue la dernière étape du cycle de vie documentaire de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle vise à garantir que les documents arrivés au terme de leur durée légale, réglementaire, administrative, contractuelle ou opérationnelle de conservation soient éliminés de manière définitive, contrôlée, irréversible et traçable, tout en préservant la confidentialité des informations, la sécurité des données et les

intérêts de l'Organisation ainsi que de ses membres, partenaires, donateurs, bénéficiaires et bailleurs de fonds.

La destruction sécurisée est réalisée conformément aux principes de bonne gouvernance, de protection des données, de gestion documentaire, de cybersécurité et de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Elle ne peut intervenir qu'après vérification que les documents concernés ne présentent plus d'utilité administrative, financière, comptable, juridique, fiscale, historique ou probatoire et qu'aucune disposition légale, réglementaire, contractuelle ou décision d'une autorité compétente n'impose leur conservation.

1. Autorisation préalable. Toute destruction documentaire est précédée d'une procédure d'autorisation formelle. Les responsables compétents vérifient la nature des documents, leur durée de conservation, leur statut juridique, les éventuelles procédures en cours ainsi que l'absence de toute obligation de maintien des archives. Aucune destruction ne peut être effectuée sans validation préalable conformément aux procédures internes de l'Organisation.

2. Vérification des obligations de conservation. Avant toute opération, une analyse documentaire est réalisée afin de s'assurer que les documents ne sont pas concernés par un audit, une enquête, un contrôle réglementaire, une procédure judiciaire, une investigation LBC/FT, une demande d'une autorité compétente ou un contentieux susceptible de nécessiter leur production ultérieure. Dans ces situations, la destruction est immédiatement suspendue jusqu'à la clôture officielle des procédures concernées.

3. Destruction des archives physiques. Les documents papier sont détruits au moyen de procédés garantissant leur destruction irréversible. Selon la sensibilité des informations, les méthodes utilisées peuvent comprendre le broyage, le déchiquetage sécurisé, la pulvérisation, la compression industrielle ou tout autre procédé empêchant toute reconstitution totale ou partielle des documents détruits.

4. Destruction des archives électroniques. Les documents numériques sont supprimés au moyen de techniques permettant d'empêcher leur récupération, leur restauration ou leur réutilisation. La suppression simple des fichiers étant insuffisante, l'Organisation privilégie des méthodes d'effacement sécurisé, de réécriture des supports, de destruction logique ou physique des supports de stockage lorsque cela est nécessaire, conformément aux bonnes pratiques internationales en matière de sécurité de l'information.

5. Protection des supports informatiques. Les disques durs, serveurs, clés USB, cartes mémoire, bandes de sauvegarde, équipements mobiles et tout autre support contenant des informations confidentielles font l'objet d'une procédure spécifique de destruction ou d'effacement sécurisé avant leur réutilisation, leur cession, leur recyclage ou leur mise au rebut.

6. Traçabilité des opérations. Chaque opération de destruction est enregistrée dans un registre dédié précisant notamment la nature des documents détruits, leur catégorie documentaire, la date de destruction, la méthode utilisée, le responsable ayant autorisé

l'opération, les personnes ayant procédé à la destruction ainsi que toute information utile à la traçabilité et aux contrôles ultérieurs. Lorsque la destruction est confiée à un prestataire spécialisé, un certificat de destruction peut être exigé et conservé dans les archives administratives de l'Organisation.

7. Sécurité et confidentialité. Les opérations de destruction sont réalisées dans des conditions garantissant une confidentialité absolue. Les documents destinés à être détruits demeurent protégés jusqu'à leur élimination définitive et ne peuvent être laissés sans surveillance, accessibles au public ou manipulés par des personnes non autorisées.

8. Contrôle et audit. Les procédures de destruction sécurisée font l'objet de contrôles réguliers, de revues documentaires et d'audits internes ou externes destinés à vérifier leur conformité aux politiques institutionnelles, aux exigences réglementaires et aux meilleures pratiques internationales. Toute anomalie identifiée donne lieu à des mesures correctives, à une analyse des causes et, si nécessaire, à une révision des procédures applicables.

9. Amélioration continue. AGCE International veille à adapter en permanence ses méthodes de destruction documentaire aux évolutions technologiques, aux nouvelles menaces de cybersécurité, aux exigences réglementaires et aux recommandations des autorités compétentes. Les retours d'expérience issus des audits, des incidents de sécurité et des évaluations de conformité alimentent le processus d'amélioration continue de la politique documentaire.

Par l'application de cette politique de destruction sécurisée, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que les informations confidentielles ne puissent faire l'objet d'aucune divulgation, récupération ou utilisation frauduleuse après leur élimination, protège durablement son patrimoine informationnel, renforce la confiance de ses membres et partenaires et confirme son engagement en faveur d'une gouvernance exemplaire, d'une conformité réglementaire rigoureuse et d'une sécurité documentaire conforme aux meilleures pratiques internationales.

SECTION VI

PROTECTION DES LANCEURS D'ALERTE

8.50 Politique de signalement

La **Politique de signalement** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** constitue un mécanisme essentiel de gouvernance, de transparence, d'intégrité et de conformité. Elle établit un cadre institutionnel permettant à toute personne de signaler, en toute bonne foi et sans crainte de représailles, tout fait susceptible de constituer une violation des lois, des règlements, des politiques internes, des principes éthiques ou des obligations relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Cette politique traduit

l'engagement de l'Organisation à promouvoir une culture de responsabilité, de prévention des risques et d'amélioration continue.

1. Objet de la politique. La présente politique a pour objet d'encourager le signalement rapide des comportements, actes ou omissions susceptibles de porter atteinte à la légalité, à l'éthique, à la réputation, aux ressources, au patrimoine ou aux intérêts légitimes de l'Organisation. Elle vise à permettre une détection précoce des risques, une réaction appropriée et la mise en œuvre rapide des mesures correctives nécessaires.

2. Champ d'application. La politique s'applique à l'ensemble des administrateurs, dirigeants, membres, salariés, bénévoles, consultants, partenaires, prestataires, donateurs, bénéficiaires, représentants des antennes nationales et internationales, ainsi qu'à toute personne entretenant une relation professionnelle, contractuelle ou institutionnelle avec AGCE International. Toute personne concernée peut utiliser les dispositifs de signalement lorsqu'elle constate ou soupçonne raisonnablement une irrégularité.

3. Faits pouvant être signalés. Peuvent notamment faire l'objet d'un signalement les actes de fraude, corruption, blanchiment de capitaux, financement du terrorisme, détournement de fonds, falsification documentaire, conflits d'intérêts, abus de pouvoir, harcèlement, discrimination, violations des droits humains, atteintes à la protection des données, cyberattaques, violations des politiques internes, manquements aux obligations comptables ou financières, atteintes à l'environnement, comportements contraires au Code d'éthique ou toute autre situation présentant un risque significatif pour l'Organisation ou ses parties prenantes.

4. Principe de bonne foi. Les signalements doivent être effectués de bonne foi, sur la base d'éléments raisonnablement crédibles, même si les faits signalés ne sont pas ultérieurement confirmés. Aucun lanceur d'alerte agissant honnêtement ne peut être sanctionné au seul motif que l'enquête n'a pas permis d'établir l'existence d'une irrégularité. En revanche, tout signalement volontairement mensonger, diffamatoire ou manifestement abusif peut faire l'objet de mesures disciplinaires ou de poursuites conformément aux dispositions légales applicables.

5. Canaux de signalement. L'Organisation met à disposition plusieurs canaux sécurisés permettant la transmission des alertes, notamment une adresse électronique dédiée, un formulaire sécurisé accessible via les plateformes numériques officielles, un courrier confidentiel, une déclaration écrite auprès du Responsable de la Conformité ou de toute autre autorité interne désignée, ainsi que tout dispositif complémentaire garantissant la confidentialité des informations communiquées.

6. Confidentialité du signalement. L'identité du lanceur d'alerte, celle des personnes mises en cause ainsi que l'ensemble des informations recueillies dans le cadre du signalement sont protégées par des mesures strictes de confidentialité. L'accès au dossier est limité aux seules personnes chargées de son traitement, dans le respect des principes de nécessité, de proportionnalité et de protection des données personnelles.

7. Accusé de réception et traitement. Chaque signalement recevable fait l'objet d'un accusé de réception lorsque cela est possible, puis d'une analyse préliminaire destinée à évaluer sa recevabilité, son niveau de risque et les investigations nécessaires. Les enquêtes sont conduites de manière impartiale, objective, diligente et confidentielle, dans le respect des droits des personnes concernées et des règles de procédure interne.

8. Mesures de protection. AGCE International interdit toute forme de représailles, de discrimination, de menace, d'intimidation, de licenciement, de suspension, de rétrogradation, de harcèlement ou de traitement défavorable à l'encontre d'un lanceur d'alerte ayant effectué un signalement de bonne foi. Toute mesure de rétorsion constitue une violation grave des règles de gouvernance de l'Organisation et expose son auteur à des sanctions disciplinaires, contractuelles ou judiciaires.

9. Conservation et traçabilité. Les dossiers de signalement, les éléments de preuve, les rapports d'enquête, les décisions prises et les mesures correctives mises en œuvre sont conservés conformément à la politique de conservation documentaire de l'Organisation. Chaque étape du traitement est documentée afin de garantir la traçabilité, la transparence des investigations et la disponibilité des informations lors des audits ou contrôles réglementaires.

10. Amélioration continue. Les informations issues des signalements contribuent au renforcement du dispositif de contrôle interne, de gestion des risques et de conformité. Les enseignements tirés des investigations permettent d'identifier les causes profondes des dysfonctionnements, de renforcer les procédures, d'améliorer les contrôles, de développer les actions de sensibilisation et de consolider la culture d'intégrité au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**.

Par cette politique de signalement, l'Organisation affirme sa volonté de promouvoir un environnement institutionnel fondé sur l'éthique, la responsabilité, la transparence, la protection des personnes de bonne foi et la prévention de toute forme de fraude, de corruption, de blanchiment de capitaux, de financement du terrorisme ou d'atteinte aux valeurs fondamentales qui guident ses missions humanitaires, sociales et de développement durable.

8.51 Canaux sécurisés

La mise à disposition de **canaux sécurisés de signalement** constitue un élément fondamental du dispositif de protection des lanceurs d'alerte de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Ces mécanismes ont pour objectif de permettre à toute personne concernée de transmettre une alerte en toute sécurité, de manière confidentielle, sans risque de divulgation non autorisée de son identité et sans crainte de représailles. Ils participent au renforcement de la gouvernance, de la transparence, de l'intégrité institutionnelle et de la conformité aux exigences relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

1. Principe général. L'Organisation met à la disposition de l'ensemble de ses parties prenantes des moyens de communication sécurisés permettant de signaler tout fait susceptible de constituer une fraude, un acte de corruption, un conflit d'intérêts, une violation des politiques internes, une atteinte aux droits fondamentaux, une irrégularité financière, une cyberattaque ou toute autre situation présentant un risque pour l'Organisation.

2. Multiplicité des canaux. Afin de garantir l'accessibilité du dispositif, plusieurs moyens de signalement sont proposés, notamment une adresse électronique institutionnelle dédiée, un formulaire sécurisé accessible depuis les plateformes numériques officielles de l'Organisation, une correspondance écrite sous pli confidentiel, un entretien avec le Responsable de la Conformité ou toute autre autorité interne habilitée, ainsi que tout dispositif sécurisé pouvant être déployé dans les différentes antennes nationales et internationales de l'Organisation.

3. Sécurité des communications. Les canaux de signalement utilisent des mécanismes techniques destinés à préserver la confidentialité des informations transmises. Les communications sont protégées par des mesures appropriées telles que le chiffrement des échanges, l'authentification des utilisateurs habilités, la journalisation des accès, la protection contre les interceptions illicites et les contrôles d'intégrité garantissant que les informations reçues n'ont fait l'objet d'aucune modification non autorisée.

4. Protection de l'identité. L'identité du lanceur d'alerte, lorsqu'elle est connue, bénéficie d'une protection renforcée. Elle ne peut être révélée qu'aux seules personnes strictement habilitées à traiter le signalement ou lorsque cette communication est exigée par une autorité compétente dans le respect des dispositions légales applicables. Lorsque les circonstances le permettent, l'Organisation peut également recevoir des signalements anonymes, sous réserve que les informations communiquées soient suffisamment précises pour permettre leur analyse.

5. Accessibilité et égalité de traitement. Les canaux de signalement sont conçus pour être accessibles aux administrateurs, membres, salariés, bénévoles, partenaires, prestataires, bénéficiaires, donateurs et toute autre personne entretenant une relation avec AGCE International. Aucune discrimination ne peut être fondée sur la qualité de la personne effectuant le signalement, dès lors que celui-ci est réalisé de bonne foi.

6. Disponibilité permanente. Les dispositifs de signalement sont maintenus en état de fonctionnement afin de permettre la réception des alertes dans des délais compatibles avec la gravité des situations signalées. Des procédures de continuité sont prévues afin d'assurer leur disponibilité en cas d'incident technique ou de situation exceptionnelle.

7. Sensibilisation des utilisateurs. L'Organisation veille à informer régulièrement l'ensemble de ses parties prenantes de l'existence des canaux sécurisés, des modalités de leur utilisation, des garanties offertes aux lanceurs d'alerte et des principes de confidentialité applicables. Cette sensibilisation contribue au développement d'une culture d'intégrité et de responsabilité.

8. Contrôle et amélioration continue. Les canaux de signalement font l'objet d'évaluations régulières destinées à vérifier leur efficacité, leur niveau de sécurité, leur accessibilité et leur

conformité aux exigences réglementaires. Les enseignements issus des audits, des incidents et des retours d'expérience permettent d'améliorer continuellement le dispositif.

Par la mise en œuvre de canaux de signalement sécurisés, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit aux lanceurs d'alerte un environnement de confiance favorisant la remontée rapide des informations sensibles, le renforcement du contrôle interne et la prévention des risques institutionnels.

8.52 Réception des alertes

La **réception des alertes** constitue la première étape opérationnelle du processus de traitement des signalements au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Cette phase est conduite selon des principes d'impartialité, de confidentialité, de diligence, de traçabilité et de respect des droits des personnes concernées. Elle vise à garantir que chaque signalement reçu soit enregistré, analysé et orienté de manière appropriée, tout en préservant la sécurité du lanceur d'alerte et l'intégrité de la procédure.

1. Enregistrement des alertes. Toute alerte reçue par un canal officiel est immédiatement enregistrée dans un registre sécurisé des signalements. Cet enregistrement comprend notamment la date et l'heure de réception, le canal utilisé, la nature du signalement, le niveau de sensibilité, les pièces éventuellement transmises et un identifiant unique permettant d'assurer le suivi du dossier.

2. Vérification de recevabilité. Une analyse préliminaire est réalisée afin de vérifier que le signalement relève effectivement du champ d'application de la politique de signalement. Cette vérification porte notamment sur la nature des faits dénoncés, la cohérence des informations fournies, l'existence éventuelle d'éléments justificatifs et le niveau de risque identifié.

3. Confidentialité du traitement. Dès la réception de l'alerte, toutes les informations communiquées sont protégées par des mesures strictes de confidentialité. Seules les personnes spécialement habilitées à traiter le dossier peuvent accéder aux informations recueillies. Toute divulgation non autorisée est strictement interdite et peut donner lieu à des mesures disciplinaires ou judiciaires.

4. Accusé de réception. Lorsque les coordonnées du lanceur d'alerte sont connues et que les circonstances le permettent, un accusé de réception est adressé dans un délai raisonnable afin de confirmer la bonne prise en charge du signalement. Cette communication ne préjuge ni de la recevabilité définitive ni des conclusions qui pourront être tirées de l'enquête.

5. Qualification du niveau de risque. Les alertes sont classées selon leur gravité, leur urgence et leur impact potentiel sur l'Organisation. Une attention particulière est accordée aux signalements relatifs au blanchiment de capitaux, au financement du terrorisme, à la fraude

financière, à la corruption, aux violations graves des droits humains, aux cyberattaques ou à toute situation susceptible de compromettre la continuité des activités.

6. Conservation des éléments de preuve. Dès la réception de l'alerte, toutes les informations, documents et éléments matériels transmis sont sécurisés afin d'éviter toute perte, altération ou destruction. Les preuves recueillies sont conservées conformément à la politique de conservation documentaire et aux règles de protection des données applicables.

7. Orientation vers les autorités compétentes. Après l'analyse de recevabilité, le dossier est transmis au Responsable de la Conformité ou à l'instance interne compétente pour la conduite des investigations. Lorsque la nature des faits l'exige, l'Organisation peut également transmettre le signalement aux autorités administratives, judiciaires ou réglementaires compétentes, dans le respect des obligations légales et de la confidentialité.

8. Traçabilité et suivi. Chaque étape du processus de réception est documentée afin de garantir la traçabilité complète des opérations réalisées. Les informations enregistrées permettent d'assurer le suivi du dossier, de faciliter les audits internes et externes, de démontrer le respect des procédures institutionnelles et d'alimenter les mécanismes d'amélioration continue du dispositif de conformité.

Par cette procédure de réception des alertes, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit un traitement rigoureux, sécurisé et impartial des signalements, favorise la détection précoce des risques, renforce l'efficacité de son système de contrôle interne et affirme son engagement constant en faveur de l'éthique, de la transparence, de la bonne gouvernance et de la conformité aux meilleures pratiques internationales.

8.53 Protection contre les représailles

La **protection contre les représailles** constitue un principe fondamental de la politique de protection des lanceurs d'alerte de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle garantit que toute personne effectuant un signalement de bonne foi bénéficie d'une protection effective contre toute mesure de rétorsion, de discrimination, d'intimidation ou de traitement défavorable résultant directement ou indirectement de son alerte. Cette politique vise à instaurer un climat de confiance favorisant la remontée des informations essentielles à la prévention des risques, à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), ainsi qu'au renforcement de la gouvernance, de la transparence et de l'intégrité institutionnelle.

1. Principe de non-représailles. Aucun administrateur, dirigeant, membre, salarié, bénévole, consultant, partenaire, prestataire, donateur ou bénéficiaire ayant effectué un signalement de bonne foi ne peut faire l'objet de sanctions, de menaces, de pressions ou de mesures défavorables en raison de son alerte. Cette protection s'applique indépendamment du fait que les éléments signalés soient ou non confirmés à l'issue des investigations.

2. Interdiction des mesures de rétorsion. Sont notamment interdites toute forme de licenciement, suspension, rétrogradation, refus de promotion, modification abusive des fonctions, réduction de responsabilités, rupture de contrat, intimidation, harcèlement, discrimination, exclusion, diffamation, isolement professionnel, refus d'accès aux ressources de l'Organisation, dégradation volontaire des conditions de travail ou toute autre mesure susceptible de porter préjudice au lanceur d'alerte.

3. Protection des personnes associées. La protection peut également être étendue, lorsque les circonstances le justifient, aux personnes ayant contribué au signalement, aux témoins, aux personnes ayant fourni des informations utiles, ainsi qu'aux collaborateurs ou proches susceptibles de subir des représailles en raison de leur lien avec le lanceur d'alerte.

4. Mesures conservatoires. Lorsqu'un risque de représailles est identifié, AGCE International peut mettre en œuvre des mesures temporaires de protection, telles que l'adaptation des conditions de travail, la limitation de l'accès à certaines informations sensibles, la réorganisation des circuits hiérarchiques, la protection renforcée des données personnelles ou toute autre mesure destinée à préserver la sécurité et les intérêts du lanceur d'alerte.

5. Signalement des représailles. Toute personne estimant être victime d'une mesure de rétorsion peut saisir immédiatement les autorités internes compétentes. Ces signalements bénéficient du même niveau de confidentialité et donnent lieu à une analyse prioritaire afin d'identifier les faits, de mettre fin aux représailles éventuelles et d'engager les mesures correctives appropriées.

6. Mesures disciplinaires. Toute personne reconnue responsable d'actes de représailles ou de tentatives d'intimidation s'expose à des mesures disciplinaires pouvant aller de l'avertissement à la cessation de toute collaboration avec l'Organisation, sans préjudice des poursuites civiles, administratives ou pénales prévues par les lois applicables.

7. Suivi des situations. Les responsables de la conformité assurent un suivi régulier des situations concernant les lanceurs d'alerte afin de vérifier qu'aucune mesure défavorable n'est intervenue après le signalement. Ce suivi peut inclure des entretiens confidentiels, des contrôles documentaires et des évaluations des conditions de collaboration.

8. Sensibilisation institutionnelle. L'Organisation développe une culture de respect des lanceurs d'alerte au moyen d'actions de formation, de sensibilisation et de communication destinées à rappeler les principes de non-représailles, les obligations des responsables hiérarchiques et les conséquences disciplinaires attachées à toute violation de cette politique.

9. Amélioration continue. Les procédures de protection contre les représailles sont régulièrement évaluées à partir des retours d'expérience, des audits, des enquêtes internes et des évolutions réglementaires afin de renforcer en permanence leur efficacité et leur conformité aux meilleures pratiques internationales.

Par cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme que la protection des lanceurs d'alerte constitue une responsabilité institutionnelle majeure et un élément indispensable au maintien d'une gouvernance exemplaire, d'une culture d'intégrité et d'un environnement de travail fondé sur la confiance, la responsabilité et le respect des droits fondamentaux.

8.54 Confidentialité

La **confidentialité** constitue l'une des garanties essentielles offertes par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** dans le cadre de son dispositif de protection des lanceurs d'alerte. Elle a pour finalité de préserver l'identité des personnes concernées, la sécurité des informations communiquées, l'intégrité des investigations et les droits de l'ensemble des parties impliquées. Le respect de ce principe est indispensable pour encourager les signalements de bonne foi, prévenir les représailles et garantir la crédibilité du dispositif institutionnel de conformité.

1. Protection de l'identité. L'identité du lanceur d'alerte, des témoins, des personnes ayant participé au signalement ainsi que des personnes mises en cause est protégée durant l'ensemble de la procédure. Elle ne peut être communiquée qu'aux seules personnes expressément habilitées à traiter le dossier ou lorsque cette divulgation est imposée par une autorité compétente conformément aux dispositions légales applicables.

2. Confidentialité des informations. Toutes les données, déclarations, documents, pièces justificatives, éléments de preuve et rapports d'enquête sont traités comme des informations strictement confidentielles. Leur accès est limité aux personnes dont les fonctions rendent cette consultation indispensable au traitement du dossier.

3. Accès restreint aux dossiers. Les dossiers de signalement sont conservés dans des environnements physiques et numériques hautement sécurisés. Les droits d'accès sont attribués selon le principe du moindre privilège et font l'objet d'une révision régulière. Toute consultation, modification ou transmission des informations est enregistrée afin d'assurer une traçabilité complète.

4. Protection des communications. Les échanges relatifs aux signalements sont réalisés au moyen de canaux sécurisés bénéficiant de mécanismes de chiffrement, d'authentification forte, de contrôle des accès et de journalisation. Les informations sensibles ne peuvent être transmises par des moyens non sécurisés ou accessibles à des personnes non autorisées.

5. Devoir de discrétion. Les personnes chargées de recevoir, d'analyser ou d'instruire les signalements sont soumises à une obligation stricte de confidentialité. Elles s'engagent à ne divulguer aucune information obtenue dans le cadre de leurs missions, sauf dans les cas prévus par la loi ou autorisés par les procédures internes de l'Organisation.

6. Conservation sécurisée. Les dossiers de signalement sont conservés conformément à la politique de conservation documentaire de l'Organisation. Ils bénéficient de mesures renforcées de protection contre la perte, l'altération, la divulgation, le vol ou l'accès non autorisé, pendant toute la durée de conservation applicable.

7. Violation de la confidentialité. Toute divulgation non autorisée d'informations relatives à un signalement constitue une faute grave susceptible d'entraîner des mesures disciplinaires, contractuelles ou judiciaires. L'Organisation met en œuvre sans délai les actions nécessaires pour limiter les conséquences de toute atteinte à la confidentialité et renforcer les mesures de sécurité.

8. Révision du dispositif. Les mécanismes de confidentialité font l'objet de contrôles périodiques, d'audits de conformité et d'évaluations régulières afin de vérifier leur efficacité, leur adéquation avec l'évolution des risques et leur conformité aux exigences légales et réglementaires applicables.

Par l'application de cette politique de confidentialité, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit aux lanceurs d'alerte un environnement sécurisé favorisant la libre expression des préoccupations légitimes, protège les droits de l'ensemble des personnes concernées et renforce durablement la confiance dans son dispositif de gouvernance, de conformité et de prévention des risques institutionnels.

8.55 Traitement des signalements

Le **traitement des signalements** constitue l'étape centrale du dispositif de protection des lanceurs d'alerte mis en place par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour objectif de garantir qu'à compter de sa réception, chaque signalement fasse l'objet d'une analyse rigoureuse, impartiale, confidentielle, diligente et documentée, conformément aux principes de bonne gouvernance, d'intégrité, de transparence, de protection des droits des personnes concernées et de conformité aux exigences relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

1. Ouverture du dossier. Dès qu'un signalement est déclaré recevable, un dossier confidentiel est ouvert et enregistré dans le registre officiel des signalements. Un identifiant unique lui est attribué afin d'assurer la traçabilité complète de l'ensemble des opérations réalisées jusqu'à sa clôture.

2. Désignation des responsables. Le traitement du dossier est confié exclusivement aux personnes spécialement habilitées, notamment le Responsable de la Conformité, le Responsable du Contrôle Interne, le Comité d'Éthique, le Comité de Conformité ou toute autre autorité compétente désignée par les organes de gouvernance de l'Organisation. Les personnes présentant un conflit d'intérêts sont immédiatement écartées de la procédure.

3. Analyse préliminaire. Une première évaluation est effectuée afin d'apprécier la nature des faits signalés, leur gravité, les risques encourus par l'Organisation, les éléments de preuve disponibles ainsi que les investigations complémentaires à réaliser. Cette analyse permet de déterminer le niveau de priorité du traitement.

4. Conduite des investigations. Les investigations sont réalisées avec impartialité, objectivité, indépendance et confidentialité. Elles peuvent comprendre l'examen de documents, l'analyse de données comptables et financières, la consultation de journaux informatiques, la réalisation d'entretiens, la collecte de témoignages, l'analyse des opérations concernées ainsi que toute autre mesure légalement autorisée permettant d'établir les faits.

5. Respect des droits des personnes concernées. Les investigations sont conduites dans le respect des droits fondamentaux des personnes mises en cause, notamment le principe du contradictoire lorsque celui-ci est applicable, la présomption de bonne foi, la protection des données personnelles et la confidentialité des informations recueillies.

6. Conservation des preuves. Toutes les informations, pièces justificatives, témoignages, rapports d'analyse, données électroniques et autres éléments de preuve sont sécurisés, conservés et documentés conformément aux politiques de conservation documentaire de l'Organisation afin d'assurer leur intégrité et leur valeur probatoire.

7. Mesures conservatoires. Lorsque les circonstances l'exigent, des mesures temporaires peuvent être prises afin de protéger les intérêts de l'Organisation, préserver les preuves, limiter les risques de fraude, empêcher la poursuite d'une irrégularité ou garantir la sécurité des personnes concernées, sans préjuger des conclusions définitives de l'enquête.

8. Décision et recommandations. À l'issue des investigations, un rapport motivé est établi présentant les faits constatés, les analyses réalisées, les conclusions retenues et les recommandations formulées. Selon les résultats obtenus, l'Organisation peut mettre en œuvre des mesures correctives, disciplinaires, organisationnelles, contractuelles ou transmettre le dossier aux autorités administratives, judiciaires ou réglementaires compétentes lorsque la loi l'exige.

9. Traçabilité et amélioration continue. L'ensemble des étapes du traitement est enregistré dans les systèmes documentaires sécurisés de l'Organisation. Les enseignements tirés des dossiers traités sont intégrés aux dispositifs de contrôle interne, de gestion des risques, de conformité et de prévention afin de renforcer continuellement les mécanismes de gouvernance et de protection institutionnelle.

Par cette procédure, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit un traitement professionnel, impartial et conforme des signalements, favorisant la prévention des risques, la protection des lanceurs d'alerte et le maintien d'un environnement institutionnel fondé sur l'intégrité, la responsabilité et la transparence.

8.56 Clôture des dossiers

La **clôture des dossiers de signalement** marque l'achèvement du processus d'examen des alertes au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Cette étape est réalisée uniquement lorsque l'ensemble des investigations nécessaires a été conduit, que les éléments de preuve ont été analysés, que les décisions appropriées ont été prises et que toutes les mesures de suivi jugées nécessaires ont été engagées. Elle garantit une conclusion formelle, documentée et traçable de chaque dossier, conformément aux principes de gouvernance, de transparence, de conformité et de protection des droits des personnes concernées.

1. Conditions de clôture. Un dossier ne peut être clôturé qu'après la finalisation des investigations, l'évaluation complète des faits signalés, la formulation des conclusions officielles et la validation des décisions par les autorités internes compétentes. Aucune clôture ne peut intervenir tant que des investigations complémentaires demeurent nécessaires ou qu'une procédure externe est en cours.

2. Rapport final. Un rapport de clôture est établi pour chaque dossier. Ce document présente notamment le contexte du signalement, les investigations réalisées, les éléments de preuve examinés, les analyses effectuées, les conclusions retenues, les mesures adoptées ainsi que les recommandations destinées à prévenir le renouvellement de situations similaires.

3. Décisions institutionnelles. Selon les résultats de l'enquête, AGCE International peut décider de classer le dossier sans suite, de mettre en œuvre des mesures correctives, des actions disciplinaires, des améliorations organisationnelles, des renforcements du contrôle interne, des actions de formation ou, lorsque les circonstances le justifient, de transmettre les informations aux autorités administratives, judiciaires ou réglementaires compétentes.

4. Information du lanceur d'alerte. Lorsque cela est possible, compatible avec les exigences de confidentialité et autorisé par la réglementation applicable, le lanceur d'alerte est informé de la clôture du dossier ainsi que de l'issue générale du traitement, sans divulguer d'informations confidentielles susceptibles de porter atteinte aux droits des autres personnes concernées ou aux intérêts de l'Organisation.

5. Archivage sécurisé. À la clôture du dossier, l'ensemble des documents, rapports, preuves, décisions et correspondances est intégré au système officiel de conservation documentaire de l'Organisation. Les dossiers sont archivés dans des conditions garantissant leur confidentialité, leur intégrité, leur disponibilité et leur traçabilité pendant toute la durée de conservation applicable.

6. Suivi des mesures correctives. La clôture administrative du dossier ne met pas fin aux obligations de suivi. Les responsables compétents veillent à la mise en œuvre effective des mesures correctives décidées, évaluent leur efficacité et procèdent, si nécessaire, à des contrôles complémentaires afin de prévenir la réapparition des dysfonctionnements constatés.

7. Protection continue des personnes. La clôture du dossier ne met pas fin aux mesures de protection accordées au lanceur d'alerte lorsqu'un risque de représailles subsiste. L'Organisation continue de veiller au respect de ses droits et au maintien des garanties prévues par la présente politique.

8. Retour d'expérience et amélioration continue. Chaque dossier clôturé fait l'objet d'une analyse rétrospective destinée à identifier les enseignements utiles à l'amélioration des procédures internes, du contrôle interne, de la gestion des risques, de la conformité et de la politique de protection des lanceurs d'alerte. Les recommandations issues de ces analyses alimentent les programmes de formation, les dispositifs de sensibilisation et les révisions périodiques des politiques institutionnelles.

9. Contrôle et audit. Les dossiers clôturés peuvent être examinés dans le cadre des audits internes, des audits externes ou des contrôles réglementaires afin de vérifier la conformité des procédures appliquées, la qualité des investigations, la pertinence des décisions prises et l'efficacité globale du dispositif de signalement.

Par cette procédure de clôture, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** assure une gestion complète, transparente et sécurisée des signalements, renforce la crédibilité de son système de protection des lanceurs d'alerte et confirme son engagement permanent en faveur d'une gouvernance responsable, d'une conformité exemplaire et d'une culture institutionnelle fondée sur l'éthique et l'intégrité.

SECTION VII

FORMATION ET SENSIBILISATION

8.57 Objectifs

La **formation et la sensibilisation** constituent des piliers essentiels du dispositif de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elles permettent de développer une culture institutionnelle fondée sur l'éthique, la transparence, la responsabilité, la vigilance et le respect des obligations légales, réglementaires et internes relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). L'Organisation considère que la maîtrise des risques ne repose pas uniquement sur les procédures et les contrôles techniques, mais également sur les compétences, les connaissances et l'engagement de l'ensemble des personnes qui participent à ses activités au Cameroun, au Canada ainsi que dans ses représentations nationales et internationales.

La présente politique de formation poursuit une démarche permanente d'amélioration des connaissances, de prévention des risques, de professionnalisation des pratiques et de consolidation du système de gouvernance. Elle vise à garantir que chaque administrateur,

dirigeant, membre, employé, bénévole, consultant, partenaire, prestataire et représentant institutionnel comprennent pleinement ses responsabilités en matière de conformité et soit en mesure d'identifier, de prévenir, de signaler et de gérer efficacement toute situation susceptible d'exposer l'Organisation à un risque juridique, financier, opérationnel ou réputationnel.

1. Développer une culture de conformité. Les programmes de formation ont pour premier objectif de promouvoir une culture institutionnelle dans laquelle le respect des lois, des règlements, des politiques internes, du Code d'éthique et des principes de bonne gouvernance constitue une responsabilité partagée par l'ensemble des parties prenantes de l'Organisation.

2. Renforcer les compétences professionnelles. Les actions de formation permettent aux participants d'acquérir les connaissances techniques et réglementaires nécessaires pour exercer leurs fonctions conformément aux exigences de la LBC/FT, de la gouvernance financière, de la gestion documentaire, de la cybersécurité, de la protection des données personnelles et du contrôle interne.

3. Identifier les risques. Les formations visent à développer la capacité des participants à reconnaître les indicateurs de fraude, de corruption, de blanchiment de capitaux, de financement du terrorisme, de conflits d'intérêts, de cybercriminalité, de falsification documentaire et de toute autre situation susceptible de compromettre les missions ou la réputation de l'Organisation.

4. Maîtriser les procédures internes. Chaque participant est formé à l'application correcte des politiques, procédures, mécanismes de contrôle, circuits de validation, obligations de vigilance, procédures de signalement, dispositifs de protection des lanceurs d'alerte et règles de conservation documentaire adoptés par AGCE International.

5. Favoriser une réaction appropriée. Les programmes de sensibilisation permettent aux collaborateurs de connaître les comportements à adopter face à une situation inhabituelle, une opération suspecte ou un manquement aux règles internes, afin d'assurer une réaction rapide, proportionnée et conforme aux procédures institutionnelles.

6. Renforcer la responsabilité individuelle et collective. La formation rappelle que chaque personne intervenant au sein de l'Organisation participe activement à la prévention des risques et à la protection des ressources institutionnelles. Le respect des obligations de conformité constitue un devoir professionnel et éthique applicable à tous les niveaux de responsabilité.

7. Accompagner les évolutions réglementaires. Les contenus pédagogiques sont régulièrement actualisés afin de tenir compte des évolutions des législations nationales et internationales, des recommandations des autorités compétentes, des nouvelles normes de conformité, des innovations technologiques ainsi que de l'évolution des menaces liées au blanchiment de capitaux, au financement du terrorisme et à la criminalité financière.

8. Développer une culture de vigilance permanente. Les actions de sensibilisation encouragent chaque acteur à adopter une attitude proactive fondée sur l'observation, la

prévention, le respect des procédures et le signalement des situations présentant un risque pour l'Organisation. Cette vigilance quotidienne contribue à renforcer la résilience institutionnelle et la capacité d'anticipation face aux menaces émergentes.

9. Promouvoir l'amélioration continue. Les formations s'inscrivent dans une démarche d'amélioration permanente des compétences institutionnelles. Les retours d'expérience, les résultats des audits, les incidents de conformité, les exercices pratiques et les évaluations régulières sont intégrés dans les programmes afin d'assurer leur adaptation constante aux besoins de l'Organisation.

10. Renforcer la confiance des parties prenantes. En investissant durablement dans la formation et la sensibilisation, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** démontre son engagement à maintenir les plus hauts standards de gouvernance, de transparence et de conformité. Cette démarche contribue à renforcer la crédibilité de l'Organisation auprès de ses membres, partenaires, donateurs, bénéficiaires, institutions publiques, autorités de contrôle et bailleurs de fonds nationaux et internationaux.

Par la mise en œuvre de ces objectifs stratégiques, AGCE International fait de la formation un levier essentiel de prévention, de responsabilisation et d'excellence institutionnelle. Elle consolide ainsi une culture organisationnelle où chaque acteur dispose des connaissances, des compétences et des outils nécessaires pour contribuer activement à la protection de l'Organisation, à la maîtrise des risques et au respect des exigences nationales et internationales en matière de conformité, d'intégrité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

8.58 Personnel

Le personnel de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** occupe une place centrale dans la mise en œuvre du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). À ce titre, l'Organisation veille à ce que chaque salarié, collaborateur, bénévole, consultant, prestataire intégré aux activités opérationnelles ainsi que toute personne exerçant des fonctions permanentes ou temporaires dispose des connaissances, des compétences et des outils nécessaires pour exercer ses responsabilités dans le respect des exigences légales, réglementaires et institutionnelles. La formation du personnel constitue un investissement stratégique destiné à renforcer la maîtrise des risques, la qualité des contrôles internes, la conformité des opérations et la protection de la réputation de l'Organisation.

1. Formation d'intégration. Toute personne rejoignant AGCE International bénéficie, dès sa prise de fonction, d'un programme d'intégration portant sur les principes de gouvernance, le Code d'éthique, les politiques de conformité, les règles de contrôle interne, la lutte contre le blanchiment de capitaux et le financement du terrorisme, la protection des données personnelles ainsi que les procédures applicables à son domaine d'activité.

2. Formation continue. Le personnel participe régulièrement à des sessions de formation destinées à maintenir ses connaissances à jour et à renforcer ses compétences face à l'évolution des risques, des technologies, des réglementations nationales et internationales ainsi que des procédures internes de l'Organisation.

3. Adaptation aux fonctions exercées. Les contenus pédagogiques sont adaptés aux responsabilités de chaque catégorie de personnel. Les collaborateurs occupant des fonctions financières, comptables, administratives, numériques, juridiques, logistiques ou de gestion des partenariats bénéficient de formations spécifiques tenant compte des risques propres à leurs activités.

4. Identification des risques. Les formations permettent au personnel d'identifier les opérations inhabituelles, les comportements suspects, les tentatives de fraude, les conflits d'intérêts, les actes de corruption, les cybermenaces, les manipulations documentaires et tout indice pouvant révéler un risque de blanchiment de capitaux ou de financement du terrorisme.

5. Maîtrise des procédures internes. Chaque collaborateur est formé à l'application des procédures de vigilance, de contrôle interne, de conservation documentaire, de sécurité des paiements, de protection des lanceurs d'alerte, de gestion des incidents et de signalement des opérations suspectes.

6. Responsabilisation individuelle. Chaque membre du personnel demeure personnellement responsable du respect des politiques internes dans l'exercice de ses fonctions. Il lui appartient d'appliquer les procédures en vigueur, de préserver la confidentialité des informations traitées et de signaler sans délai toute situation présentant un risque pour l'Organisation.

7. Évaluation des connaissances. Les formations peuvent être complétées par des évaluations, des exercices pratiques, des études de cas ou des simulations permettant de mesurer le niveau de compréhension des participants et d'identifier les besoins complémentaires en renforcement des capacités.

8. Sensibilisation permanente. En complément des formations formelles, l'Organisation organise des campagnes régulières de sensibilisation, diffuse des notes d'information, des guides pratiques, des rappels réglementaires et des retours d'expérience afin de maintenir un niveau élevé de vigilance au sein des équipes.

9. Suivi et amélioration continue. Les programmes de formation font l'objet d'une évaluation périodique afin de mesurer leur efficacité, d'intégrer les enseignements issus des audits, des incidents de conformité et des évolutions réglementaires, et d'assurer leur amélioration continue.

Par cette politique de formation du personnel, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme que le développement des compétences constitue un levier essentiel de prévention des risques, de

renforcement de la conformité et de consolidation d'une culture institutionnelle fondée sur l'intégrité, la responsabilité et l'excellence opérationnelle.

8.59 Administrateurs

Les **administrateurs** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** exercent une responsabilité stratégique dans la définition, la supervision et le contrôle du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). En raison de leurs fonctions de gouvernance, ils doivent disposer d'une compréhension approfondie des risques institutionnels, des exigences réglementaires et des meilleures pratiques internationales afin d'assurer une direction efficace, transparente et conforme aux objectifs de l'Organisation.

1. Formation spécifique des administrateurs. Chaque administrateur bénéficie d'une formation adaptée à ses responsabilités portant notamment sur la gouvernance institutionnelle, la conformité réglementaire, la gestion des risques, le contrôle interne, la lutte contre le blanchiment de capitaux et le financement du terrorisme, les obligations fiduciaires, la protection des données et les principes d'éthique.

2. Compréhension des responsabilités fiduciaires. Les administrateurs sont sensibilisés aux responsabilités civiles, administratives et, le cas échéant, pénales pouvant découler de leurs décisions ou de leurs omissions dans l'exercice de leurs fonctions de gouvernance.

3. Supervision du dispositif de conformité. Les formations leur permettent de contrôler efficacement les politiques de conformité, d'évaluer les rapports présentés par les responsables compétents, de suivre les indicateurs de risques et de s'assurer de l'efficacité globale des mécanismes de contrôle interne.

4. Lecture et interprétation des rapports. Les administrateurs développent leur capacité à analyser les rapports d'audit, les rapports financiers, les rapports de conformité, les évaluations des risques, les signalements de lanceurs d'alerte et les recommandations formulées par les organes de contrôle internes ou externes.

5. Gestion des risques stratégiques. Les programmes de formation renforcent leur aptitude à identifier les risques émergents susceptibles d'affecter l'Organisation, notamment ceux liés à la criminalité financière, aux technologies numériques, à la cybersécurité, aux partenariats internationaux, aux financements et aux opérations transfrontalières.

6. Prise de décision responsable. Les administrateurs sont formés à intégrer les exigences de conformité, d'éthique, de transparence et de gestion des risques dans l'ensemble des décisions stratégiques prises au sein des organes de gouvernance.

7. Actualisation permanente des connaissances. Compte tenu de l'évolution constante des normes internationales, les administrateurs participent régulièrement à des séances de mise à

jour portant sur les nouvelles réglementations, les recommandations des autorités compétentes, les standards internationaux de gouvernance ainsi que les nouvelles menaces identifiées.

8. Évaluation des compétences. L'Organisation procède périodiquement à l'évaluation des connaissances et des besoins de formation des administrateurs afin d'assurer le maintien d'un niveau élevé de compétence au sein des organes décisionnels.

9. Promotion d'une culture d'exemplarité. Les administrateurs ont la responsabilité de promouvoir, par leurs décisions et leur comportement, une culture institutionnelle fondée sur l'intégrité, la transparence, la responsabilité, la redevabilité et le respect des obligations de conformité. Ils constituent un modèle de référence pour l'ensemble des collaborateurs, partenaires et représentants de l'Organisation.

Par cette politique de formation des administrateurs, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce les capacités de ses organes de gouvernance, améliore la qualité de ses décisions stratégiques et consolide un système de gouvernance conforme aux meilleures pratiques nationales et internationales en matière de conformité, de gestion des risques et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

8.60 Responsables financiers

Les **responsables financiers** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** occupent une fonction essentielle dans la prévention, la détection et la gestion des risques liés au blanchiment de capitaux, au financement du terrorisme (LBC/FT), à la fraude financière et aux autres infractions économiques. En raison de leur accès privilégié aux opérations financières, aux systèmes comptables, aux moyens de paiement et aux informations budgétaires, ils sont soumis à un programme de formation renforcé leur permettant d'exercer leurs responsabilités avec un niveau élevé de compétence, de vigilance et de professionnalisme. Cette politique vise à garantir que chaque responsable financier maîtrise les obligations légales, réglementaires et institutionnelles applicables, tout en contribuant activement au renforcement du système global de gouvernance financière de l'Organisation.

1. Formation spécialisée obligatoire. Tout responsable financier bénéficie, dès sa prise de fonction, d'une formation approfondie portant sur la réglementation LBC/FT, les normes comptables, les procédures financières internes, les contrôles budgétaires, les obligations de vigilance, la gestion des risques, les exigences de conformité ainsi que les politiques institutionnelles applicables.

2. Maîtrise des procédures financières. Les formations permettent aux responsables financiers de maîtriser les procédures relatives à la gestion des recettes, des dépenses, des dons, des cotisations, des subventions, des paiements électroniques, des virements bancaires,

des rapprochements comptables, des validations hiérarchiques et de l'ensemble des mécanismes de contrôle financier mis en œuvre par l'Organisation.

3. Détection des opérations atypiques. Les responsables financiers sont formés à identifier les opérations inhabituelles, les transactions complexes, les mouvements financiers incohérents, les tentatives de fraude, les opérations suspectes, les manipulations comptables et tout indice pouvant révéler un risque de blanchiment de capitaux, de financement du terrorisme ou de détournement de ressources.

4. Utilisation sécurisée des outils financiers. Les programmes de formation couvrent également l'utilisation sécurisée des plateformes bancaires, des solutions de paiement électronique, des logiciels comptables, des systèmes d'information financière et des dispositifs d'authentification renforcée afin de limiter les risques de fraude, de cybercriminalité et d'accès non autorisé.

5. Contrôle interne et séparation des fonctions. Les responsables financiers sont sensibilisés au respect des principes de séparation des tâches, de double validation, de traçabilité des opérations, de justification documentaire et de contrôle permanent afin de garantir la fiabilité des traitements financiers.

6. Obligation de signalement. Toute anomalie, irrégularité ou opération suspecte identifiée dans l'exercice de leurs fonctions doit être signalée sans délai conformément aux procédures internes de signalement et aux obligations réglementaires applicables. Les responsables financiers sont formés à distinguer les situations nécessitant une simple vérification interne de celles devant faire l'objet d'une déclaration auprès des autorités compétentes.

7. Actualisation des compétences. Les responsables financiers participent régulièrement à des sessions de perfectionnement afin d'intégrer les évolutions des normes comptables, des réglementations financières, des technologies de paiement, des recommandations internationales et des nouvelles méthodes utilisées par les organisations criminelles.

8. Évaluation et certification. Les connaissances acquises peuvent faire l'objet d'évaluations périodiques, d'exercices pratiques ou de mises en situation permettant de mesurer la maîtrise des procédures financières et d'identifier les besoins complémentaires en renforcement des capacités.

9. Contribution à l'amélioration continue. Les responsables financiers participent activement au retour d'expérience, à l'identification des vulnérabilités du dispositif financier, à la formulation de recommandations et à l'amélioration permanente des procédures de contrôle, de conformité et de gestion des risques.

Par cette politique de formation, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** veille à ce que ses responsables financiers disposent des compétences nécessaires pour assurer une gestion rigoureuse, transparente et conforme des ressources de l'Organisation, tout en renforçant

durablement la confiance des membres, des partenaires, des donateurs et des autorités de contrôle.

8.61 Bénévoles

Les **bénévoles** constituent une composante essentielle des activités humanitaires, sociales, éducatives, environnementales et de développement conduites par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Bien qu'ils exercent leurs missions sans contrepartie financière, ils représentent l'Organisation auprès des bénéficiaires, des partenaires, des institutions publiques et des communautés locales. À ce titre, ils doivent bénéficier d'une formation adaptée leur permettant de comprendre les principes fondamentaux de gouvernance, de conformité, d'éthique, de protection des données et de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), en tenant compte de la nature des responsabilités qui leur sont confiées.

1. Formation d'accueil. Avant le début de leurs activités, les bénévoles participent à une session d'intégration leur présentant les valeurs de l'Organisation, son règlement intérieur, son Code d'éthique, ses politiques institutionnelles, les règles de confidentialité, les obligations de conformité ainsi que les comportements attendus dans le cadre de leurs missions.

2. Sensibilisation aux risques. Les bénévoles sont sensibilisés aux principaux risques susceptibles d'être rencontrés dans leurs activités, notamment les tentatives de fraude, les conflits d'intérêts, les sollicitations abusives, les manipulations financières, les comportements contraires à l'éthique, les atteintes à la réputation de l'Organisation et les situations pouvant présenter un risque de blanchiment de capitaux ou de financement du terrorisme.

3. Respect des procédures internes. Les bénévoles sont informés des procédures applicables à leurs missions, notamment celles relatives à la gestion des informations, à la protection des données personnelles, à l'utilisation des ressources de l'Organisation, à la sécurité des activités, à la conservation des documents et aux mécanismes de signalement des incidents.

4. Confidentialité et devoir de réserve. Dans l'exercice de leurs fonctions, les bénévoles sont tenus de respecter une stricte confidentialité concernant les informations auxquelles ils ont accès. Ils s'engagent à protéger les données des bénéficiaires, des membres, des partenaires et de l'Organisation contre toute divulgation non autorisée.

5. Obligation de vigilance. Les bénévoles contribuent activement à la prévention des risques en signalant toute situation inhabituelle, tout comportement suspect, toute tentative de fraude ou toute violation des politiques internes dont ils pourraient avoir connaissance dans le cadre de leurs missions.

6. Formation adaptée aux missions. Lorsque les bénévoles interviennent dans des domaines spécifiques tels que la gestion des dons, les programmes humanitaires, les campagnes de

collecte, les activités numériques, les événements publics ou les projets internationaux, des formations complémentaires adaptées aux risques particuliers de ces missions leur sont dispensées.

7. Actualisation des connaissances. Les bénévoles participent, selon la durée et la nature de leur engagement, à des séances de sensibilisation périodiques destinées à maintenir leurs connaissances à jour et à les informer des évolutions des politiques institutionnelles et des exigences réglementaires.

8. Évaluation et accompagnement. Les responsables des programmes assurent un suivi régulier des bénévoles afin d'évaluer leur compréhension des règles applicables, de répondre à leurs besoins d'accompagnement et de renforcer leurs compétences par des conseils, des retours d'expérience et des actions de formation continue.

9. Promotion des valeurs institutionnelles. Les bénévoles sont encouragés à adopter en permanence un comportement exemplaire fondé sur l'intégrité, la neutralité, le respect des personnes, la transparence, la responsabilité et l'engagement humanitaire. Ils contribuent ainsi à diffuser les valeurs d'AGCE International auprès des communautés et des partenaires, tout en renforçant la crédibilité et la réputation de l'Organisation.

Par cette politique de formation et de sensibilisation, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** reconnaît le rôle déterminant des bénévoles dans la réalisation de ses missions et veille à leur fournir les connaissances, les compétences et les outils nécessaires pour exercer leurs activités dans le respect des plus hauts standards d'éthique, de conformité, de sécurité et de gouvernance institutionnelle.

8.62 Partenaires

Les **partenaires** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** jouent un rôle déterminant dans la réalisation de ses missions humanitaires, sociales, éducatives, sanitaires, environnementales et de développement économique et numérique. Qu'il s'agisse d'institutions publiques, d'organisations internationales, d'associations, de fondations, d'entreprises, d'établissements d'enseignement, de bailleurs de fonds ou d'autres organisations de la société civile, leur collaboration implique le respect des mêmes exigences d'intégrité, de transparence et de conformité que celles applicables à l'Organisation. Dans cette perspective, AGCE International met en œuvre une politique de formation et de sensibilisation destinée à renforcer les capacités de ses partenaires et à promouvoir une compréhension commune des obligations relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), à la prévention de la fraude et à la bonne gouvernance.

1. Sensibilisation dès l'entrée en partenariat. Avant le démarrage des activités communes, les partenaires reçoivent une présentation des politiques institutionnelles d'AGCE International,

notamment en matière d'éthique, de conformité, de gouvernance financière, de contrôle interne, de protection des données et de prévention des risques.

2. Communication des obligations contractuelles. Les partenaires sont informés des engagements de conformité figurant dans les conventions, protocoles d'accord, contrats de partenariat et autres instruments juridiques conclus avec l'Organisation. Ils reconnaissent leur obligation de respecter ces dispositions pendant toute la durée de leur collaboration.

3. Formation adaptée aux risques. Lorsque la nature du partenariat le justifie, AGCE International organise des sessions de formation spécifiques portant sur les risques liés aux financements internationaux, à la gestion des dons, aux opérations transfrontalières, aux projets humanitaires, aux paiements électroniques, à la cybersécurité et à la prévention des conflits d'intérêts.

4. Promotion des bonnes pratiques. Les partenaires sont encouragés à adopter les meilleures pratiques internationales en matière de gouvernance, de transparence financière, de redevabilité, de gestion documentaire, de contrôle interne et de conformité réglementaire afin de garantir la sécurité et la crédibilité des projets réalisés conjointement.

5. Vigilance partagée. Les formations rappellent que la prévention des risques constitue une responsabilité commune. Les partenaires sont invités à identifier les situations inhabituelles, à appliquer les mesures de vigilance appropriées et à informer rapidement l'Organisation de toute anomalie susceptible d'affecter les activités ou les ressources mises en commun.

6. Respect des exigences de confidentialité. Les partenaires sont sensibilisés aux obligations de confidentialité applicables aux informations stratégiques, financières, techniques, administratives et personnelles auxquelles ils peuvent avoir accès dans le cadre de leurs missions.

7. Actualisation régulière. AGCE International diffuse régulièrement des notes d'information, des guides de conformité, des recommandations et des mises à jour réglementaires afin de permettre à ses partenaires d'adapter leurs pratiques aux évolutions législatives, technologiques et opérationnelles.

8. Évaluation de l'efficacité. Les actions de sensibilisation peuvent être complétées par des réunions techniques, des questionnaires, des ateliers ou des audits collaboratifs permettant d'évaluer la compréhension des exigences de conformité et d'identifier les besoins d'amélioration.

9. Renforcement de la coopération. La formation constitue un outil de consolidation des relations de partenariat en favorisant un langage commun, une meilleure coordination des actions et une gestion harmonisée des risques institutionnels.

Par cette politique de formation des partenaires, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce la qualité de

ses collaborations nationales et internationales, sécurise la mise en œuvre de ses programmes et favorise le développement d'un réseau de partenaires partageant les mêmes exigences d'intégrité, de transparence, de responsabilité et de conformité.

8.63 Prestataires

Les **prestataires** intervenant pour le compte de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** participent directement ou indirectement à la réalisation de nombreuses activités institutionnelles, notamment dans les domaines des technologies numériques, des services financiers, des infrastructures, des formations, des prestations intellectuelles, de la logistique, des communications, des services professionnels et des projets humanitaires. En raison de leur contribution aux opérations de l'Organisation, ils doivent être sensibilisés aux exigences de conformité applicables afin de prévenir tout risque juridique, financier, opérationnel ou réputationnel.

1. Information préalable. Dès la conclusion de la relation contractuelle, les prestataires reçoivent les principales informations relatives aux politiques institutionnelles d'AGCE International, notamment celles concernant la lutte contre le blanchiment de capitaux et le financement du terrorisme, l'éthique, la prévention de la corruption, la protection des données personnelles et les règles de confidentialité.

2. Formation adaptée aux prestations. Les actions de sensibilisation sont adaptées à la nature des prestations réalisées et au niveau de risque associé. Les prestataires intervenant sur des opérations financières, informatiques, numériques ou comportant un accès à des informations sensibles bénéficient d'un accompagnement renforcé.

3. Respect des obligations contractuelles. Les prestataires sont informés des clauses contractuelles relatives à la conformité, à la sécurité des informations, au contrôle interne, à la confidentialité, aux audits et au respect des lois applicables. Ils s'engagent à respecter ces obligations pendant toute la durée de leurs interventions.

4. Prévention des risques. Les formations permettent aux prestataires d'identifier les situations susceptibles de constituer une fraude, un conflit d'intérêts, une tentative de corruption, une cyberattaque, une manipulation documentaire ou une opération financière inhabituelle pouvant affecter l'Organisation.

5. Utilisation sécurisée des systèmes. Les prestataires ayant accès aux systèmes d'information d'AGCE International sont sensibilisés aux règles de cybersécurité, de gestion des identifiants, d'authentification, de protection des données, de sauvegarde et de signalement des incidents de sécurité.

6. Obligation de signalement. Les prestataires sont encouragés à signaler sans délai toute irrégularité, toute tentative de fraude ou tout événement susceptible de compromettre la

sécurité, la conformité ou la réputation de l'Organisation, conformément aux procédures internes de signalement.

7. Actualisation des connaissances. Lorsque les prestations s'inscrivent dans la durée, AGCE International met à disposition des prestataires des informations actualisées sur les évolutions réglementaires, les nouvelles procédures internes et les bonnes pratiques applicables à leurs activités.

8. Contrôle de la conformité. L'Organisation peut vérifier le respect des exigences de conformité au moyen de revues documentaires, de contrôles contractuels, d'évaluations périodiques ou d'audits réalisés conformément aux dispositions prévues dans les contrats de prestation.

9. Amélioration continue. Les retours d'expérience issus des missions réalisées par les prestataires sont intégrés dans le processus d'amélioration continue des politiques de conformité, de gestion des risques et de gouvernance. Cette démarche favorise le renforcement des relations contractuelles, l'amélioration des performances et la maîtrise durable des risques.

Par cette politique de formation et de sensibilisation, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** veille à ce que l'ensemble de ses prestataires intervienne dans un cadre sécurisé, conforme et transparent, contribuant ainsi à la protection de ses ressources, au succès de ses programmes et au respect des meilleures pratiques nationales et internationales en matière de gouvernance et de conformité.

8.64 Fréquence des formations

La **fréquence des formations** constitue un élément essentiel de l'efficacité du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. L'Organisation reconnaît que les risques financiers, juridiques, technologiques et opérationnels évoluent continuellement et qu'une formation ponctuelle ne saurait garantir durablement un niveau satisfaisant de conformité. En conséquence, elle met en œuvre un programme structuré de formation initiale, continue et exceptionnelle, permettant à l'ensemble de ses administrateurs, dirigeants, responsables financiers, employés, bénévoles, partenaires et prestataires de maintenir leurs connaissances à jour et d'adapter leurs pratiques aux évolutions des normes nationales et internationales.

1. Formation à l'intégration. Toute personne intégrant l'Organisation ou débutant une collaboration avec celle-ci reçoit une formation d'accueil avant ou dès sa prise de fonction. Cette formation présente les politiques institutionnelles, les règles de conformité, les procédures internes, les mécanismes de contrôle, les obligations de vigilance ainsi que les responsabilités attachées aux fonctions exercées.

2. Formation périodique obligatoire. L'ensemble des personnes concernées participe à des formations de recyclage organisées à intervalles réguliers afin de consolider les acquis, de rappeler les bonnes pratiques et de maintenir un niveau élevé de vigilance face aux risques de fraude, de corruption, de blanchiment de capitaux, de financement du terrorisme et de cybercriminalité.

3. Formation fondée sur les risques. La fréquence des formations peut être renforcée pour les personnes occupant des fonctions exposées à des risques élevés, notamment les responsables financiers, les gestionnaires de projets, les responsables des paiements, les administrateurs des systèmes d'information, les responsables des partenariats et toute autre fonction identifiée comme sensible par l'analyse des risques de l'Organisation.

4. Formation lors des évolutions réglementaires. Chaque modification importante de la législation, de la réglementation, des recommandations des autorités compétentes ou des politiques internes donne lieu, lorsque cela est nécessaire, à une formation spécifique permettant aux personnes concernées de maîtriser rapidement les nouvelles exigences applicables.

5. Formation après un incident. Lorsqu'un incident de conformité, une fraude, une cyberattaque, une anomalie financière ou toute autre situation présentant un risque significatif est constaté, des actions de sensibilisation complémentaires peuvent être organisées afin d'en analyser les causes, d'en tirer les enseignements et de prévenir leur réapparition.

6. Exercices pratiques réguliers. En complément des formations théoriques, l'Organisation organise des études de cas, des simulations, des ateliers collaboratifs et des exercices pratiques permettant aux participants de mettre en application les procédures institutionnelles dans des situations proches de la réalité opérationnelle.

7. Planification annuelle. Les actions de formation sont intégrées dans un plan annuel élaboré par les responsables compétents. Ce plan précise les publics concernés, les objectifs pédagogiques, les thèmes abordés, les modalités de formation, les ressources mobilisées ainsi que les indicateurs de suivi.

8. Suivi de la participation. La présence aux formations obligatoires fait l'objet d'un enregistrement systématique. Les absences sont justifiées, suivies et, lorsque cela est nécessaire, donnent lieu à des sessions de rattrapage afin de garantir que chaque personne dispose du niveau de compétence attendu.

9. Révision du programme. La fréquence des formations est réévaluée périodiquement au regard des résultats des audits, des contrôles internes, des évaluations des risques, des retours d'expérience et des évolutions des activités de l'Organisation.

Par cette politique de formation continue, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit le maintien durable des compétences de ses parties prenantes et renforce sa capacité à prévenir les

risques, à assurer sa conformité réglementaire et à promouvoir une culture institutionnelle fondée sur l'intégrité, la vigilance et la responsabilité.

8.65 Évaluation des compétences

L'évaluation des compétences constitue un mécanisme essentiel permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de mesurer l'efficacité de son dispositif de formation et de s'assurer que les connaissances acquises sont effectivement maîtrisées et appliquées dans les activités quotidiennes. Cette démarche s'inscrit dans une logique d'amélioration continue, de gestion des risques et de renforcement permanent de la conformité aux exigences de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT).

1. Objectif de l'évaluation. Les évaluations ont pour finalité de vérifier le niveau de compréhension des politiques institutionnelles, des procédures internes, des obligations réglementaires et des bonnes pratiques applicables aux fonctions exercées par chaque participant.

2. Évaluation initiale. À l'issue des formations d'intégration, les participants peuvent être soumis à une évaluation permettant de confirmer leur aptitude à exercer leurs missions conformément aux exigences de conformité de l'Organisation.

3. Évaluations périodiques. Des évaluations régulières sont organisées afin de mesurer le maintien des connaissances, d'identifier les besoins de mise à niveau et d'adapter les programmes de formation aux évolutions des risques et des responsabilités.

4. Diversité des méthodes d'évaluation. Les compétences peuvent être appréciées au moyen de questionnaires, d'études de cas, de mises en situation, de simulations, d'entretiens, d'exercices pratiques, d'observations en situation de travail ou de tout autre outil pédagogique adapté aux fonctions concernées.

5. Évaluation des compétences opérationnelles. L'Organisation veille à mesurer non seulement les connaissances théoriques, mais également la capacité des participants à appliquer correctement les procédures de vigilance, de contrôle interne, de signalement, de gestion documentaire, de protection des données et de sécurité financière.

6. Analyse des résultats. Les résultats des évaluations sont analysés afin d'identifier les points forts, les insuffisances éventuelles et les domaines nécessitant un renforcement des compétences. Cette analyse contribue à l'amélioration des contenus pédagogiques et des méthodes de formation.

7. Mesures d'accompagnement. Lorsque des lacunes sont identifiées, des actions correctives sont mises en œuvre, notamment des formations complémentaires, des séances

de tutorat, des ateliers pratiques, des accompagnements individualisés ou des programmes de perfectionnement adaptés aux besoins des personnes concernées.

8. Traçabilité des évaluations. Les résultats des évaluations, les attestations de participation, les certificats de réussite et les actions de formation réalisées sont enregistrés dans les dossiers administratifs de formation afin d'assurer leur suivi, leur traçabilité et leur disponibilité lors des audits internes ou externes.

9. Amélioration continue. Les conclusions issues des évaluations alimentent le processus global d'amélioration continue de la gouvernance, de la conformité et de la gestion des risques. Elles permettent d'adapter les plans de formation, de renforcer les dispositifs de contrôle interne et de maintenir un niveau élevé de compétence au sein de l'Organisation.

Par cette politique d'évaluation des compétences, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** confirme sa volonté de développer un personnel, des administrateurs, des partenaires, des prestataires et des bénévoles hautement qualifiés, capables d'appliquer avec rigueur les principes de conformité, de gouvernance, de transparence et de prévention des risques. Cette démarche contribue directement à la crédibilité institutionnelle de l'Organisation et au renforcement de la confiance accordée par ses membres, ses partenaires, ses bailleurs de fonds et les autorités compétentes.

8.66 Mise à jour continue

La **mise à jour continue** constitue un principe fondamental de la politique de formation et de sensibilisation de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Dans un environnement marqué par l'évolution permanente des réglementations, des technologies numériques, des méthodes de fraude, des risques de blanchiment de capitaux et de financement du terrorisme (LBC/FT), l'Organisation considère que le maintien des compétences ne peut être assuré que par un processus permanent d'actualisation des connaissances, des procédures et des pratiques professionnelles. Cette démarche permet de garantir que l'ensemble des administrateurs, dirigeants, responsables financiers, collaborateurs, bénévoles, partenaires et prestataires demeure en mesure d'exercer ses responsabilités conformément aux meilleures pratiques nationales et internationales de gouvernance, de conformité et de gestion des risques.

1. Principe d'amélioration permanente. AGCE International adopte une approche dynamique de la formation reposant sur l'amélioration continue des connaissances et des compétences. Les programmes pédagogiques ne sont jamais considérés comme définitifs et font l'objet d'une révision régulière afin de demeurer adaptés aux réalités opérationnelles de l'Organisation.

2. Veille réglementaire permanente. Les responsables de la conformité assurent une veille continue des évolutions législatives, réglementaires et normatives applicables au Cameroun, au Canada ainsi que dans les autres juridictions où intervient l'Organisation. Les nouvelles

exigences sont intégrées dans les programmes de formation dès leur entrée en vigueur ou lorsque leur application devient pertinente.

3. Intégration des recommandations internationales. Les contenus pédagogiques sont actualisés afin de prendre en considération les recommandations des organismes internationaux compétents en matière de lutte contre le blanchiment de capitaux, de financement du terrorisme, de gouvernance, de protection des données, de cybersécurité, de gestion des risques et de conformité institutionnelle.

4. Prise en compte des évolutions technologiques. L'Organisation adapte régulièrement ses formations afin d'intégrer les innovations relatives aux systèmes d'information, aux plateformes numériques, aux paiements électroniques, à l'intelligence artificielle, aux services infonuagiques, aux outils collaboratifs, à la cybersécurité ainsi qu'aux nouvelles techniques de fraude susceptibles d'affecter les activités institutionnelles.

5. Exploitation des retours d'expérience. Les enseignements tirés des audits internes et externes, des contrôles de conformité, des inspections réglementaires, des incidents opérationnels, des signalements, des exercices pratiques et des évaluations des risques sont systématiquement analysés afin d'améliorer les contenus de formation et de renforcer les dispositifs de prévention.

6. Révision des procédures internes. Toute modification des politiques institutionnelles, des procédures opérationnelles, des mécanismes de contrôle interne, des règles de gouvernance ou des dispositifs de sécurité donne lieu à une mise à jour des supports pédagogiques et à une information rapide des personnes concernées afin d'assurer une application homogène des nouvelles dispositions.

7. Adaptation aux profils des participants. Les programmes de mise à jour tiennent compte des responsabilités exercées, des fonctions occupées et du niveau d'exposition aux risques. Les contenus sont adaptés aux besoins spécifiques des administrateurs, responsables financiers, collaborateurs, bénévoles, partenaires et prestataires afin d'assurer une formation pertinente et efficace.

8. Utilisation de méthodes pédagogiques diversifiées. La mise à jour des compétences peut être assurée au moyen de formations en présentiel, de classes virtuelles, de modules d'apprentissage en ligne, de webinaires, d'ateliers pratiques, de simulations, de bulletins d'information, de guides techniques, de notes de service, de fiches réflexes et de séances de partage d'expérience, permettant ainsi une diffusion rapide et homogène des nouvelles connaissances.

9. Suivi et traçabilité des mises à jour. Chaque action de mise à jour fait l'objet d'une planification, d'un enregistrement et d'un suivi documenté. Les dates de diffusion, les thèmes abordés, les participants concernés, les supports utilisés ainsi que les résultats des évaluations sont conservés dans le système de gestion documentaire de l'Organisation afin de démontrer

le respect des obligations de formation lors des audits internes, des contrôles réglementaires ou des évaluations institutionnelles.

10. Évaluation de l'efficacité des mises à jour. L'Organisation procède régulièrement à l'évaluation de l'impact des actions de mise à jour sur les connaissances, les comportements professionnels et l'application effective des procédures. Les résultats obtenus permettent d'ajuster les méthodes pédagogiques, de renforcer les actions de sensibilisation et d'améliorer continuellement le dispositif global de formation.

11. Responsabilité partagée. La réussite de la mise à jour continue repose sur l'engagement conjoint de l'Organisation et de l'ensemble de ses parties prenantes. Chaque administrateur, dirigeant, collaborateur, bénévole, partenaire ou prestataire est invité à participer activement aux actions de formation organisées, à maintenir ses connaissances à jour et à contribuer, par ses retours d'expérience, à l'amélioration des pratiques institutionnelles.

Par cette politique de **mise à jour continue**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme que le développement permanent des compétences constitue un facteur stratégique de performance, de résilience et de conformité. En maintenant un haut niveau d'expertise face aux évolutions réglementaires, technologiques et opérationnelles, l'Organisation renforce durablement sa gouvernance, sécurise ses activités, protège ses ressources et consolide la confiance de ses membres, partenaires, donateurs, bailleurs de fonds et autorités de contrôle, conformément aux plus hauts standards internationaux de transparence, d'intégrité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

SECTION VIII

GESTION DES INCIDENTS

8.67 Typologie des incidents

La **gestion des incidents** constitue une composante essentielle du dispositif de maîtrise des risques de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle permet d'identifier, de classer, de traiter et de prévenir tout événement susceptible de compromettre la conformité, la sécurité, l'intégrité, la disponibilité ou la réputation de l'Organisation. Dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), une connaissance précise de la typologie des incidents permet de mettre en œuvre des mesures de réponse adaptées, proportionnées et coordonnées, tout en renforçant le système de contrôle interne et la résilience institutionnelle.

La présente classification constitue un référentiel destiné à faciliter la détection précoce des incidents, leur évaluation, leur enregistrement, leur traitement et leur suivi,

conformément aux politiques de gouvernance, de gestion des risques, de cybersécurité, de protection des données et de conformité applicables à l'Organisation.

1. Incidents financiers. Sont considérés comme incidents financiers toutes les anomalies affectant la gestion des ressources financières de l'Organisation, notamment les erreurs comptables significatives, les paiements non autorisés, les doubles paiements, les détournements de fonds, les fraudes, les irrégularités budgétaires, les opérations inhabituelles, les manipulations comptables, les tentatives de blanchiment de capitaux, le financement du terrorisme ainsi que toute opération contraire aux procédures financières internes.

2. Incidents de conformité. Cette catégorie regroupe les violations des lois, des règlements, des politiques institutionnelles, des procédures internes, des obligations contractuelles ou des exigences imposées par les autorités compétentes. Elle comprend notamment les manquements aux obligations de vigilance, aux procédures KYC, aux contrôles internes, aux obligations déclaratives et aux dispositifs de conformité LBC/FT.

3. Incidents de cybersécurité. Il s'agit de tout événement compromettant la sécurité des systèmes d'information, des plateformes numériques, des infrastructures technologiques ou des données de l'Organisation. Sont notamment concernés les accès non autorisés, les tentatives d'intrusion, les logiciels malveillants, les rançongiciels, les attaques par hameçonnage, les compromissions de comptes, les fuites de données, les interruptions de services numériques et les attaques contre les moyens de paiement électroniques.

4. Incidents liés à la protection des données. Cette catégorie couvre toute perte, divulgation, modification, destruction ou utilisation non autorisée de données personnelles, financières, médicales, administratives ou institutionnelles détenues par AGCE International, qu'elles concernent les membres, bénéficiaires, partenaires, donateurs, employés ou toute autre partie prenante.

5. Incidents opérationnels. Les incidents opérationnels concernent les dysfonctionnements susceptibles d'affecter la continuité des activités de l'Organisation, tels que les erreurs de procédure, les défaillances organisationnelles, les interruptions de services, les pertes documentaires, les indisponibilités techniques, les erreurs humaines, les défauts de coordination ou les insuffisances de contrôle.

6. Incidents éthiques et disciplinaires. Cette catégorie comprend les comportements contraires au Code d'éthique, aux valeurs institutionnelles ou aux règles de gouvernance, notamment les conflits d'intérêts non déclarés, les actes de corruption, les abus d'autorité, les discriminations, le harcèlement, les violences, les atteintes à la dignité des personnes, les violations des règles de confidentialité ou toute autre faute disciplinaire.

7. Incidents contractuels et partenariaux. Relèvent de cette catégorie les situations résultant du non-respect des engagements contractuels par un partenaire, un prestataire, un fournisseur ou tout autre cocontractant, notamment les manquements aux clauses de conformité, les

retards importants, les inexécutions contractuelles, les fraudes documentaires ou les violations des obligations de confidentialité.

8. Incidents matériels et environnementaux. Cette catégorie regroupe les événements affectant les biens, les infrastructures ou l'environnement de travail de l'Organisation, notamment les incendies, inondations, catastrophes naturelles, actes de vandalisme, vols, dégradations, accidents techniques, pannes majeures ou tout événement susceptible d'interrompre les activités institutionnelles.

9. Incidents liés aux ressources humaines. Sont visés les événements ayant un impact sur la gestion du personnel, tels que les violations des règles internes, les absences injustifiées, les manquements aux obligations professionnelles, les usurpations d'identité, les falsifications de documents administratifs, les comportements incompatibles avec les missions de l'Organisation ou toute autre situation présentant un risque humain ou organisationnel.

10. Classification selon le niveau de gravité. Chaque incident est évalué selon sa nature, son impact, son niveau de criticité, sa probabilité de récurrence et les conséquences potentielles sur les activités, les ressources, la réputation et la conformité de l'Organisation. Cette classification permet de définir les priorités de traitement, les mesures d'urgence à mettre en œuvre, le niveau de décision requis ainsi que les modalités de suivi et d'escalade.

11. Révision permanente de la typologie. La présente typologie fait l'objet d'une révision régulière afin d'intégrer les nouveaux risques émergents, les évolutions technologiques, les modifications réglementaires, les enseignements tirés des audits, des incidents constatés et des recommandations formulées par les autorités compétentes ou les partenaires institutionnels.

Par cette classification des incidents, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** établit un cadre méthodologique cohérent permettant une identification rapide des événements à risque, une réponse adaptée à leur gravité et une amélioration continue de son dispositif de gouvernance, de contrôle interne, de sécurité et de conformité. Cette approche contribue à renforcer durablement la résilience institutionnelle, la protection des ressources et la confiance des membres, des partenaires, des donateurs, des bénéficiaires, des bailleurs de fonds et des autorités de contrôle nationales et internationales.

8.68 Fraude

La **fraude** constitue l'un des risques majeurs susceptibles de compromettre l'intégrité, la stabilité financière, la conformité réglementaire et la réputation de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Dans le cadre de sa politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), l'Organisation adopte une approche de tolérance zéro à l'égard de tout acte frauduleux, qu'il soit commis par un membre, un administrateur, un employé, un bénévole,

un partenaire, un prestataire, un donateur ou toute autre personne en relation avec ses activités. La présente politique définit les principales catégories de fraude, les mécanismes de prévention, les modalités de détection ainsi que les mesures de traitement destinées à protéger durablement les ressources, les bénéficiaires et la crédibilité institutionnelle de l'Organisation.

1. Définition de la fraude. Est considérée comme fraude toute action ou omission volontaire destinée à obtenir un avantage indu, à causer un préjudice financier, matériel, administratif ou réputationnel à l'Organisation, ou à contourner les règles légales, contractuelles ou institutionnelles par la tromperie, la falsification, la dissimulation ou l'abus de confiance.

2. Typologie des fraudes. Les actes de fraude peuvent notamment concerner les détournements de fonds, les fausses factures, les doubles paiements, les falsifications comptables, les usurpations d'identité, les manipulations documentaires, les déclarations mensongères, les fraudes aux dons, les abus de cartes de paiement, les paiements fictifs, les conflits d'intérêts dissimulés, les marchés irréguliers, les escroqueries numériques ainsi que toute tentative de blanchiment de capitaux ou de financement du terrorisme.

3. Identification des facteurs de risque. L'Organisation procède régulièrement à une analyse des vulnérabilités susceptibles de favoriser les comportements frauduleux, notamment les insuffisances de contrôle interne, les défauts de séparation des fonctions, les accès informatiques excessifs, les procédures incomplètes ou les faiblesses documentaires.

4. Mesures de prévention. AGCE International met en œuvre des mécanismes de prévention comprenant la séparation des responsabilités, la double validation des opérations sensibles, les contrôles hiérarchiques, les rapprochements comptables, la vérification des pièces justificatives, les audits réguliers, les contrôles informatiques, les formations de sensibilisation ainsi que les procédures de vigilance renforcée.

5. Détection des fraudes. Les anomalies financières, les opérations inhabituelles, les incohérences documentaires, les alertes des systèmes d'information, les signalements des lanceurs d'alerte et les résultats des audits constituent les principaux mécanismes de détection des comportements frauduleux.

6. Signalement obligatoire. Toute personne ayant connaissance ou soupçonnant raisonnablement un acte de fraude est tenue de le signaler immédiatement par les canaux sécurisés mis en place par l'Organisation. Les lanceurs d'alerte bénéficient des protections prévues par la politique institutionnelle.

7. Investigation. Chaque suspicion de fraude fait l'objet d'une enquête impartiale, confidentielle et documentée permettant d'établir les faits, de préserver les preuves, d'évaluer les conséquences financières et de déterminer les responsabilités.

8. Mesures correctives et disciplinaires. En fonction des résultats de l'enquête, l'Organisation peut mettre en œuvre des mesures conservatoires, disciplinaires, contractuelles,

financières ou judiciaires, ainsi que des actions destinées à renforcer les procédures internes afin d'éviter la réapparition de situations similaires.

9. Retour d'expérience. Les enseignements issus des incidents de fraude sont intégrés dans les dispositifs de gestion des risques, de contrôle interne et de formation afin d'améliorer continuellement la capacité de prévention et de détection de l'Organisation.

Par cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme son engagement à prévenir toute forme de fraude, à protéger ses ressources, à préserver la confiance de ses partenaires et à maintenir les plus hauts standards de gouvernance, de transparence et de conformité.

8.69 Cyberattaque

La **cyberattaque** représente un risque majeur pour les activités numériques de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En raison de l'utilisation de plateformes numériques, de services bancaires en ligne, de solutions de paiement électronique, de systèmes d'information, d'applications web et de bases de données contenant des informations sensibles, l'Organisation met en œuvre une politique globale de prévention, de détection, de gestion et de réponse aux incidents de cybersécurité. Cette politique vise à protéger la confidentialité, l'intégrité, la disponibilité et la traçabilité des informations institutionnelles, tout en assurant la continuité des activités et la conformité aux exigences réglementaires relatives à la LBC/FT.

1. Définition de la cyberattaque. Une cyberattaque désigne toute tentative intentionnelle visant à compromettre les systèmes d'information, les réseaux, les applications, les équipements numériques ou les données de l'Organisation, par des moyens techniques ou humains, dans le but d'obtenir un accès non autorisé, de voler des informations, de perturber les services ou de provoquer un dommage.

2. Typologie des cyberattaques. Les incidents concernés comprennent notamment les logiciels malveillants, les rançongiciels (ransomwares), les attaques par hameçonnage (phishing), les compromissions de comptes, les attaques par déni de service (DDoS), les intrusions dans les systèmes d'information, les fuites de données, les vols d'identifiants, les attaques contre les infrastructures infonuagiques, les manipulations des paiements électroniques et toute autre menace numérique.

3. Prévention des risques. L'Organisation déploie des mesures de cybersécurité comprenant l'authentification multifactorielle, le chiffrement des données, les pare-feu, les systèmes de détection d'intrusion, les antivirus, les sauvegardes sécurisées, la gestion des correctifs de sécurité, la segmentation des accès ainsi que la surveillance permanente des infrastructures numériques.

4. Détection des incidents. Les événements de sécurité sont surveillés au moyen d'outils de journalisation, d'alertes automatiques, d'analyses comportementales, de contrôles d'accès, d'audits techniques et de dispositifs de supervision permettant d'identifier rapidement toute activité anormale.

5. Réponse immédiate. En cas de cyberattaque, des mesures d'urgence sont immédiatement mises en œuvre afin de contenir l'incident, d'isoler les systèmes concernés, de préserver les preuves numériques, de limiter les impacts opérationnels et de maintenir la continuité des services essentiels.

6. Notification et escalade. Les incidents de cybersécurité sont signalés sans délai aux responsables compétents. Lorsque la réglementation l'impose, les autorités compétentes, les partenaires concernés ou les personnes affectées sont informés conformément aux obligations légales et contractuelles applicables.

7. Investigation numérique. Chaque cyberattaque fait l'objet d'une analyse technique approfondie destinée à identifier les causes, les vulnérabilités exploitées, les conséquences de l'incident et les mesures correctives à mettre en œuvre.

8. Rétablissement des activités. Les systèmes affectés sont restaurés selon les procédures de continuité et de reprise d'activité de l'Organisation. Les restaurations sont réalisées à partir de sauvegardes sécurisées et font l'objet de contrôles destinés à garantir l'intégrité des données et la sécurité des infrastructures avant leur remise en production.

9. Renforcement du dispositif. Les enseignements tirés de chaque cyberattaque alimentent le processus d'amélioration continue des politiques de cybersécurité, des formations, des contrôles techniques et des procédures de gestion des incidents afin de réduire durablement les risques futurs.

Par cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** réaffirme son engagement à protéger son patrimoine numérique, les données de ses membres, partenaires, donateurs et bénéficiaires, ainsi que l'ensemble de ses systèmes d'information contre les menaces cybernétiques. Cette démarche contribue à renforcer la résilience numérique de l'Organisation, la continuité de ses missions humanitaires et le respect des meilleures pratiques internationales en matière de cybersécurité, de gouvernance et de conformité.

8.70 Usurpation d'identité

L'**usurpation d'identité** constitue un risque majeur susceptible d'affecter la sécurité, la réputation, la conformité et les ressources de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Dans un environnement caractérisé par la numérisation des services, les échanges électroniques, les plateformes de paiement, les espaces membres et les partenariats internationaux, ce type

d'incident peut entraîner des pertes financières, des violations de données, des opérations frauduleuses et des atteintes graves à la confiance des membres, donateurs, bénéficiaires, partenaires et autorités compétentes. L'Organisation adopte ainsi une politique de prévention, de détection et de gestion des cas d'usurpation d'identité conforme aux principes de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), de cybersécurité et de protection des données.

1. Définition. L'usurpation d'identité désigne toute utilisation frauduleuse, totale ou partielle, de l'identité d'une personne physique ou morale, ou de ses éléments d'identification, dans le but d'obtenir un avantage indu, de tromper un tiers, de réaliser une opération non autorisée ou de porter atteinte aux intérêts de l'Organisation.

2. Formes d'usurpation. L'incident peut concerner l'utilisation illicite du nom, de la qualité, des documents officiels, de la signature, de l'adresse électronique, des identifiants numériques, des comptes utilisateurs, des moyens de paiement, des documents administratifs ou de toute information permettant de se faire passer pour une autre personne ou une autre organisation.

3. Facteurs de risque. Les risques sont accrus en présence de documents falsifiés, de procédures d'identification insuffisantes, de mots de passe faibles, de divulgation d'informations sensibles, d'attaques par hameçonnage, d'ingénierie sociale ou de compromission des systèmes d'information.

4. Mesures de prévention. AGCE International met en œuvre des procédures d'identification et de vérification renforcées, comprenant notamment les contrôles KYC, l'authentification multifactorielle, la validation des pièces justificatives, la vérification des coordonnées bancaires, la sécurisation des accès numériques et la sensibilisation régulière des utilisateurs.

5. Détection des incidents. Toute incohérence d'identité, tentative d'accès inhabituelle, modification non autorisée des informations personnelles, demande suspecte ou comportement anormal détecté par les systèmes de surveillance fait l'objet d'une analyse immédiate afin de confirmer ou d'écarter l'existence d'une usurpation.

6. Signalement immédiat. Toute personne suspectant une usurpation d'identité concernant l'Organisation, un membre, un partenaire ou un bénéficiaire est tenue d'en informer sans délai les responsables compétents par les canaux sécurisés prévus par la politique de signalement.

7. Mesures conservatoires. En cas de suspicion fondée, l'Organisation peut suspendre temporairement les accès concernés, bloquer certaines opérations, renforcer les contrôles d'authentification, demander des justificatifs complémentaires ou mettre en œuvre toute autre mesure destinée à limiter les conséquences de l'incident.

8. Investigation et coopération. Les incidents font l'objet d'une enquête documentée permettant d'identifier leur origine, les personnes concernées, les impacts potentiels et les mesures correctives à appliquer. Lorsque les circonstances l'exigent, l'Organisation coopère avec les autorités compétentes et les partenaires concernés.

9. Amélioration continue. Les enseignements tirés des cas d'usurpation d'identité alimentent la révision des procédures de vérification, des mécanismes d'authentification, des programmes de sensibilisation et des dispositifs de contrôle interne afin de réduire durablement les risques de récurrence.

Par cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme sa volonté de protéger l'identité de l'ensemble de ses parties prenantes, de préserver l'intégrité de ses opérations et de maintenir un environnement numérique fiable, sécurisé et conforme aux meilleures pratiques internationales.

8.71 Compte compromis

Un **compte compromis** correspond à toute situation dans laquelle un compte utilisateur, un accès informatique, un profil numérique ou une identité électronique utilisé dans le cadre des activités de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** est utilisé, contrôlé ou manipulé par une personne non autorisée. Ce type d'incident représente un risque élevé pour la confidentialité des informations, la sécurité des systèmes, la protection des données personnelles, la continuité des activités et la conformité aux exigences de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). L'Organisation met en œuvre des procédures spécifiques permettant d'identifier rapidement ces situations, d'en limiter les conséquences et de restaurer la sécurité des accès concernés.

1. Définition. Un compte est considéré comme compromis lorsqu'il existe des indices raisonnables démontrant qu'un tiers non autorisé a obtenu, utilisé ou tenté d'utiliser les identifiants, les moyens d'authentification ou les privilèges d'accès d'un utilisateur légitime.

2. Causes possibles. Les compromissions peuvent résulter d'attaques par hameçonnage, de logiciels malveillants, de vols d'identifiants, de mots de passe insuffisamment sécurisés, de fuites de données, d'ingénierie sociale, de réutilisation de mots de passe ou d'un accès physique non autorisé à un équipement.

3. Signes de compromission. Les principaux indicateurs comprennent des connexions inhabituelles, des modifications non autorisées des paramètres du compte, des opérations inexplicables, des envois de messages non autorisés, des changements d'identifiants, des demandes anormales de validation ou toute activité incompatible avec les habitudes de l'utilisateur.

4. Détection et surveillance. Les systèmes de sécurité de l'Organisation assurent une surveillance continue des connexions, des journaux d'activité, des tentatives d'authentification, des accès privilégiés et des événements de sécurité afin de détecter rapidement toute activité suspecte.

5. Mesures d'urgence. Dès la détection d'une compromission présumée, AGCE International procède sans délai au blocage temporaire du compte concerné, à la réinitialisation des identifiants, à la révocation des sessions actives, à la vérification des opérations réalisées et à la mise en œuvre des mesures nécessaires pour contenir l'incident.

6. Investigation technique. Une analyse approfondie est réalisée afin de déterminer l'origine de la compromission, les vulnérabilités exploitées, les données consultées ou modifiées, les opérations effectuées et les conséquences potentielles pour l'Organisation et ses parties prenantes.

7. Notification des parties concernées. Lorsque cela est requis par la réglementation applicable ou nécessaire à la protection des intérêts des personnes concernées, les utilisateurs affectés, les partenaires, les autorités compétentes ou les fournisseurs de services sont informés dans les meilleurs délais, conformément aux procédures internes et aux obligations légales.

8. Restauration sécurisée. Avant la réactivation d'un compte compromis, l'Organisation vérifie que toutes les vulnérabilités identifiées ont été corrigées, que les mécanismes d'authentification ont été renforcés et que l'utilisateur concerné a reçu les recommandations nécessaires pour prévenir toute nouvelle compromission.

9. Retour d'expérience et prévention. Chaque incident de compromission fait l'objet d'une analyse rétrospective destinée à améliorer les dispositifs de cybersécurité, les procédures d'authentification, les campagnes de sensibilisation, les contrôles d'accès et les mécanismes de surveillance. Les enseignements tirés sont intégrés dans le programme d'amélioration continue de la gouvernance numérique et de la conformité.

Par cette politique de gestion des comptes compromis, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce la protection de son patrimoine informationnel, garantit la sécurité de ses plateformes numériques et confirme son engagement à maintenir un niveau élevé de résilience face aux menaces cybernétiques, tout en assurant la continuité de ses missions humanitaires et institutionnelles dans le respect des meilleures pratiques internationales.

8.72 Paiement frauduleux

Le **paiement frauduleux** constitue un incident critique susceptible d'entraîner des pertes financières, des atteintes à la réputation et des manquements aux obligations réglementaires de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En raison de l'utilisation de multiples moyens de paiement, notamment les virements bancaires, les cartes de paiement, les portefeuilles électroniques, les plateformes numériques et les solutions de paiement internationales, l'Organisation applique une politique stricte de prévention, de détection, de traitement et de récupération des opérations frauduleuses. Cette politique s'inscrit dans le cadre du dispositif de

lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), de la cybersécurité, du contrôle interne et de la gestion des risques financiers.

1. Définition. Est considéré comme paiement frauduleux tout paiement, encaissement, remboursement, transfert ou mouvement financier exécuté de manière irrégulière, trompeuse, falsifiée ou non autorisée, en violation des procédures internes ou des dispositions légales applicables.

2. Typologie des paiements frauduleux. Cette catégorie comprend notamment les paiements effectués à partir de comptes compromis, les usurpations d'identité, les faux ordres de virement, les modifications frauduleuses de coordonnées bancaires, les doubles paiements volontaires, les paiements réalisés au moyen de cartes volées, les remboursements fictifs, les détournements de dons, les manipulations de factures, les faux bénéficiaires et toute transaction destinée à masquer l'origine ou la destination de fonds illicites.

3. Prévention. L'Organisation met en œuvre des mécanismes de prévention reposant sur la séparation des fonctions, la double validation des paiements sensibles, l'authentification multifactorielle, la vérification systématique des bénéficiaires, les contrôles de cohérence, les plafonds d'autorisation, la surveillance automatisée des transactions et la formation régulière des utilisateurs.

4. Détection. Les paiements inhabituels sont détectés grâce aux contrôles comptables, aux alertes des plateformes de paiement, aux rapprochements bancaires, aux outils de surveillance des transactions, aux audits internes et aux signalements effectués par les collaborateurs ou les partenaires.

5. Mesures immédiates. Dès la découverte d'un paiement frauduleux ou suspect, l'Organisation procède au blocage des opérations concernées lorsque cela est encore possible, suspend les accès impliqués, informe les établissements financiers concernés, préserve les éléments de preuve et engage les investigations nécessaires.

6. Investigation. Une analyse complète est menée afin d'identifier les circonstances de l'incident, les personnes concernées, les failles exploitées, les montants en cause et les impacts juridiques, financiers, opérationnels et réputationnels.

7. Notification et coopération. Lorsque les circonstances l'exigent, AGCE International informe les autorités compétentes, les établissements financiers, les partenaires techniques, les prestataires de paiement et les personnes concernées, conformément aux obligations réglementaires et contractuelles.

8. Mesures correctives. À l'issue des investigations, l'Organisation renforce les procédures internes, met à jour les contrôles de sécurité, corrige les vulnérabilités identifiées et engage, le cas échéant, des actions disciplinaires, contractuelles ou judiciaires.

9. Amélioration continue. Les enseignements tirés des incidents de paiement frauduleux sont intégrés dans le dispositif global de gestion des risques afin de renforcer durablement la sécurité des paiements et la conformité institutionnelle.

Par cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** confirme son engagement à protéger l'intégrité de ses flux financiers, à sécuriser les ressources qui lui sont confiées et à maintenir les plus hauts standards de gouvernance financière.

8.73 Réponse aux incidents

La **réponse aux incidents** désigne l'ensemble des mesures organisationnelles, techniques, administratives et opérationnelles mises en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** afin de limiter les conséquences d'un incident, d'en assurer la maîtrise rapide et de restaurer un fonctionnement normal dans les meilleurs délais. Cette réponse est guidée par les principes de réactivité, de coordination, de proportionnalité, de traçabilité et d'amélioration continue.

1. Détection et qualification. Tout incident signalé est immédiatement analysé afin d'en déterminer la nature, le niveau de gravité, les impacts potentiels et le niveau de priorité du traitement.

2. Activation de la procédure. Selon la criticité de l'incident, les responsables compétents déclenchent les procédures prévues dans le plan de gestion des incidents et désignent les personnes chargées de coordonner les actions de réponse.

3. Mesures de confinement. L'Organisation prend toutes les mesures nécessaires pour limiter la propagation de l'incident, sécuriser les systèmes concernés, suspendre les opérations à risque, protéger les ressources et préserver les éléments de preuve.

4. Coordination des acteurs. Les responsables de la conformité, des finances, des technologies de l'information, des ressources humaines, de la communication et de la gouvernance coopèrent afin d'assurer une réponse cohérente et rapide.

5. Communication interne. Les informations relatives à l'incident sont communiquées aux seules personnes habilitées, selon le principe du besoin d'en connaître, afin de garantir une gestion maîtrisée de la situation.

6. Communication externe. Lorsque cela est nécessaire, l'Organisation informe les partenaires concernés, les prestataires, les établissements financiers, les autorités compétentes ou toute autre partie prenante conformément aux obligations légales et contractuelles.

7. Analyse des causes. Une investigation approfondie est menée afin d'identifier les causes profondes de l'incident, les vulnérabilités exploitées et les mesures permettant d'éviter sa réapparition.

8. Rétablissement des activités. Les systèmes, processus et services affectés sont progressivement remis en fonctionnement après validation des mesures correctives et vérification de leur sécurité.

9. Retour d'expérience. Chaque incident donne lieu à un rapport détaillé intégrant les enseignements tirés, les recommandations formulées et les améliorations à apporter aux procédures, aux contrôles et aux dispositifs de prévention.

Par cette procédure, AGCE International garantit une gestion rapide, coordonnée et efficace des incidents tout en renforçant durablement sa résilience opérationnelle et sa capacité à protéger ses missions humanitaires.

8.74 Gestion de crise

La **gestion de crise** constitue le niveau le plus élevé du dispositif de gestion des incidents de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle est déclenchée lorsqu'un événement exceptionnel menace gravement la continuité des activités, la sécurité des personnes, les ressources financières, les systèmes d'information, la réputation institutionnelle ou le respect des obligations réglementaires. Cette politique établit les principes permettant d'assurer une gouvernance de crise efficace, coordonnée et adaptée aux enjeux.

1. Définition de la crise. Une crise correspond à un incident majeur dont les conséquences dépassent les capacités normales de gestion opérationnelle et nécessitent une mobilisation exceptionnelle des ressources de l'Organisation.

2. Critères de déclenchement. La cellule de crise peut être activée en cas de cyberattaque majeure, de fraude financière importante, de fuite massive de données, de catastrophe naturelle, de défaillance critique des infrastructures, de menace sécuritaire, de crise sanitaire, de contentieux majeur ou de tout autre événement susceptible de compromettre durablement les activités de l'Organisation.

3. Activation de la cellule de crise. Dès la reconnaissance de la situation de crise, une cellule de crise est constituée sous l'autorité de la Direction Générale ou des organes de gouvernance compétents. Elle coordonne l'ensemble des décisions stratégiques et opérationnelles.

4. Coordination des actions. La cellule de crise organise les priorités d'intervention, répartit les responsabilités, mobilise les ressources humaines, techniques et financières nécessaires et assure le suivi permanent de l'évolution de la situation.

5. Protection des personnes et des ressources. Les premières mesures visent à garantir la sécurité des personnes, la préservation des données, la protection des actifs financiers, la continuité des activités essentielles et la limitation des dommages.

6. Communication de crise. Toute communication interne ou externe est centralisée, validée et diffusée de manière cohérente afin de fournir une information fiable, de limiter les rumeurs et de préserver la confiance des membres, partenaires, donateurs, bénéficiaires, autorités publiques et bailleurs de fonds.

7. Coopération avec les autorités. Lorsque la nature de la crise l'exige, AGCE International coopère pleinement avec les autorités administratives, judiciaires, réglementaires, les établissements financiers, les services de secours et les partenaires institutionnels compétents.

8. Retour à la normale. Une fois la crise maîtrisée, l'Organisation met en œuvre un plan de rétablissement permettant la reprise progressive des activités, la restauration des systèmes, le suivi des mesures correctives et l'accompagnement des personnes affectées.

9. Capitalisation de l'expérience. Chaque crise fait l'objet d'un rapport d'évaluation détaillé présentant les décisions prises, les difficultés rencontrées, les résultats obtenus et les recommandations destinées à renforcer les plans de continuité d'activité, la gestion des risques, les dispositifs de sécurité et la préparation aux crises futures.

Par cette politique de gestion de crise, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** démontre sa capacité à anticiper, gérer et surmonter les événements majeurs pouvant affecter ses activités. Elle consolide ainsi la continuité de ses missions humanitaires, la protection de ses ressources, la confiance de ses parties prenantes et son engagement permanent en faveur d'une gouvernance responsable, résiliente et conforme aux meilleures pratiques internationales.

8.75 Communication interne

La **communication interne** constitue un pilier essentiel de la gestion efficace des incidents au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Une circulation rapide, fiable, cohérente et sécurisée de l'information permet de coordonner les actions, de limiter les impacts opérationnels, d'assurer la protection des personnes et des ressources, et de favoriser une prise de décision éclairée. Dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), toute communication interne relative à un incident est réalisée dans le respect des principes de confidentialité, d'intégrité, de traçabilité et du besoin d'en connaître.

1. Objectif

La communication interne vise à assurer une transmission rapide des informations essentielles afin de permettre une réaction coordonnée, proportionnée et efficace face à tout incident susceptible d'affecter les activités de l'Organisation.

2. Activation du dispositif

Dès la détection d'un incident, les responsables compétents déclenchent le processus de communication interne conformément au niveau de gravité constaté et aux procédures institutionnelles.

3. Identification des destinataires

Les informations sont diffusées exclusivement aux personnes dont les responsabilités nécessitent leur connaissance, notamment les membres de la Direction, les responsables de la conformité, les équipes financières, informatiques, juridiques, administratives ainsi que toute autre personne concernée.

4. Exactitude des informations

Toutes les communications doivent être objectives, exactes, vérifiées et documentées afin d'éviter toute diffusion d'informations erronées, contradictoires ou incomplètes.

5. Confidentialité

Les informations relatives aux incidents sont classifiées selon leur niveau de sensibilité et protégées contre toute divulgation non autorisée.

6. Canaux de communication

Les échanges utilisent exclusivement les canaux institutionnels sécurisés mis à disposition par l'Organisation : messagerie professionnelle, plateformes collaboratives sécurisées, systèmes de ticketing, appels téléphoniques officiels ou réunions d'urgence.

7. Coordination

Chaque responsable veille à transmettre les informations utiles à son équipe tout en assurant une coordination permanente avec les autres services impliqués.

8. Suivi documentaire

Toutes les communications importantes sont enregistrées afin d'assurer leur traçabilité, leur archivage et leur exploitation lors des audits ou des retours d'expérience.

9. Amélioration continue

Chaque incident permet d'améliorer les procédures de communication, les délais de diffusion et les mécanismes de coordination interne.

En adoptant une communication interne structurée, AGCE International garantit une gestion harmonisée des incidents, une meilleure coordination des équipes et une réduction significative des impacts opérationnels.

8.76 Communication externe

La **communication externe** représente une composante stratégique de la gestion des incidents. Elle vise à préserver la confiance des membres, bénéficiaires, donateurs, partenaires, établissements financiers, autorités publiques, bailleurs de fonds et du grand public tout en respectant les exigences légales, réglementaires et contractuelles. AGCE International veille à diffuser une information transparente, maîtrisée et cohérente, sans compromettre les investigations en cours ni la confidentialité des données.

1. Objectif

Informar les parties prenantes concernées de manière responsable tout en protégeant les intérêts de l'Organisation.

2. Autorisation préalable

Aucune communication externe ne peut être diffusée sans validation préalable de la Direction Générale ou des responsables officiellement habilités.

3. Porte-parole officiel

Seules les personnes expressément désignées sont autorisées à représenter l'Organisation auprès des médias, des autorités ou des partenaires.

4. Transparence

Les informations communiquées doivent être sincères, précises, proportionnées et conformes aux faits établis.

5. Respect de la confidentialité

Les données sensibles, personnelles, bancaires, médicales ou couvertes par une enquête ne peuvent être divulguées sans autorisation légale.

6. Communication avec les autorités

L'Organisation coopère pleinement avec les autorités administratives, judiciaires, financières et de régulation lorsqu'une déclaration est exigée.

7. Information des partenaires

Les partenaires concernés sont informés lorsque l'incident est susceptible d'avoir un impact sur leurs activités ou leurs obligations contractuelles.

8. Gestion des médias

Toute sollicitation médiatique est traitée selon une procédure spécifique garantissant une communication cohérente et institutionnelle.

9. Retour d'expérience

Après résolution de l'incident, l'Organisation peut publier des informations générales destinées à renforcer la sensibilisation et l'amélioration continue, sans compromettre la confidentialité.

Cette politique renforce la crédibilité institutionnelle d'AGCE International et consolide les relations de confiance avec l'ensemble de ses parties prenantes.

8.77 Plan de continuité d'activité

Le **Plan de Continuité d'Activité (PCA)** constitue un dispositif stratégique permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** d'assurer le maintien de ses missions essentielles malgré la survenance d'un incident majeur, d'une catastrophe ou d'une crise. Il garantit la continuité des activités humanitaires, administratives, financières et numériques en limitant les interruptions de service.

1. Objectif

Maintenir les activités critiques et réduire les conséquences des interruptions.

2. Identification des activités essentielles

L'Organisation identifie les processus indispensables au fonctionnement de ses missions.

3. Analyse des risques

Les scénarios susceptibles d'interrompre les activités sont régulièrement évalués.

4. Organisation des responsabilités

Les rôles et responsabilités des équipes sont clairement définis avant toute situation de crise.

5. Ressources critiques

Les ressources humaines, financières, documentaires, logistiques et numériques indispensables sont identifiées et sécurisées.

6. Solutions de continuité

Des procédures alternatives permettent de poursuivre les activités essentielles en cas d'indisponibilité des infrastructures principales.

7. Tests réguliers

Le PCA est testé périodiquement au moyen d'exercices et de simulations.

8. Formation

Les collaborateurs sont sensibilisés aux procédures de continuité afin de garantir leur bonne application.

9. Révision permanente

Le PCA est régulièrement actualisé afin de tenir compte des évolutions organisationnelles, réglementaires et technologiques.

Grâce à ce plan, AGCE International renforce sa résilience institutionnelle et assure la continuité de ses engagements humanitaires dans toutes les circonstances.

8.78 Reprise après sinistre

La **reprise après sinistre** regroupe l'ensemble des procédures permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de restaurer rapidement ses infrastructures, ses systèmes d'information, ses données et ses activités après un événement majeur. Ce dispositif complète le Plan de Continuité d'Activité en assurant un retour sécurisé à un fonctionnement normal.

1. Objectif

Rétablir les activités de l'Organisation dans les meilleurs délais après un sinistre.

2. Évaluation des dommages

Une analyse rapide est réalisée afin de mesurer les impacts humains, matériels, financiers, numériques et organisationnels.

3. Priorisation

Les systèmes et services les plus critiques sont restaurés en priorité.

4. Sauvegardes

Les restaurations sont effectuées exclusivement à partir de sauvegardes sécurisées, vérifiées et régulièrement testées.

5. Vérification de l'intégrité

Avant toute remise en production, les systèmes restaurés sont contrôlés afin de garantir leur intégrité, leur sécurité et leur conformité.

6. Coordination

Les équipes techniques, administratives, financières, juridiques et de conformité collaborent étroitement durant toute la phase de reprise.

7. Communication

Les parties prenantes concernées sont informées de l'évolution des opérations de rétablissement selon les procédures de communication de crise.

8. Retour progressif à la normale

Les activités sont rétablies progressivement après validation de chaque étape de reprise.

9. Retour d'expérience

Chaque sinistre fait l'objet d'un rapport détaillé identifiant les causes, les actions correctives et les améliorations à intégrer aux plans de continuité, de sécurité et de gestion des risques.

Par cette politique de reprise après sinistre, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme son engagement à préserver la continuité de ses missions humanitaires, la sécurité de son patrimoine informationnel, la protection de ses ressources financières et la confiance de ses membres, partenaires, donateurs, bénéficiaires et autorités compétentes, conformément aux meilleures pratiques internationales en matière de résilience organisationnelle, de gouvernance et de conformité.

SECTION IX

AUDIT, CONFORMITÉ ET AMÉLIORATION CONTINUE

8.79 Auto-évaluation

L'**auto-évaluation** constitue un mécanisme fondamental du système de gouvernance, de contrôle interne et de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle permet à l'Organisation d'apprécier régulièrement le niveau d'efficacité de ses dispositifs de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), de contrôle interne, de gestion des risques, de cybersécurité, de protection des données, de gouvernance et de gestion financière. En favorisant une analyse critique et objective de ses propres pratiques, l'Organisation renforce sa capacité à identifier les points forts, détecter les insuffisances, anticiper les risques émergents et mettre en œuvre les actions correctives nécessaires avant la survenance d'incidents majeurs ou de non-conformités. L'auto-évaluation constitue ainsi un levier essentiel d'amélioration continue, de transparence institutionnelle et de responsabilisation de l'ensemble des acteurs impliqués dans la gouvernance de l'Organisation.

1. Objectif de l'auto-évaluation

L'auto-évaluation a pour objectif de mesurer périodiquement le niveau de conformité de l'Organisation avec les exigences légales, réglementaires, contractuelles et institutionnelles, tout en évaluant l'efficacité des dispositifs de prévention, de détection et de maîtrise des risques.

2. Champ d'application

Le processus d'auto-évaluation couvre l'ensemble des activités de l'Organisation, notamment la gouvernance, les opérations financières, les systèmes d'information, les dispositifs LBC/FT, les procédures KYC, les ressources humaines, les partenariats, les programmes humanitaires, les plateformes numériques, la protection des données, les paiements électroniques, les mécanismes de contrôle interne ainsi que les activités administratives et opérationnelles.

3. Responsabilité des acteurs

Chaque administrateur, dirigeant, responsable de service, collaborateur, bénévole et partenaire concerné participe, dans son domaine de compétence, au processus d'auto-évaluation en fournissant des informations exactes, complètes et documentées permettant une appréciation objective des pratiques et des résultats.

4. Méthodologie d'évaluation

L'Organisation utilise des référentiels internes, des grilles d'analyse, des indicateurs de performance, des questionnaires d'auto-contrôle, des revues documentaires, des entretiens, des analyses de risques et des contrôles de cohérence afin d'évaluer de manière structurée chaque composante de son dispositif de conformité.

5. Analyse des résultats

Les résultats obtenus sont examinés afin d'identifier les écarts entre les exigences applicables et les pratiques effectivement mises en œuvre. Cette analyse permet de distinguer les bonnes pratiques, les axes d'amélioration, les vulnérabilités, les non-conformités et les risques susceptibles d'affecter les objectifs institutionnels.

6. Élaboration des plans d'action

Toute insuffisance identifiée donne lieu à un plan d'action formalisé précisant les mesures correctives, les responsabilités attribuées, les ressources nécessaires, les délais de mise en œuvre ainsi que les indicateurs permettant d'en mesurer l'efficacité.

7. Suivi des actions correctives

Les recommandations issues de l'auto-évaluation font l'objet d'un suivi régulier jusqu'à leur mise en œuvre complète. Les responsables désignés rendent compte périodiquement de l'état d'avancement des actions engagées afin de garantir leur exécution effective.

8. Documentation et traçabilité

L'ensemble des travaux d'auto-évaluation, des observations, des conclusions, des plans d'action et des décisions prises est documenté, archivé et conservé conformément aux politiques institutionnelles de gestion documentaire et de conservation des preuves, afin de faciliter les audits internes, externes et les contrôles réglementaires.

9. Révision périodique

L'auto-évaluation est réalisée selon une fréquence définie par l'Organisation et peut être renouvelée à tout moment en cas d'évolution réglementaire, de modification des activités, d'incident majeur, de recommandation d'audit ou d'apparition de nouveaux risques susceptibles d'affecter la conformité ou la sécurité des opérations.

10. Culture de l'amélioration continue

L'auto-évaluation ne constitue pas un simple exercice de contrôle, mais un processus permanent d'apprentissage institutionnel favorisant l'innovation, le renforcement des compétences, l'amélioration des procédures, l'optimisation des contrôles internes et le développement d'une culture de conformité partagée par l'ensemble des parties prenantes.

11. Intégration dans la gouvernance institutionnelle

Les conclusions de l'auto-évaluation sont communiquées aux organes de gouvernance compétents afin d'alimenter la prise de décision stratégique, l'allocation des ressources, la planification des audits, la gestion des risques et la définition des priorités d'amélioration. Elles contribuent à renforcer la responsabilité des dirigeants et à assurer une supervision efficace des dispositifs de conformité et de contrôle interne.

Par cette politique d'auto-évaluation, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme son engagement en faveur d'une gouvernance proactive, transparente et responsable. En évaluant régulièrement ses pratiques, en corrigeant les insuffisances identifiées et en adaptant continuellement ses mécanismes de contrôle, l'Organisation consolide la résilience de son système de conformité, protège durablement ses ressources, garantit la qualité de ses opérations et renforce la confiance de ses membres, partenaires, donateurs, bénéficiaires, bailleurs de fonds et autorités de contrôle, conformément aux meilleures pratiques nationales et internationales en matière de gouvernance, de lutte contre le blanchiment de capitaux et le financement du terrorisme.

8.80 Contrôle permanent

Le **contrôle permanent** constitue un dispositif essentiel de surveillance continue permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** d'assurer le respect constant de ses obligations légales, réglementaires, institutionnelles et opérationnelles. Contrairement aux contrôles ponctuels, le contrôle permanent s'exerce quotidiennement à tous les niveaux de l'Organisation afin de prévenir les risques, détecter rapidement les anomalies et garantir l'application effective des politiques relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), à la gouvernance, au contrôle interne, à la cybersécurité, à la protection des données et à la gestion financière. Il participe activement au maintien d'une culture de conformité, de transparence et de responsabilité dans l'ensemble des activités de l'Organisation.

1. Objectif du contrôle permanent

Le contrôle permanent a pour finalité d'assurer une surveillance continue des activités afin d'identifier rapidement toute anomalie, non-conformité ou situation susceptible de compromettre les objectifs stratégiques et les obligations réglementaires de l'Organisation.

2. Champ d'application

Le dispositif couvre l'ensemble des processus administratifs, financiers, comptables, numériques, opérationnels, logistiques, contractuels, humanitaires et institutionnels de l'Organisation, sans exception.

3. Responsabilité des acteurs

Chaque responsable hiérarchique exerce un contrôle permanent dans son domaine de compétence. Tous les collaborateurs, bénévoles, administrateurs et partenaires contribuent à la qualité du dispositif en respectant les procédures internes et en signalant toute anomalie constatée.

4. Contrôles quotidiens

Les opérations sensibles font l'objet de vérifications régulières portant notamment sur les paiements, les encaissements, les autorisations, les rapprochements comptables, les accès informatiques, les habilitations, les dossiers KYC, les contrats et les engagements financiers.

5. Surveillance des risques

Le contrôle permanent repose sur une surveillance continue des indicateurs de risque, des alertes automatiques, des incidents déclarés, des opérations inhabituelles et des évolutions réglementaires susceptibles d'affecter l'Organisation.

6. Documentation

Toutes les opérations de contrôle sont documentées de manière claire, datée et traçable afin de permettre leur vérification lors des audits internes, externes ou des inspections des autorités compétentes.

7. Traitement des anomalies

Toute anomalie identifiée fait immédiatement l'objet d'une analyse, d'une évaluation des risques et, lorsque cela est nécessaire, d'un plan d'action correctif permettant d'éliminer la cause du dysfonctionnement.

8. Reporting

Les résultats du contrôle permanent sont communiqués périodiquement aux organes de gouvernance afin d'éclairer les décisions stratégiques et de renforcer la maîtrise des risques.

9. Amélioration continue

Les enseignements issus du contrôle permanent alimentent la révision des procédures, des dispositifs de sécurité, des programmes de formation et des mécanismes de gouvernance.

Par cette politique de contrôle permanent, **AGCE International – AGCE Canada** garantit une surveillance continue de ses activités, renforce la maîtrise de ses risques et favorise une gouvernance responsable conforme aux meilleures pratiques internationales.

8.81 Audit interne

L'**audit interne** constitue une fonction indépendante et objective destinée à évaluer l'efficacité des dispositifs de gouvernance, de contrôle interne, de gestion des risques et de conformité mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il fournit aux organes de gouvernance une assurance raisonnable sur la qualité des processus institutionnels tout en formulant des recommandations destinées à renforcer la performance, la transparence et la conformité de l'Organisation.

1. Objet de l'audit interne

L'audit interne vise à apprécier l'efficacité des politiques, procédures, contrôles et mécanismes de gouvernance afin d'améliorer durablement le fonctionnement de l'Organisation.

2. Indépendance

Les missions d'audit sont réalisées en toute indépendance, objectivité et impartialité, sans interférence des services audités.

3. Champ d'intervention

Les audits peuvent porter sur les finances, la comptabilité, les ressources humaines, les achats, les systèmes d'information, la cybersécurité, la protection des données, les projets humanitaires, les partenariats, les dispositifs LBC/FT, les contrôles KYC et tout autre domaine jugé prioritaire.

4. Planification

Les missions sont programmées selon une approche fondée sur les risques, la criticité des activités, les obligations réglementaires et les priorités stratégiques de l'Organisation.

5. Déroulement des missions

Chaque mission comprend une phase de préparation, de collecte des informations, de vérification documentaire, d'entretiens, de tests de conformité, d'analyse des risques et de formulation des constats.

6. Rapport d'audit

À l'issue de chaque mission, un rapport détaillé présente les observations, les risques identifiés, les bonnes pratiques constatées, les recommandations formulées ainsi que les priorités de mise en conformité.

7. Plans d'action

Les responsables des services concernés élaborent des plans d'action destinés à mettre en œuvre les recommandations dans les délais convenus.

8. Suivi des recommandations

L'audit interne assure le suivi de l'exécution des mesures correctives jusqu'à leur mise en œuvre effective.

9. Confidentialité

Toutes les informations recueillies durant les missions d'audit sont protégées conformément aux règles de confidentialité, de sécurité des données et de secret professionnel.

10. Contribution à l'amélioration continue

Les conclusions des audits alimentent la gestion des risques, la révision des politiques, la formation des équipes et le renforcement du contrôle interne.

Par cette politique, **AGCE International – AGCE Canada** affirme que l'audit interne constitue un instrument stratégique d'amélioration continue, de bonne gouvernance et de conformité institutionnelle.

8.82 Audit externe

L'**audit externe** permet à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de faire évaluer de manière indépendante ses états financiers, ses dispositifs de gouvernance, ses mécanismes de contrôle interne et ses procédures de conformité par des professionnels ou organismes compétents. Il renforce la crédibilité de l'Organisation auprès des autorités publiques, des partenaires, des bailleurs de fonds, des institutions financières, des donateurs et des bénéficiaires, en apportant une assurance indépendante sur la qualité de sa gestion et le respect de ses obligations.

1. Objectif

L'audit externe vise à fournir une appréciation indépendante sur la sincérité des informations financières, l'efficacité des contrôles et le niveau global de conformité de l'Organisation.

2. Indépendance des auditeurs

Les auditeurs externes sont choisis selon des critères de compétence, d'intégrité, d'indépendance et d'absence de conflit d'intérêts.

3. Domaines audités

Les missions peuvent porter sur les états financiers, les procédures comptables, les systèmes d'information, les contrôles internes, la conformité réglementaire, les dispositifs LBC/FT, les projets financés, les subventions, les dons et les programmes institutionnels.

4. Collaboration

L'Organisation met à la disposition des auditeurs l'ensemble des documents, informations, systèmes et personnes nécessaires à la réalisation de leurs travaux, dans le respect des règles de confidentialité.

5. Rapport d'audit

À l'issue de la mission, les auditeurs remettent un rapport présentant leurs observations, leurs conclusions, leur opinion professionnelle ainsi que les recommandations destinées à améliorer les dispositifs existants.

6. Mise en œuvre des recommandations

Les recommandations issues des audits externes sont examinées par les organes de gouvernance qui élaborent un plan d'action précisant les responsabilités, les échéances et les modalités de suivi.

7. Suivi institutionnel

La Direction et les organes de gouvernance assurent le suivi régulier de la mise en œuvre des recommandations formulées afin de garantir leur exécution effective.

8. Transparence

Les résultats des audits externes peuvent être communiqués aux partenaires, bailleurs de fonds, autorités compétentes ou autres parties prenantes lorsque les obligations légales, contractuelles ou institutionnelles le prévoient.

9. Renforcement de la gouvernance

Les conclusions des audits externes contribuent à améliorer la gouvernance, la gestion des risques, la conformité réglementaire, la qualité des contrôles internes et la performance globale de l'Organisation.

10. Amélioration continue

Les enseignements tirés des audits externes sont intégrés dans les politiques, procédures, formations et mécanismes de contrôle afin d'assurer une amélioration permanente des pratiques institutionnelles.

Par cette politique d'audit externe, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** réaffirme son engagement en faveur d'une gestion rigoureuse, transparente et responsable. En soumettant régulièrement ses dispositifs à une évaluation indépendante, l'Organisation renforce la confiance de ses membres, partenaires, donateurs, bailleurs de fonds et autorités de contrôle, tout en consolidant sa conformité aux meilleures pratiques nationales et internationales en matière de gouvernance, de lutte contre le blanchiment de capitaux et le financement du terrorisme.

8.83 Revues périodiques

Les **revues périodiques** constituent un mécanisme stratégique de surveillance et d'amélioration continue permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** d'évaluer régulièrement l'efficacité de son dispositif de gouvernance, de conformité, de contrôle interne, de gestion des risques, de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), de cybersécurité et de protection des données. Ces revues permettent d'apprécier l'adéquation des politiques, des procédures et des contrôles au regard des évolutions réglementaires, des risques émergents, des objectifs institutionnels et des meilleures pratiques internationales. Elles contribuent à garantir une gouvernance proactive, transparente et fondée sur l'amélioration permanente.

1. Objectif des revues périodiques

Les revues périodiques visent à vérifier que les politiques, procédures, dispositifs de contrôle et mécanismes de conformité demeurent efficaces, adaptés et pleinement opérationnels.

2. Champ d'application

Les revues portent sur l'ensemble des domaines d'activité de l'Organisation, notamment les opérations financières, les procédures KYC, les dispositifs LBC/FT, les systèmes d'information, la cybersécurité, les ressources humaines, les partenariats, les programmes humanitaires, les plateformes numériques, les mécanismes de gouvernance ainsi que les contrôles internes.

3. Fréquence des revues

Les revues sont réalisées selon une planification définie par l'Organisation et peuvent être complétées par des évaluations extraordinaires en cas d'évolution réglementaire, d'incident majeur, de recommandation d'audit ou d'apparition de nouveaux risques.

4. Responsabilités

Les responsables des différentes fonctions participent activement aux revues en fournissant les informations, rapports, indicateurs et éléments justificatifs nécessaires à une évaluation complète et objective.

5. Méthodologie

Les revues reposent sur l'analyse documentaire, les entretiens, les contrôles de conformité, l'examen des indicateurs de performance, les résultats des audits, les incidents déclarés, les retours d'expérience ainsi que les évaluations des risques.

6. Identification des écarts

Toute non-conformité, faiblesse de contrôle, insuffisance organisationnelle ou vulnérabilité identifiée est documentée et classée selon son niveau de criticité afin de déterminer les priorités d'intervention.

7. Plans d'amélioration

Chaque revue donne lieu à un plan d'amélioration précisant les actions correctives, les responsables, les ressources mobilisées, les échéances et les modalités de suivi.

8. Validation des résultats

Les conclusions des revues sont examinées par les organes de gouvernance compétents qui valident les recommandations et suivent leur mise en œuvre.

9. Capitalisation des enseignements

Les enseignements issus des revues périodiques alimentent la mise à jour des politiques, des procédures, des formations, des contrôles et de la cartographie des risques.

10. Amélioration continue

Les revues périodiques participent au renforcement permanent de la gouvernance, de la conformité et de la performance institutionnelle.

Par cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** confirme sa volonté de maintenir un système de gouvernance dynamique, fondé sur une évaluation régulière de ses pratiques, la maîtrise de ses risques et l'amélioration constante de ses dispositifs de conformité.

8.84 Indicateurs de conformité

Les **indicateurs de conformité** constituent des outils de pilotage permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de mesurer de manière objective l'efficacité de son dispositif de conformité, de gestion des risques et de contrôle interne. Ils fournissent une vision quantitative et qualitative de la performance des mécanismes de prévention, de détection et de correction des non-conformités, tout en facilitant la prise de décision des organes de gouvernance. Ces indicateurs permettent d'anticiper les risques, de suivre les tendances et d'évaluer l'atteinte des objectifs institutionnels dans le respect des exigences LBC/FT et des normes internationales.

1. Objectif

Mesurer en permanence le niveau de conformité de l'Organisation et l'efficacité de ses dispositifs de contrôle.

2. Principes

Les indicateurs doivent être pertinents, fiables, mesurables, vérifiables, comparables et régulièrement actualisés.

3. Domaines de mesure

Les indicateurs couvrent notamment les procédures KYC, les déclarations d'opérations suspectes, les contrôles internes, les audits, les formations, les incidents, la cybersécurité, la protection des données, les paiements, les partenariats, les projets et les obligations réglementaires.

4. Collecte des données

Les données sont collectées à partir des systèmes d'information, des rapports de contrôle, des audits, des registres institutionnels, des plateformes numériques et des tableaux de suivi.

5. Analyse

Les résultats sont comparés aux objectifs fixés, aux seuils d'alerte et aux performances historiques afin d'identifier les écarts, les tendances et les risques émergents.

6. Alerte

Des seuils de vigilance sont définis pour déclencher des investigations ou des actions correctives lorsqu'un indicateur révèle une dégradation significative.

7. Reporting

Les indicateurs sont présentés périodiquement aux organes de gouvernance afin d'appuyer les décisions stratégiques et opérationnelles.

8. Révision

Les indicateurs sont régulièrement adaptés en fonction de l'évolution des risques, des activités et des exigences réglementaires.

9. Utilisation stratégique

Les indicateurs servent également à mesurer la maturité du dispositif de conformité et à orienter les priorités d'amélioration continue.

10. Culture de la performance

L'Organisation encourage une utilisation responsable des indicateurs comme outils de progrès, de transparence et de responsabilisation.

Par cette politique, AGCE International fait des indicateurs de conformité un instrument central de pilotage permettant d'assurer une surveillance continue, une meilleure anticipation des risques et un renforcement durable de la gouvernance institutionnelle.

8.85 Tableaux de bord

Les **tableaux de bord** constituent des instruments de gouvernance et d'aide à la décision permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de suivre en temps réel ou à intervalles réguliers l'état de son dispositif de conformité, de gestion des risques, de contrôle interne et de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Ils centralisent les informations essentielles, facilitent la surveillance des indicateurs clés de performance et permettent aux organes de gouvernance d'identifier rapidement les situations nécessitant une intervention.

1. Finalité

Les tableaux de bord permettent de disposer d'une vision synthétique, fiable et actualisée de la performance des dispositifs de gouvernance et de conformité.

2. Contenu

Ils regroupent notamment les indicateurs de conformité, les résultats des contrôles permanents, les conclusions des audits, les incidents enregistrés, les risques identifiés, les actions

correctives, les formations réalisées, les déclarations réglementaires ainsi que les niveaux de conformité des différents services.

3. Actualisation

Les tableaux de bord sont mis à jour selon une fréquence adaptée à la nature des indicateurs et aux besoins de pilotage de l'Organisation.

4. Accessibilité

L'accès est limité aux personnes dûment habilitées conformément aux règles de confidentialité, de sécurité de l'information et de gestion des habilitations.

5. Analyse décisionnelle

Les données présentées permettent aux responsables d'identifier rapidement les écarts, les tendances, les priorités d'action et les risques nécessitant une décision immédiate.

6. Suivi des plans d'action

Les tableaux de bord assurent le suivi de l'avancement des mesures correctives, des recommandations d'audit et des projets d'amélioration.

7. Aide à la gouvernance

Ils constituent un support essentiel lors des réunions de direction, des comités de conformité, des audits et des revues stratégiques.

8. Traçabilité

Toutes les données intégrées aux tableaux de bord sont documentées, vérifiables et conservées conformément aux politiques institutionnelles de gestion documentaire.

9. Évolution continue

Les tableaux de bord sont régulièrement enrichis afin d'intégrer de nouveaux indicateurs, de nouvelles exigences réglementaires, les innovations technologiques et les besoins émergents de l'Organisation.

10. Contribution à l'excellence institutionnelle

Les tableaux de bord favorisent une prise de décision rapide, objective et fondée sur des données fiables, renforçant ainsi la transparence, la responsabilité et la performance globale de l'Organisation.

Par cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** fait des tableaux de bord un outil stratégique de pilotage et de gouvernance, garantissant un suivi permanent de la conformité, une meilleure maîtrise des risques et une amélioration continue de ses performances institutionnelles conformément aux meilleures pratiques internationales.

8.86 Gestion des non-conformités

La **gestion des non-conformités** constitue un élément central du dispositif de gouvernance, de contrôle interne et d'amélioration continue de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle vise à identifier, enregistrer, analyser, traiter et corriger toute situation dans laquelle une activité, une procédure, un comportement, une décision ou un résultat ne respecte pas les exigences légales, réglementaires, contractuelles ou institutionnelles applicables. Cette démarche contribue à renforcer la maîtrise des risques, la conformité aux obligations relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), ainsi que la qualité globale des activités de l'Organisation.

1. Définition de la non-conformité

Une non-conformité désigne tout écart constaté entre une exigence applicable et les pratiques effectivement mises en œuvre au sein de l'Organisation. Elle peut résulter d'une erreur, d'une omission, d'un dysfonctionnement, d'une défaillance organisationnelle ou d'un non-respect volontaire des règles établies.

2. Champ d'application

La gestion des non-conformités concerne l'ensemble des domaines d'activité de l'Organisation, notamment la gouvernance, les finances, la comptabilité, les ressources humaines, les achats, les systèmes d'information, la cybersécurité, les projets humanitaires, les partenariats, les procédures KYC, les dispositifs LBC/FT, la protection des données et les obligations réglementaires.

3. Identification

Les non-conformités peuvent être détectées lors des contrôles permanents, des audits internes ou externes, des auto-évaluations, des inspections, des signalements, des incidents opérationnels ou des revues périodiques.

4. Enregistrement

Toute non-conformité identifiée est enregistrée dans un registre institutionnel sécurisé précisant sa nature, son origine, sa date de détection, son niveau de gravité, les personnes concernées et les premières mesures prises.

5. Évaluation des risques

Chaque non-conformité fait l'objet d'une analyse permettant d'évaluer ses conséquences potentielles sur les plans juridique, financier, opérationnel, technologique, réputationnel et organisationnel.

6. Traitement

Des mesures immédiates peuvent être mises en œuvre afin de limiter les impacts de la non-conformité, de protéger les ressources de l'Organisation et de prévenir toute aggravation de la situation.

7. Recherche des causes

Une analyse approfondie est conduite afin d'identifier les causes profondes de la non-conformité, qu'elles soient organisationnelles, humaines, techniques, procédurales ou réglementaires.

8. Responsabilisation

Les responsables concernés participent activement à la résolution des non-conformités et à la mise en œuvre des mesures correctives dans le respect des principes de transparence, de responsabilité et de coopération.

9. Documentation et traçabilité

Toutes les étapes de traitement sont documentées afin de garantir la traçabilité des décisions, de faciliter les audits et de démontrer le respect des obligations de conformité.

10. Intégration dans l'amélioration continue

Les enseignements issus des non-conformités alimentent la révision des politiques, des procédures, des contrôles internes, des formations et des dispositifs de gestion des risques.

Par cette politique de gestion des non-conformités, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce sa capacité à détecter rapidement les écarts, à mettre en œuvre des solutions adaptées et à consolider une culture institutionnelle fondée sur la conformité, la transparence, la responsabilité et l'amélioration continue.

8.87 Plans d'actions correctives

Les **plans d'actions correctives** constituent le prolongement opérationnel de la gestion des non-conformités. Ils permettent à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de transformer les

constats issus des audits, contrôles, inspections, incidents, auto-évaluations ou revues périodiques en actions concrètes, planifiées et mesurables. Leur objectif est d'éliminer durablement les causes des dysfonctionnements, de prévenir leur réapparition et de renforcer l'efficacité globale des dispositifs de gouvernance, de conformité et de contrôle interne.

1. Élaboration du plan

Chaque non-conformité significative donne lieu à un plan d'actions correctives formalisé et validé par les responsables compétents.

2. Définition des objectifs

Les actions proposées visent à supprimer les causes identifiées, à restaurer la conformité et à réduire durablement les risques.

3. Désignation des responsables

Chaque action est confiée à un responsable clairement identifié disposant des compétences et des moyens nécessaires à sa mise en œuvre.

4. Détermination des délais

Les échéances de réalisation sont fixées en fonction du niveau de priorité, de la gravité des risques et des contraintes opérationnelles.

5. Allocation des ressources

L'Organisation mobilise les ressources humaines, financières, techniques et organisationnelles nécessaires à l'exécution des actions prévues.

6. Priorisation

Les mesures sont classées selon leur niveau d'urgence et leur impact potentiel sur la conformité, la sécurité et la continuité des activités.

7. Validation

Les plans d'actions sont examinés et approuvés par les instances de gouvernance compétentes avant leur mise en œuvre.

8. Contrôle de l'exécution

L'état d'avancement des actions est régulièrement vérifié afin de garantir le respect des délais et l'efficacité des mesures adoptées.

9. Vérification de l'efficacité

Une fois les actions réalisées, leur efficacité est évaluée afin de confirmer que les causes de la non-conformité ont effectivement été éliminées.

10. Révision continue

Les plans d'actions peuvent être ajustés lorsque de nouveaux risques apparaissent, lorsque les circonstances évoluent ou lorsque les résultats obtenus nécessitent des adaptations complémentaires.

Par cette politique, AGCE International garantit que chaque anomalie identifiée donne lieu à une réponse structurée, mesurable et durable, contribuant au renforcement permanent de son système de gouvernance et de conformité.

8.88 Suivi des recommandations

Le **suivi des recommandations** constitue la dernière étape du cycle d'audit, de contrôle et d'amélioration continue de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il garantit que les recommandations formulées à l'issue des audits internes, des audits externes, des contrôles permanents, des auto-évaluations, des inspections et des revues périodiques sont effectivement mises en œuvre et produisent les résultats attendus. Ce suivi permet de mesurer les progrès accomplis, d'assurer la responsabilisation des acteurs et de maintenir un niveau élevé de conformité institutionnelle.

1. Objectif

Le suivi des recommandations vise à garantir la mise en œuvre effective des mesures d'amélioration approuvées par les organes de gouvernance.

2. Enregistrement

Chaque recommandation est inscrite dans un registre de suivi indiquant son origine, sa description, son niveau de priorité, son responsable et son échéance.

3. Attribution des responsabilités

Les recommandations sont confiées aux responsables concernés qui rendent compte régulièrement de leur état d'avancement.

4. Planification

Les actions sont programmées selon un calendrier réaliste prenant en compte leur priorité, leur complexité et les ressources disponibles.

5. Contrôle de l'avancement

Les responsables de la conformité et du contrôle interne vérifient périodiquement la progression des actions et identifient les éventuels retards ou difficultés.

6. Vérification des résultats

Une fois les recommandations mises en œuvre, leur efficacité est évaluée afin de confirmer qu'elles répondent pleinement aux objectifs fixés.

7. Escalade

Lorsque les recommandations ne sont pas exécutées dans les délais prévus ou demeurent insuffisamment appliquées, les organes de gouvernance compétents sont informés afin de décider des mesures appropriées.

8. Reporting

Des rapports périodiques présentent aux instances dirigeantes le niveau de mise en œuvre des recommandations, les résultats obtenus et les difficultés rencontrées.

9. Capitalisation

Les enseignements issus du suivi sont intégrés dans les politiques, procédures, formations et outils de pilotage afin de renforcer durablement les dispositifs de gouvernance et de conformité.

10. Clôture

Une recommandation n'est considérée comme clôturée qu'après vérification de sa mise en œuvre complète, de son efficacité et de la réduction effective des risques identifiés.

Par cette politique de suivi des recommandations, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** démontre son engagement envers une gouvernance responsable, un contrôle interne performant et une amélioration continue de ses pratiques. En assurant un suivi rigoureux de chaque recommandation, l'Organisation renforce la maîtrise de ses risques, la qualité de ses processus, la confiance de ses partenaires et sa conformité aux meilleures pratiques nationales et internationales en matière de gouvernance, de transparence et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

SECTION X

SANCTIONS DISCIPLINAIRES

8.89 Principes

Les **principes applicables aux sanctions disciplinaires** constituent un élément fondamental du dispositif de gouvernance, de conformité et de contrôle interne de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Ils traduisent la volonté de l'Organisation de garantir le respect des lois, des règlements, des politiques institutionnelles, du Code d'éthique, des procédures internes ainsi que des exigences relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Les sanctions disciplinaires ne poursuivent pas uniquement une finalité répressive ; elles participent également à la prévention des risques, à la protection des intérêts de l'Organisation, à la responsabilisation des acteurs et au maintien d'une culture d'intégrité, de transparence, d'équité et de bonne gouvernance. Toute mesure disciplinaire est mise en œuvre dans le respect des droits fondamentaux des personnes concernées, des principes d'impartialité, de proportionnalité, de confidentialité et de respect de la dignité humaine.

1. Objet des sanctions disciplinaires

Les sanctions disciplinaires ont pour objectif d'assurer le respect des obligations professionnelles, statutaires, contractuelles et institutionnelles, de prévenir la répétition des comportements fautifs et de préserver l'intégrité des activités, des ressources et de la réputation de l'Organisation.

2. Champ d'application

Les présentes dispositions s'appliquent à l'ensemble des administrateurs, dirigeants, membres, salariés, bénévoles, consultants, prestataires, partenaires, représentants, stagiaires ainsi qu'à toute personne agissant au nom ou pour le compte d'AGCE International – AGCE Canada, dans les limites prévues par les textes applicables et les engagements contractuels.

3. Principe de légalité

Aucune sanction disciplinaire ne peut être prononcée sans qu'un manquement aux lois, aux règlements, aux statuts, aux politiques internes, aux procédures, au Code d'éthique ou aux obligations contractuelles n'ait été préalablement identifié, documenté et évalué.

4. Principe d'équité et d'impartialité

Toute procédure disciplinaire est conduite avec objectivité, neutralité et indépendance. Les décisions sont prises sans discrimination fondée notamment sur l'origine, le sexe, la nationalité,

la religion, les opinions, le handicap, l'âge ou toute autre considération étrangère aux faits reprochés.

5. Principe du contradictoire

Avant toute décision disciplinaire, la personne concernée est informée des faits qui lui sont reprochés et dispose d'un délai raisonnable pour présenter ses observations, produire des éléments justificatifs et exercer, le cas échéant, les recours prévus par les procédures internes ou les dispositions légales applicables.

6. Principe de proportionnalité

La nature et le niveau de la sanction sont déterminés en tenant compte de la gravité des faits, de leur caractère intentionnel ou non, des conséquences produites, des circonstances de leur commission, des antécédents disciplinaires éventuels ainsi que des risques encourus par l'Organisation et ses parties prenantes.

7. Principe de confidentialité

Les procédures disciplinaires sont conduites dans le strict respect de la confidentialité. Les informations relatives aux enquêtes, aux auditions, aux décisions et aux pièces du dossier sont accessibles uniquement aux personnes habilitées à en connaître dans le cadre de leurs fonctions.

8. Principe de traçabilité

Chaque procédure disciplinaire fait l'objet d'une documentation complète comprenant les signalements, les éléments de preuve, les comptes rendus d'audition, les analyses réalisées, les décisions prises ainsi que les mesures correctives éventuellement mises en œuvre. Cette documentation est conservée conformément aux politiques institutionnelles de gestion documentaire.

9. Principe de cohérence et d'amélioration continue

Les enseignements issus des procédures disciplinaires sont exploités afin d'identifier les causes des manquements, d'améliorer les politiques internes, de renforcer les dispositifs de contrôle, de perfectionner les programmes de formation et de prévenir la récurrence des comportements non conformes.

10. Principe de conformité réglementaire

L'application des sanctions disciplinaires s'effectue dans le respect des législations nationales et internationales applicables, des exigences relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme, des règles de protection des données, des obligations contractuelles ainsi que des principes de bonne gouvernance reconnus par les partenaires institutionnels et les bailleurs de fonds.

11. Principe de protection des intérêts de l'Organisation

Les mesures disciplinaires ont également pour finalité de préserver les ressources financières, les actifs matériels et numériques, les informations sensibles, les droits des bénéficiaires, des donateurs, des partenaires et des membres, ainsi que la crédibilité et la réputation institutionnelle d'AGCE International – AGCE Canada.

En adoptant ces **principes directeurs des sanctions disciplinaires**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme son engagement à appliquer un régime disciplinaire juste, transparent, proportionné et conforme aux meilleures pratiques internationales. Ce dispositif contribue à renforcer la responsabilité individuelle et collective, à préserver la confiance des membres, partenaires, donateurs, bénéficiaires, bailleurs de fonds et autorités de contrôle, tout en consolidant durablement la gouvernance, l'intégrité institutionnelle et l'efficacité du système de conformité de l'Organisation.

8.90 Manquements

Les **manquements** désignent tout comportement, toute action, toute omission ou toute négligence susceptible de contrevenir aux lois, aux règlements, aux statuts, aux politiques institutionnelles, aux procédures internes, aux obligations contractuelles ou aux principes éthiques de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Dans le cadre de son dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), l'Organisation considère que l'identification et le traitement rigoureux des manquements constituent des éléments essentiels de la bonne gouvernance, de la maîtrise des risques et de la protection de ses ressources. Chaque manquement est apprécié de manière objective, documentée et proportionnée, en tenant compte de sa gravité, de son contexte, de son caractère intentionnel ou non, de ses conséquences et des risques qu'il fait peser sur l'Organisation et ses parties prenantes.

1. Définition du manquement

Constitue un manquement toute violation des obligations légales, réglementaires, statutaires, contractuelles, éthiques ou procédurales applicables aux activités de l'Organisation.

2. Champ des manquements

Les manquements peuvent concerner la gouvernance, les finances, la comptabilité, les ressources humaines, les achats, les systèmes d'information, la cybersécurité, la protection des données, les dispositifs KYC, les procédures LBC/FT, les partenariats, les projets humanitaires, les obligations de confidentialité ou toute autre activité institutionnelle.

3. Classification

Les manquements sont classés selon leur nature, leur gravité, leur fréquence, leur caractère intentionnel, leurs conséquences opérationnelles, financières, juridiques, réputationnelles ou sécuritaires.

4. Détection

Les manquements peuvent être identifiés lors des contrôles permanents, des audits, des inspections, des auto-évaluations, des signalements, des investigations, des incidents ou de toute autre activité de surveillance.

5. Obligation de signalement

Toute personne ayant connaissance d'un manquement est tenue d'en informer les responsables compétents selon les procédures institutionnelles de signalement.

6. Analyse

Chaque manquement fait l'objet d'une évaluation permettant d'en déterminer les causes, les responsabilités, les risques associés et les mesures appropriées.

7. Respect des droits

Toute personne concernée bénéficie des garanties prévues par les procédures disciplinaires, notamment le droit d'être entendue, de présenter ses observations et de produire tout élément utile à sa défense.

8. Mesures correctives

Outre les éventuelles sanctions disciplinaires, les manquements peuvent donner lieu à des actions correctives, des formations complémentaires, des renforcements de contrôle ou des modifications de procédures.

9. Documentation

L'ensemble des éléments relatifs au manquement est enregistré, conservé et protégé conformément aux règles institutionnelles de gestion documentaire et de confidentialité.

10. Amélioration continue

Les enseignements issus des manquements contribuent au renforcement des politiques internes, de la gouvernance, du contrôle interne et de la culture de conformité.

Par cette politique de gestion des manquements, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme sa volonté de

promouvoir une culture de responsabilité, de prévenir les comportements non conformes et de garantir le respect durable des principes de transparence, d'intégrité et de bonne gouvernance.

8.91 Mesures conservatoires

Les **mesures conservatoires** constituent des décisions temporaires prises par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** lorsqu'il existe des indices sérieux laissant présumer l'existence d'un manquement grave, d'une fraude, d'un risque de sécurité, d'une atteinte à la conformité ou de toute situation susceptible de compromettre les intérêts de l'Organisation. Elles ont pour seule finalité de préserver les personnes, les biens, les informations, les ressources financières, les preuves et le bon déroulement des investigations, sans préjuger de la responsabilité définitive de la personne concernée.

1. Objet

Les mesures conservatoires visent à prévenir toute aggravation du risque pendant la durée des investigations.

2. Caractère préventif

Elles ne constituent ni une sanction disciplinaire ni une reconnaissance de culpabilité, mais une mesure temporaire de protection.

3. Conditions de mise en œuvre

Les mesures conservatoires sont décidées lorsqu'un risque sérieux est identifié et qu'une intervention immédiate est nécessaire pour protéger les intérêts de l'Organisation.

4. Types de mesures

Selon les circonstances, elles peuvent comprendre la limitation des accès, le retrait temporaire d'habilitations, la suspension de certaines opérations, la mise sous contrôle renforcé d'un dossier, la sécurisation des équipements ou toute autre mesure proportionnée.

5. Autorité compétente

La décision est prise par les responsables habilités conformément aux règles de gouvernance et aux délégations de pouvoir de l'Organisation.

6. Proportionnalité

Les mesures sont limitées au strict nécessaire, adaptées à la gravité des faits et réévaluées régulièrement.

7. Respect des droits

La personne concernée est informée des mesures prises, sauf si cette information risque de compromettre les investigations ou la sécurité de l'Organisation.

8. Durée

Les mesures conservatoires demeurent applicables uniquement pendant le temps nécessaire aux vérifications, aux investigations ou à la maîtrise du risque identifié.

9. Révision

Les mesures peuvent être maintenues, adaptées ou levées en fonction de l'évolution des investigations et des éléments recueillis.

10. Traçabilité

Toute décision conservatoire est motivée, documentée, validée et conservée dans les dossiers institutionnels conformément aux règles de confidentialité.

Par cette politique, AGCE International garantit une gestion prudente, équilibrée et juridiquement sécurisée des situations présentant un risque immédiat pour l'Organisation, tout en préservant les droits des personnes concernées.

8.92 Suspension

La **suspension** constitue une mesure exceptionnelle pouvant être prononcée par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** lorsqu'un manquement grave, un risque important ou une situation susceptible de compromettre les intérêts de l'Organisation justifie l'interruption temporaire des fonctions, des accès, des habilitations, des activités ou de certaines prérogatives d'une personne physique ou morale. Cette mesure est mise en œuvre dans le respect des principes de légalité, de proportionnalité, d'impartialité et du contradictoire, ainsi que des dispositions légales et contractuelles applicables.

1. Objet de la suspension

La suspension vise à protéger les personnes, les ressources, les systèmes d'information, les données, les opérations financières et la réputation de l'Organisation durant le traitement d'une situation sensible.

2. Cas de recours

Elle peut être décidée notamment en cas de fraude présumée, de corruption, de conflit d'intérêts grave, de violation des règles LBC/FT, de compromission d'un système d'information,

de divulgation d'informations confidentielles ou de tout autre manquement présentant un risque élevé.

3. Nature de la mesure

La suspension est une mesure temporaire qui ne préjuge pas de la décision disciplinaire ou judiciaire définitive.

4. Autorité décisionnelle

La décision appartient aux organes ou responsables compétents conformément aux statuts, aux règlements internes et aux délégations de pouvoir.

5. Notification

La décision de suspension est notifiée à la personne concernée, accompagnée des motifs, de la durée prévisible et des modalités de réexamen, sous réserve des exigences liées aux investigations en cours.

6. Effets

Pendant la suspension, les accès, habilitations, moyens matériels ou fonctions concernés peuvent être temporairement retirés ou limités afin de préserver les intérêts de l'Organisation.

7. Réexamen

La suspension fait l'objet d'un suivi régulier et peut être modifiée, prolongée ou levée en fonction des résultats des investigations ou de l'évolution de la situation.

8. Respect des droits

La personne concernée conserve les droits procéduraux prévus par les règles internes et les dispositions légales applicables, notamment le droit de présenter ses observations.

9. Clôture de la mesure

À l'issue des investigations, la suspension prend fin et peut être suivie d'une réintégration, d'une sanction disciplinaire, d'une mesure corrective ou de toute autre décision appropriée.

10. Archivage et confidentialité

Toutes les décisions relatives à une suspension sont documentées, conservées de manière sécurisée et accessibles uniquement aux personnes habilitées.

Par cette politique de suspension, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** réaffirme son

engagement à protéger ses missions humanitaires, ses ressources, ses membres, ses partenaires et sa réputation, tout en garantissant un traitement équitable, transparent et conforme aux meilleures pratiques nationales et internationales en matière de gouvernance, de conformité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

8.93 Exclusion

L'**exclusion** constitue la sanction disciplinaire la plus élevée pouvant être prononcée par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** à l'encontre d'un administrateur, d'un membre, d'un collaborateur, d'un bénévole, d'un partenaire, d'un prestataire ou de toute autre personne physique ou morale entretenant une relation institutionnelle avec l'Organisation. Cette mesure exceptionnelle est réservée aux situations dans lesquelles les faits constatés présentent un degré de gravité incompatible avec le maintien des relations institutionnelles ou compromettent durablement les intérêts, la sécurité, la conformité, la réputation ou les missions de l'Organisation. L'exclusion est mise en œuvre dans le strict respect des principes de légalité, de proportionnalité, d'impartialité, du contradictoire et des dispositions statutaires, réglementaires et contractuelles applicables.

1. Objet de l'exclusion

L'exclusion vise à protéger durablement l'Organisation, ses membres, ses bénéficiaires, ses partenaires, ses donateurs, ses ressources financières, ses systèmes d'information et sa réputation contre les conséquences de comportements gravement incompatibles avec ses valeurs et ses obligations.

2. Cas pouvant justifier une exclusion

L'exclusion peut être prononcée notamment en cas de fraude, corruption, blanchiment de capitaux, financement du terrorisme, détournement de fonds, falsification documentaire, violation grave des règles de confidentialité, atteinte volontaire aux systèmes d'information, conflits d'intérêts dissimulés, comportements contraires au Code d'éthique ou récidive de manquements disciplinaires majeurs.

3. Procédure préalable

Toute procédure d'exclusion est précédée d'une enquête impartiale, d'une analyse des faits, de la collecte des preuves nécessaires et du respect des droits de la défense de la personne concernée.

4. Respect du contradictoire

La personne susceptible d'être exclue est informée des faits qui lui sont reprochés et dispose de la possibilité de présenter ses observations, ses explications et tout élément de preuve utile avant qu'une décision définitive ne soit prise.

5. Décision compétente

La décision d'exclusion est prise exclusivement par l'organe ou l'autorité compétente conformément aux statuts, au règlement intérieur, aux délégations de pouvoir et aux procédures disciplinaires de l'Organisation.

6. Effets de l'exclusion

L'exclusion entraîne la perte de la qualité de membre, collaborateur, partenaire ou représentant concerné, ainsi que la suppression des droits, accès, habilitations, mandats, autorisations et privilèges attachés à cette qualité, sous réserve des dispositions légales applicables.

7. Protection des intérêts de l'Organisation

Toutes les mesures nécessaires sont prises afin d'assurer la restitution des biens, documents, équipements, supports numériques, identifiants, badges, moyens d'accès et informations appartenant à l'Organisation.

8. Documentation

La procédure d'exclusion est intégralement documentée afin d'assurer la traçabilité des décisions, la conservation des preuves et le respect des obligations de gouvernance.

9. Recours

La personne concernée peut exercer les voies de recours prévues par les statuts, les règlements internes ou les dispositions légales applicables.

10. Amélioration continue

Les enseignements issus des procédures d'exclusion contribuent au renforcement des dispositifs de gouvernance, de prévention, de contrôle interne et de conformité.

Par cette politique, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que toute mesure d'exclusion demeure exceptionnelle, objectivement justifiée, juridiquement sécurisée et exclusivement motivée par la protection durable de ses missions, de ses ressources et de l'intérêt général.

8.94 Résiliation des relations

La **résiliation des relations** constitue une mesure institutionnelle permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de mettre fin, de manière anticipée ou à échéance, à toute relation contractuelle, partenariale, professionnelle, financière ou institutionnelle devenue incompatible avec ses exigences de gouvernance, de conformité, d'éthique, de sécurité ou de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT). Cette décision vise à préserver les intérêts de l'Organisation, à limiter les risques juridiques, financiers, opérationnels et réputationnels et à garantir le respect des engagements pris envers les parties prenantes.

1. Objet de la résiliation

Mettre un terme à toute relation susceptible de compromettre les intérêts, la conformité ou la réputation de l'Organisation.

2. Champ d'application

La résiliation peut concerner les conventions de partenariat, contrats de prestation, conventions de financement, adhésions, affiliations, protocoles d'accord, mandats, contrats de travail, conventions de bénévolat ou toute autre relation juridique.

3. Motifs

Elle peut être décidée notamment en cas de manquement grave, fraude, corruption, non-respect des obligations contractuelles, violation des règles LBC/FT, défaut de conformité, perte de confiance, conflit d'intérêts majeur ou atteinte à la réputation de l'Organisation.

4. Évaluation préalable

Avant toute décision, les faits sont analysés, documentés et évalués afin de déterminer la mesure la plus appropriée.

5. Respect des engagements contractuels

La résiliation est mise en œuvre dans le respect des clauses contractuelles, des obligations légales, des délais de préavis éventuellement applicables et des principes de bonne foi.

6. Notification

La décision est notifiée par écrit à la partie concernée en précisant les motifs, la date d'effet et les conséquences de la résiliation.

7. Mesures consécutives

L'Organisation procède, si nécessaire, à la clôture des accès, à la restitution des biens, à la récupération des documents, à la résiliation des habilitations et au règlement des obligations contractuelles restantes.

8. Archivage

L'ensemble de la procédure est documenté et conservé conformément aux règles institutionnelles de gestion documentaire.

9. Prévention des risques futurs

Les causes ayant conduit à la résiliation sont analysées afin de renforcer les procédures de sélection, de diligence raisonnable, de contractualisation et de suivi des partenaires.

10. Amélioration continue

Les retours d'expérience issus des résiliations permettent d'améliorer les politiques de conformité, de gouvernance et de gestion des partenariats.

Par cette politique, AGCE International garantit que toute résiliation de relation institutionnelle est prise de manière responsable, objective et proportionnée, dans le respect du droit applicable et de ses engagements éthiques.

8.95 Signalement aux autorités

Le **signalement aux autorités compétentes** constitue une obligation de conformité essentielle lorsque **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** identifie des faits susceptibles de constituer une infraction pénale, un acte de blanchiment de capitaux, un financement du terrorisme, une fraude grave, une corruption, une atteinte à la cybersécurité ou toute autre violation imposant une déclaration en vertu des lois et réglementations applicables. Cette démarche s'inscrit dans le respect des obligations nationales et internationales de coopération avec les autorités administratives, judiciaires, financières et de contrôle, tout en garantissant la protection des droits des personnes concernées, la confidentialité des informations et la préservation des preuves.

1. Objet du signalement

Le signalement vise à permettre aux autorités compétentes d'exercer leurs missions de contrôle, d'enquête, de poursuite et de prévention conformément aux textes en vigueur.

2. Situations concernées

Peuvent faire l'objet d'un signalement les opérations suspectes, les fraudes majeures, les actes de corruption, les détournements de fonds, les infractions financières, les cyberattaques graves, les violations importantes des réglementations LBC/FT ainsi que tout fait dont la déclaration est légalement obligatoire.

3. Respect du cadre juridique

Les signalements sont réalisés conformément aux lois nationales applicables, aux conventions internationales, aux exigences des autorités de supervision et aux obligations contractuelles de l'Organisation.

4. Autorités compétentes

Les déclarations sont adressées exclusivement aux autorités administratives, judiciaires, financières, de régulation ou de contrôle légalement habilitées à recevoir ce type d'information.

5. Qualité des informations transmises

Les informations communiquées doivent être exactes, complètes, objectives, documentées et limitées aux éléments strictement nécessaires au traitement du dossier.

6. Confidentialité

Les signalements sont effectués dans des conditions garantissant la confidentialité des informations, la protection des données personnelles et la sécurité des personnes concernées.

7. Coopération institutionnelle

L'Organisation coopère pleinement avec les autorités compétentes en mettant à leur disposition les documents, informations et éléments de preuve légalement communicables.

8. Traçabilité

Chaque signalement fait l'objet d'un enregistrement sécurisé précisant la date, l'autorité destinataire, la nature des faits signalés et les suites données.

9. Protection contre les représailles

Les personnes ayant effectué un signalement de bonne foi bénéficient de la protection prévue par les politiques institutionnelles relatives aux lanceurs d'alerte et aux exigences légales applicables.

10. Suivi et amélioration continue

Les retours d'expérience issus des signalements permettent de renforcer les dispositifs de conformité, de contrôle interne, de prévention des risques et de coopération avec les autorités compétentes.

Par cette politique de **signalement aux autorités**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** réaffirme son engagement à respecter pleinement ses obligations légales et réglementaires, à coopérer avec les autorités compétentes et à contribuer activement à la prévention du blanchiment de capitaux, du financement du terrorisme, de la fraude, de la corruption et de toute autre activité illicite, conformément aux plus hauts standards internationaux de gouvernance, de transparence et d'intégrité.

8.96 Procédure contradictoire

La **procédure contradictoire** constitue une garantie fondamentale du dispositif disciplinaire de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle assure que toute personne susceptible de faire l'objet d'une mesure disciplinaire bénéficie d'un traitement équitable, impartial et transparent, conforme aux principes de bonne gouvernance, aux droits de la défense et aux exigences des législations applicables. Dans le cadre de la lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT), cette procédure permet de concilier la protection des intérêts de l'Organisation avec le respect des droits individuels. Aucune décision disciplinaire ne peut être prise sans que la personne concernée ait été informée des faits qui lui sont reprochés et ait disposé d'une possibilité réelle de présenter ses observations, sous réserve des mesures conservatoires rendues nécessaires par l'urgence ou la protection des intérêts essentiels de l'Organisation.

1. Objet de la procédure contradictoire

La procédure contradictoire garantit le respect des droits de la défense avant toute décision disciplinaire susceptible d'affecter les droits, les fonctions, les responsabilités ou les relations institutionnelles d'une personne.

2. Champ d'application

Elle s'applique à toute procédure pouvant conduire à un avertissement, une suspension, une exclusion, une résiliation de relation institutionnelle ou toute autre mesure disciplinaire prévue par les textes internes de l'Organisation.

3. Information préalable

La personne concernée est informée, dans un délai raisonnable, des faits qui lui sont reprochés, des dispositions prétendument violées, des éléments connus à ce stade de l'enquête ainsi que de la procédure applicable.

4. Communication des éléments utiles

Sous réserve des exigences de confidentialité, de sécurité ou des obligations légales, la personne concernée peut prendre connaissance des éléments essentiels servant de fondement à la procédure afin de préparer utilement sa défense.

5. Droit de présenter ses observations

La personne mise en cause dispose de la possibilité de présenter des explications écrites ou orales, de fournir tout document utile, de produire des justificatifs ou de faire valoir tout élément susceptible d'éclairer la décision.

6. Examen impartial du dossier

Les observations recueillies sont examinées avec objectivité par les autorités compétentes, qui tiennent compte aussi bien des éléments à charge que des éléments à décharge avant toute décision.

7. Respect de la confidentialité

L'ensemble de la procédure est conduit dans le respect de la confidentialité, de la protection des données personnelles, de la présomption de bonne foi et de la dignité des personnes concernées.

8. Motivation de la décision

Toute décision disciplinaire est motivée de manière claire et précise, en indiquant les faits retenus, les règles applicables, les éléments ayant conduit à la décision ainsi que les conséquences qui en découlent.

9. Traçabilité de la procédure

Toutes les étapes de la procédure contradictoire sont consignées dans un dossier sécurisé comprenant les notifications, observations, pièces produites, comptes rendus, analyses et décisions finales.

10. Contribution à la bonne gouvernance

Le respect du contradictoire renforce la légitimité des décisions disciplinaires, limite les risques de contestation et contribue au développement d'une culture institutionnelle fondée sur l'équité, la transparence et la responsabilité.

Par cette procédure contradictoire, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme son engagement à concilier l'efficacité de son dispositif disciplinaire avec le respect des droits fondamentaux des personnes concernées. Cette approche garantit des décisions objectives, proportionnées et juridiquement sécurisées, conformes aux meilleures pratiques nationales et internationales en matière de gouvernance, de conformité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

8.97 Voies de recours

Les **voies de recours** constituent une garantie essentielle du dispositif disciplinaire de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elles permettent à toute personne faisant l'objet d'une décision disciplinaire de solliciter le réexamen de cette décision lorsqu'elle estime que celle-ci est entachée d'une erreur de fait, d'une erreur de droit, d'une irrégularité procédurale, d'une disproportion de la sanction ou de tout autre élément susceptible d'en affecter la légalité ou l'équité. Ce mécanisme participe au renforcement de la transparence, de la responsabilité, de la confiance institutionnelle et de l'amélioration continue des pratiques de gouvernance.

1. Objet des voies de recours

Les voies de recours permettent d'assurer un contrôle des décisions disciplinaires et de garantir leur conformité aux principes de légalité, d'impartialité, de proportionnalité et de bonne gouvernance.

2. Bénéficiaires

Toute personne physique ou morale concernée par une décision disciplinaire prise par l'Organisation peut exercer les recours prévus par les statuts, les règlements internes, les conventions applicables ou les dispositions légales en vigueur.

3. Droit de contester une décision

La personne concernée peut demander le réexamen d'une décision lorsqu'elle estime que les faits retenus sont inexacts, que la procédure n'a pas été respectée ou que la sanction apparaît inadaptée au regard des circonstances.

4. Dépôt du recours

Le recours est présenté selon les modalités définies par les procédures internes de l'Organisation. Il expose les motifs de la contestation et peut être accompagné de toute pièce ou information complémentaire jugée utile.

5. Examen du recours

Le recours est instruit par l'autorité ou l'instance compétente, indépendante de la décision initiale lorsque l'organisation de la gouvernance le permet, afin de garantir l'objectivité du réexamen.

6. Réévaluation du dossier

L'autorité compétente procède à une nouvelle analyse des faits, des preuves, des arguments présentés et de la conformité de la procédure ayant conduit à la décision contestée.

7. Décision sur le recours

À l'issue du réexamen, la décision initiale peut être confirmée, modifiée, partiellement réformée ou annulée, selon les éléments recueillis et les règles applicables.

8. Notification

La décision rendue à l'issue du recours est notifiée à la personne concernée dans des conditions garantissant la confidentialité et la traçabilité des échanges.

9. Conservation des dossiers

L'ensemble des documents relatifs aux recours est archivé conformément aux politiques institutionnelles de gestion documentaire, de protection des données et de conservation des preuves.

10. Amélioration continue

Les enseignements tirés des recours sont exploités afin d'améliorer les procédures disciplinaires, de renforcer les garanties offertes aux parties concernées, d'harmoniser les pratiques décisionnelles et de prévenir la récurrence des difficultés procédurales.

11. Respect des droits et des législations applicables

L'exercice d'une voie de recours ne prive pas la personne concernée des droits ou actions qui pourraient lui être reconnus par les juridictions compétentes ou par les autorités administratives, conformément aux lois applicables dans les pays où intervient l'Organisation.

Par cette politique relative aux **voies de recours**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que toute décision disciplinaire peut être réexaminée dans un cadre impartial, transparent et respectueux des droits des personnes concernées. Ce mécanisme contribue à renforcer la qualité des décisions, la confiance des membres, partenaires, donateurs et bénéficiaires, ainsi que la crédibilité du système de gouvernance et de conformité de l'Organisation, conformément aux meilleures pratiques internationales en matière d'éthique, de responsabilité et de justice organisationnelle.

SECTION XI

RÉVISION DE LA POLITIQUE

8.98 Principes

La **révision de la présente Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** constitue un processus permanent de gouvernance, de conformité et d'amélioration continue mis en œuvre par **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Compte tenu de l'évolution constante des risques financiers, des innovations technologiques, des nouvelles méthodes de criminalité économique, des exigences des autorités de régulation et des attentes des partenaires institutionnels et bailleurs de fonds, la présente politique ne peut demeurer figée. Elle fait donc l'objet d'une évaluation régulière afin de garantir son adéquation avec les réalités opérationnelles de l'Organisation, les meilleures pratiques internationales ainsi que les dispositions légales et réglementaires applicables dans les différents pays où AGCE International exerce ses activités. Cette démarche traduit la volonté de l'Organisation d'inscrire la conformité dans une logique d'amélioration permanente, de maîtrise des risques et de renforcement de sa gouvernance institutionnelle.

1. Objet de la révision

La révision de la politique a pour objet d'assurer l'actualisation permanente des dispositions relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme, afin de maintenir un dispositif de conformité efficace, pertinent et adapté aux évolutions juridiques, opérationnelles et technologiques.

2. Principe d'amélioration continue

La présente politique est fondée sur une démarche d'amélioration continue visant à renforcer progressivement les mécanismes de prévention, de détection, de contrôle, de surveillance, de signalement et de gestion des risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption et de criminalité financière.

3. Adaptation aux évolutions réglementaires

Toute évolution des lois nationales, des réglementations internationales, des recommandations des organismes de supervision, des normes professionnelles ou des obligations imposées aux organisations à but non lucratif peut conduire à une révision partielle ou complète de la présente politique.

4. Prise en compte de l'évolution des risques

Les révisions tiennent compte des nouveaux risques identifiés à travers les évaluations internes, les analyses sectorielles, les audits, les incidents, les signalements, les retours d'expérience ainsi que les nouvelles formes de criminalité financière ou numérique susceptibles d'affecter les activités de l'Organisation.

5. Participation des parties prenantes

Les responsables de la gouvernance, de la conformité, du contrôle interne, des finances, des ressources humaines, des systèmes d'information, des antennes nationales et internationales ainsi que toute personne concernée peuvent être associés au processus de révision afin de garantir une approche collaborative, réaliste et adaptée aux besoins opérationnels.

6. Analyse des retours d'expérience

Les constats issus des audits internes et externes, des inspections, des auto-évaluations, des recommandations formulées par les autorités compétentes, des partenaires techniques et financiers ainsi que les enseignements tirés des incidents et des procédures disciplinaires sont intégrés au processus de révision afin de renforcer l'efficacité du dispositif institutionnel.

7. Validation institutionnelle

Toute modification substantielle de la présente politique est examinée et validée par les instances compétentes de gouvernance de l'Organisation conformément aux statuts, aux règlements internes et aux délégations de pouvoir en vigueur, avant son entrée en application.

8. Communication des modifications

Les nouvelles versions de la politique, ainsi que les modifications importantes apportées au dispositif LBC/FT, sont communiquées aux administrateurs, membres, salariés, bénévoles, partenaires, prestataires et autres parties concernées afin d'assurer leur bonne compréhension et leur application effective.

9. Traçabilité et conservation

Chaque révision fait l'objet d'une documentation complète précisant la version concernée, les modifications apportées, les motifs de leur adoption, la date d'entrée en vigueur, les autorités ayant procédé à leur validation ainsi que les modalités de diffusion. Cette documentation est

conservée conformément aux règles institutionnelles de gestion documentaire et de protection des données.

10. Engagement institutionnel

La révision régulière de cette politique traduit l'engagement permanent de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** à maintenir un système de conformité robuste, évolutif et conforme aux meilleures pratiques internationales en matière de gouvernance, de transparence, de gestion des risques et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

En adoptant ces **principes de révision de la politique**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme sa volonté de faire de la conformité un processus dynamique et évolutif, capable de répondre aux exigences croissantes des autorités de régulation, des bailleurs de fonds, des partenaires institutionnels et des bénéficiaires. Cette approche garantit la pérennité, la crédibilité et l'efficacité du dispositif LBC/FT de l'Organisation, tout en renforçant durablement sa culture d'intégrité, de responsabilité, de transparence et de bonne gouvernance.

8.99 Périodicité

La **périodicité de révision** de la présente **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** constitue un mécanisme essentiel permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de maintenir un dispositif de conformité performant, actualisé et adapté à l'évolution de son environnement juridique, institutionnel, financier et technologique. Compte tenu de la nature évolutive des risques liés au blanchiment de capitaux, au financement du terrorisme, à la fraude, à la corruption, aux cybermenaces et aux exigences des bailleurs de fonds, autorités de contrôle et partenaires internationaux, l'Organisation s'engage à procéder à une révision régulière de la présente politique. Cette démarche garantit que les procédures, les contrôles internes, les mesures de vigilance et les mécanismes de gouvernance demeurent conformes aux meilleures pratiques nationales et internationales ainsi qu'aux réalités opérationnelles de l'Organisation.

1. Principe de révision périodique

La présente politique fait l'objet d'une révision programmée selon une fréquence définie par les instances de gouvernance afin de garantir son actualisation continue.

2. Révision annuelle

Sauf nécessité particulière, une révision complète est réalisée au moins une fois par an afin de vérifier la pertinence, la cohérence et l'efficacité des dispositions de la politique.

3. Évaluation intermédiaire

Entre deux révisions générales, des évaluations périodiques peuvent être organisées afin d'apprécier le fonctionnement du dispositif LBC/FT et d'identifier les éventuels besoins d'ajustement.

4. Intégration des évolutions réglementaires

La périodicité tient compte des évolutions législatives, réglementaires et normatives susceptibles d'affecter les obligations de conformité de l'Organisation.

5. Analyse des risques

Les résultats des cartographies des risques, des évaluations internes et des dispositifs de surveillance alimentent chaque cycle de révision.

6. Exploitation des audits

Les constats formulés lors des audits internes, audits externes, inspections, missions de contrôle et évaluations indépendantes sont systématiquement intégrés dans le processus de révision.

7. Prise en compte des retours d'expérience

Les incidents, non-conformités, recommandations, procédures disciplinaires et retours opérationnels constituent des sources permanentes d'amélioration de la politique.

8. Communication des échéances

Le calendrier des révisions est communiqué aux responsables concernés afin d'assurer une préparation efficace des travaux et une participation coordonnée des différentes structures.

9. Documentation

Chaque révision programmée fait l'objet d'une documentation retraçant les analyses réalisées, les modifications adoptées, les validations obtenues et les dates d'entrée en vigueur.

10. Objectif de pérennité

La périodicité de révision garantit que la politique demeure un document vivant, évolutif et pleinement adapté aux missions humanitaires, sociales, économiques et numériques d'AGCE International.

Par cette organisation périodique des révisions, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** assure le maintien d'un dispositif de conformité robuste, dynamique et conforme aux exigences des autorités

nationales, des organismes internationaux, des partenaires techniques et financiers ainsi que des meilleures pratiques de gouvernance.

8.100 Déclenchement d'une révision exceptionnelle

En complément des révisions périodiques, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** peut engager une **révision exceptionnelle** de la présente politique lorsqu'un événement majeur, un changement significatif ou un risque nouveau rend nécessaire une adaptation immédiate du dispositif LBC/FT. Cette procédure exceptionnelle permet à l'Organisation de réagir rapidement aux évolutions susceptibles d'affecter la sécurité de ses opérations, la conformité réglementaire ou la protection de ses ressources.

1. Objet de la révision exceptionnelle

Permettre une adaptation immédiate de la politique lorsqu'un changement majeur affecte son efficacité ou sa conformité.

2. Modification de la réglementation

Toute évolution importante des lois, règlements, recommandations internationales ou exigences des autorités compétentes peut justifier une révision exceptionnelle.

3. Apparition de nouveaux risques

La découverte de nouvelles typologies de blanchiment, de financement du terrorisme, de fraude, de cybercriminalité ou de corruption peut entraîner une révision anticipée.

4. Incident majeur

Une fraude importante, une cyberattaque, une violation de données, un détournement de fonds ou tout incident critique peut conduire à une actualisation immédiate des procédures.

5. Recommandations d'audit

Les conclusions d'un audit interne, externe ou d'une inspection officielle mettant en évidence des insuffisances importantes peuvent justifier une révision exceptionnelle.

6. Exigences des partenaires

Les recommandations formulées par les bailleurs de fonds, institutions financières, partenaires internationaux ou organismes de certification peuvent également déclencher une mise à jour.

7. Décision des organes de gouvernance

Les instances dirigeantes peuvent décider d'engager une révision exceptionnelle lorsqu'elles estiment que les intérêts de l'Organisation l'exigent.

8. Analyse préalable

Toute révision exceptionnelle est précédée d'une analyse documentée des risques, des impacts et des modifications envisagées.

9. Validation accélérée

Lorsque l'urgence le justifie, les procédures de validation peuvent être adaptées afin de permettre une entrée en vigueur rapide des nouvelles dispositions, tout en respectant les règles de gouvernance.

10. Information des parties concernées

Les modifications issues d'une révision exceptionnelle sont communiquées sans délai aux personnes concernées afin de garantir leur application immédiate.

Par cette faculté de révision exceptionnelle, AGCE International renforce sa capacité d'adaptation face aux évolutions rapides de son environnement réglementaire, technologique et opérationnel, tout en assurant la continuité de son dispositif de conformité.

8.101 Processus de révision

Le **processus de révision** de la présente politique est organisé selon une méthodologie structurée garantissant la qualité, la cohérence, la traçabilité et la légitimité des modifications apportées. Il mobilise les différentes instances de gouvernance, les responsables opérationnels, les fonctions de conformité et de contrôle interne, ainsi que les autres parties prenantes concernées, afin d'assurer une révision fondée sur une analyse rigoureuse des risques et des besoins institutionnels.

1. Planification

Le processus débute par la programmation des travaux de révision selon le calendrier établi ou à la suite d'une décision exceptionnelle.

2. Collecte des informations

Les données provenant des audits, contrôles, évaluations des risques, incidents, recommandations, évolutions réglementaires et retours d'expérience sont recueillies et analysées.

3. Analyse des besoins

Les responsables compétents identifient les dispositions nécessitant une mise à jour, une clarification, un renforcement ou une suppression.

4. Élaboration des modifications

Les propositions de révision sont rédigées de manière cohérente avec les autres politiques, procédures et référentiels institutionnels.

5. Concertation

Les projets de modification peuvent être soumis aux responsables concernés afin de recueillir leurs observations et de favoriser une approche collaborative.

6. Validation institutionnelle

Les modifications sont examinées et approuvées par les organes compétents conformément aux statuts, aux règlements internes et aux délégations de pouvoir.

7. Diffusion

La nouvelle version est officiellement diffusée auprès des administrateurs, membres, salariés, bénévoles, partenaires, prestataires et autres parties concernées.

8. Formation et sensibilisation

Lorsque les modifications apportées sont significatives, des actions de communication, de sensibilisation ou de formation sont organisées afin de faciliter leur compréhension et leur application.

9. Archivage des versions

Toutes les versions successives de la politique sont conservées dans un système documentaire sécurisé garantissant la traçabilité des évolutions, des validations et des dates d'application.

10. Suivi de l'application

Après son entrée en vigueur, la nouvelle version fait l'objet d'un suivi permettant d'évaluer son efficacité, son niveau d'application et les éventuels ajustements à prévoir lors des prochaines révisions.

Par ce **processus structuré de révision**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que sa Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme demeure

un référentiel institutionnel fiable, évolutif et conforme aux exigences nationales et internationales. Ce processus contribue à renforcer durablement la gouvernance, la maîtrise des risques, la transparence, la conformité réglementaire et la confiance des membres, partenaires, donateurs, bénéficiaires et autorités de contrôle.

8.102 Validation institutionnelle

La **validation institutionnelle** constitue l'étape officielle par laquelle la présente **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** acquiert son caractère exécutoire au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle garantit que toute nouvelle politique, toute modification, mise à jour ou révision a fait l'objet d'un examen approfondi, d'une concertation appropriée et d'une approbation par les instances de gouvernance compétentes. Cette validation assure la cohérence de la politique avec les statuts de l'Organisation, les règlements intérieurs, les autres politiques institutionnelles, les obligations légales nationales et internationales ainsi que les engagements pris envers les partenaires techniques, financiers et institutionnels. Elle constitue une garantie essentielle de transparence, de responsabilité et de sécurité juridique.

1. Objet de la validation institutionnelle

La validation institutionnelle a pour finalité de confirmer officiellement que la politique répond aux exigences de gouvernance, de conformité, de gestion des risques et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

2. Examen préalable

Avant toute approbation, le projet de politique ou de révision est soumis à une analyse juridique, opérationnelle, technique et organisationnelle afin d'en vérifier la cohérence, la faisabilité et la conformité.

3. Participation des parties compétentes

Les responsables de la gouvernance, de la conformité, du contrôle interne, des finances, des systèmes d'information, des ressources humaines et des autres services concernés peuvent être consultés afin d'émettre leurs observations et recommandations.

4. Vérification de la conformité

La politique est examinée afin de s'assurer de sa conformité avec les lois applicables, les recommandations internationales, les obligations réglementaires, les exigences des bailleurs de fonds ainsi que les autres référentiels internes de l'Organisation.

5. Approbation par les instances compétentes

La validation est prononcée par les organes de gouvernance habilités conformément aux statuts, aux règlements intérieurs et aux délégations de pouvoir en vigueur au sein d'AGCE International – AGCE Canada.

6. Formalisation de la décision

Toute validation donne lieu à une décision officielle précisant la version adoptée, la date d'approbation, la date d'entrée en vigueur, les autorités signataires et les éventuelles dispositions transitoires.

7. Entrée en vigueur

La politique ou sa version révisée devient applicable à compter de la date fixée par la décision de validation, sauf disposition particulière expressément prévue.

8. Valeur institutionnelle

Une fois validée, la politique devient un document de référence obligatoire pour l'ensemble des administrateurs, dirigeants, membres, salariés, bénévoles, consultants, partenaires et prestataires concernés.

9. Conservation des actes de validation

Les procès-verbaux, résolutions, décisions, comptes rendus et documents justificatifs relatifs à la validation sont archivés dans les systèmes documentaires sécurisés de l'Organisation.

10. Garantie de gouvernance

La validation institutionnelle contribue à renforcer la légitimité des décisions, la sécurité juridique des procédures, la transparence de la gouvernance et la confiance des partenaires nationaux et internationaux.

Par cette procédure de validation institutionnelle, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que sa Politique LBC/FT repose sur une gouvernance rigoureuse, une décision collégiale et un engagement permanent en faveur de la conformité, de la transparence et de l'amélioration continue.

8.103 Historique des versions

L'**historique des versions** constitue un outil essentiel de gouvernance documentaire permettant d'assurer la traçabilité de l'ensemble des évolutions apportées à la présente **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme**

(LBC/FT). Il permet à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de conserver la mémoire institutionnelle des modifications successives, d'identifier les raisons ayant motivé chaque mise à jour et de démontrer, en cas d'audit ou de contrôle, la maîtrise de son système documentaire.

1. Objet de l'historique

Conserver un enregistrement chronologique de toutes les versions de la politique depuis sa création jusqu'à ses révisions successives.

2. Identification des versions

Chaque version reçoit un numéro unique, une référence documentaire, une date d'approbation et une date d'entrée en vigueur.

3. Description des modifications

Les changements significatifs apportés à chaque version sont clairement décrits afin d'en faciliter la compréhension et le suivi.

4. Justification des évolutions

Les motifs ayant conduit à chaque révision sont documentés, notamment les évolutions réglementaires, les recommandations d'audit, les nouveaux risques ou les décisions institutionnelles.

5. Identification des autorités

L'historique précise les organes ou responsables ayant validé chaque version de la politique.

6. Conservation des versions antérieures

Les anciennes versions sont archivées de manière sécurisée afin de préserver la continuité documentaire et de répondre aux besoins de contrôle ou d'audit.

7. Gestion documentaire

L'historique est intégré au système officiel de gestion documentaire de l'Organisation afin de garantir son authenticité, son intégrité et sa disponibilité.

8. Traçabilité

Toute modification est enregistrée avec sa date, son auteur, son validateur et les documents justificatifs correspondants.

9. Consultation

L'accès à l'historique est réservé aux personnes autorisées, dans le respect des règles de confidentialité et de protection des informations institutionnelles.

10. Contribution à l'amélioration continue

L'analyse des différentes versions permet d'évaluer la maturité du dispositif de conformité et d'orienter les futures évolutions de la politique.

Par la tenue d'un historique des versions complet et rigoureux, **AGCE International – AGCE Canada** renforce la transparence de sa gouvernance documentaire, facilite les audits internes et externes et démontre son engagement permanent en faveur de la conformité et de la qualité institutionnelle.

8.104 Diffusion

La **diffusion** de la présente **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** a pour objectif d'assurer que toutes les personnes concernées disposent d'une information complète, fiable et actualisée sur les règles applicables au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Une politique, aussi rigoureuse soit-elle, ne peut produire pleinement ses effets que si elle est connue, comprise, accessible et effectivement appliquée. L'Organisation met ainsi en œuvre un dispositif structuré de diffusion garantissant la communication de la politique à l'ensemble de ses parties prenantes, tout en assurant la maîtrise des versions, la confidentialité des informations sensibles et la traçabilité des transmissions.

1. Objet de la diffusion

Assurer la communication officielle de la politique à toutes les personnes concernées afin de garantir son application uniforme.

2. Public concerné

La politique est diffusée aux administrateurs, dirigeants, membres, salariés, bénévoles, consultants, partenaires, prestataires, représentants des antennes nationales et internationales ainsi qu'à toute personne concernée par son application.

3. Supports de diffusion

La diffusion peut être réalisée au moyen des plateformes numériques institutionnelles, de l'intranet, de l'espace documentaire sécurisé, des courriers électroniques, des réunions de gouvernance, des sessions de formation ou de tout autre support officiel.

4. Version officielle

Une seule version officiellement validée est reconnue comme faisant foi. Toute diffusion doit s'appuyer sur cette version afin d'éviter les incohérences documentaires.

5. Communication des mises à jour

Chaque modification importante est accompagnée d'une information précisant les changements apportés, leur date d'entrée en vigueur et les conséquences pratiques pour les utilisateurs.

6. Accessibilité

La politique est mise à disposition dans un format permettant sa consultation, sa compréhension et son utilisation par les personnes habilitées.

7. Sensibilisation

Des actions d'information, de formation et de sensibilisation accompagnent la diffusion afin de favoriser l'appropriation des nouvelles dispositions.

8. Traçabilité de la diffusion

Les opérations de diffusion sont enregistrées afin de pouvoir démontrer que les personnes concernées ont été informées des versions applicables.

9. Protection documentaire

Les modalités de diffusion tiennent compte des exigences de confidentialité, de cybersécurité, de protection des données et de gestion des droits d'accès.

10. Évaluation de l'efficacité

L'Organisation évalue régulièrement l'efficacité de la diffusion de la politique au moyen d'actions de contrôle, d'enquêtes de compréhension, d'audits internes et de retours d'expérience afin d'améliorer continuellement la communication institutionnelle.

Par cette politique de diffusion, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** veille à ce que chaque version de sa Politique LBC/FT soit portée à la connaissance des parties prenantes concernées dans des conditions garantissant la sécurité, la traçabilité, l'accessibilité et l'application homogène de ses exigences, renforçant ainsi durablement la culture de conformité, de transparence et de bonne gouvernance au sein de l'Organisation.

8.105 Entrée en vigueur

L'entrée en vigueur de la présente **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** marque le moment à partir duquel l'ensemble de ses dispositions deviennent officiellement applicables au sein de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Cette étape consacre l'aboutissement du processus de rédaction, d'analyse, de validation et de diffusion de la politique, tout en garantissant la sécurité juridique, l'uniformité d'application et la bonne information de l'ensemble des parties prenantes. Dès son entrée en vigueur, cette politique constitue un référentiel institutionnel obligatoire auquel doivent se conformer les administrateurs, dirigeants, membres, salariés, bénévoles, consultants, prestataires, partenaires, représentants des antennes nationales et internationales ainsi que toute personne agissant pour le compte de l'Organisation. L'entrée en vigueur s'inscrit dans une démarche de gouvernance responsable visant à assurer une application cohérente, progressive et contrôlée des exigences de conformité.

1. Objet de l'entrée en vigueur

L'entrée en vigueur a pour objet de rendre la présente politique pleinement applicable et opposable à l'ensemble des personnes concernées par son champ d'application.

2. Date d'application

La politique entre en vigueur à la date fixée dans la décision officielle de validation institutionnelle, sauf disposition particulière prévoyant un calendrier différent pour certaines mesures.

3. Caractère obligatoire

À compter de son entrée en vigueur, le respect des dispositions de la présente politique devient obligatoire pour toutes les personnes relevant de son champ d'application, conformément aux statuts, règlements et engagements contractuels de l'Organisation.

4. Abrogation des dispositions antérieures

L'entrée en vigueur entraîne, le cas échéant, l'abrogation, le remplacement ou la mise à jour des politiques, procédures, directives ou instructions antérieures devenues incompatibles avec la présente politique.

5. Information des parties concernées

Avant ou au moment de son entrée en vigueur, l'Organisation veille à informer les parties prenantes concernées des nouvelles dispositions, de leurs obligations et des éventuelles évolutions introduites.

6. Mise à disposition de la version officielle

La version officiellement approuvée est diffusée par les canaux institutionnels appropriés afin de garantir son accessibilité, son authenticité et son utilisation uniforme.

7. Mesures d'accompagnement

Lorsque les modifications apportées sont substantielles, des actions de sensibilisation, de formation, d'assistance ou de communication peuvent être organisées afin de faciliter leur mise en œuvre effective.

8. Coordination de la mise en œuvre

Les responsables de la gouvernance, de la conformité, du contrôle interne et des différentes structures opérationnelles veillent à la bonne application des nouvelles dispositions dès leur entrée en vigueur.

9. Traçabilité

La date d'entrée en vigueur, les actes de validation, les modalités de diffusion et les mesures d'accompagnement sont documentés et archivés conformément aux procédures institutionnelles de gestion documentaire.

10. Engagement institutionnel

L'entrée en vigueur de la présente politique traduit l'engagement officiel d'AGCE International – AGCE Canada à appliquer un dispositif moderne, cohérent et conforme aux meilleures pratiques en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme, la gouvernance, la transparence et la gestion des risques.

Par cette procédure d'entrée en vigueur, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** garantit que la présente Politique LBC/FT devient un cadre de référence pleinement opérationnel, contribuant à renforcer durablement la conformité réglementaire, la protection des ressources institutionnelles, la confiance des partenaires et la qualité de sa gouvernance.

8.106 Suivi de l'application

Le suivi de l'application de la présente **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** constitue un mécanisme permanent destiné à vérifier que les dispositions adoptées sont effectivement mises en œuvre, comprises et respectées par l'ensemble des personnes concernées. Pour **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**, la conformité ne se limite pas à l'adoption d'un document institutionnel ; elle repose également sur un contrôle continu de son application, l'identification des difficultés rencontrées, la mesure

de son efficacité et la mise en œuvre d'actions correctives lorsque cela s'avère nécessaire. Ce suivi contribue à renforcer la culture de conformité, à améliorer la maîtrise des risques et à garantir l'adaptation permanente du dispositif LBC/FT aux réalités opérationnelles de l'Organisation.

1. Objet du suivi

Le suivi vise à contrôler l'application effective des dispositions de la politique et à mesurer leur niveau de conformité au sein de l'Organisation.

2. Responsabilités

Les responsables de la conformité, du contrôle interne, de la gouvernance, des finances, des ressources humaines, des systèmes d'information et des différentes structures opérationnelles participent au suivi selon leurs compétences respectives.

3. Contrôles réguliers

Des contrôles périodiques sont organisés afin de vérifier le respect des procédures, l'application des mesures de vigilance, des obligations déclaratives et des dispositifs de prévention des risques.

4. Évaluation de l'efficacité

Le fonctionnement de la politique est évalué au regard d'indicateurs de performance, des résultats des audits, des inspections, des auto-évaluations, des incidents déclarés et des recommandations formulées.

5. Identification des écarts

Tout manquement, difficulté d'application, insuffisance de procédure ou risque émergent identifié au cours du suivi fait l'objet d'une analyse et d'un traitement approprié.

6. Mise en œuvre des actions correctives

Lorsque des non-conformités sont constatées, des mesures correctives, préventives ou organisationnelles sont définies, mises en œuvre et suivies jusqu'à leur complète réalisation.

7. Reporting institutionnel

Des rapports périodiques sont élaborés afin d'informer les instances de gouvernance sur le niveau d'application de la politique, les résultats obtenus, les difficultés rencontrées et les améliorations proposées.

8. Sensibilisation continue

Les résultats du suivi peuvent conduire à renforcer les actions de communication, de formation et d'accompagnement destinées à améliorer la compréhension et l'application des exigences de la politique.

9. Documentation et traçabilité

Toutes les activités de suivi, les contrôles réalisés, les constats, les actions correctives et les décisions prises sont documentés, archivés et conservés conformément aux règles de gestion documentaire de l'Organisation.

10. Amélioration continue

Les enseignements issus du suivi alimentent les processus de révision de la politique, d'actualisation des procédures, de renforcement des contrôles internes et d'amélioration globale du dispositif de conformité.

11. Garantie de conformité durable

Le suivi permanent permet à l'Organisation de maintenir un haut niveau de conformité réglementaire, d'anticiper les évolutions des risques, de répondre efficacement aux attentes des autorités compétentes et des partenaires institutionnels, et de préserver la crédibilité ainsi que la réputation d'AGCE International – AGCE Canada.

Par ce dispositif de **suivi de l'application**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme sa volonté de faire de la conformité un processus permanent, dynamique et mesurable. Cette démarche garantit que la présente Politique LBC/FT demeure effectivement appliquée dans toutes les composantes de l'Organisation, tout en favorisant une amélioration continue de la gouvernance, de la transparence, de la maîtrise des risques et de la protection des intérêts institutionnels.

ANNEXES

ANNEXE A

Glossaire LBC/FT

Le présent **Glossaire de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour objectif d'harmoniser la compréhension des principaux termes techniques, juridiques, financiers, opérationnels et institutionnels employés dans la présente politique ainsi que dans les procédures qui en découlent. L'utilisation d'une terminologie commune contribue à renforcer la cohérence des pratiques, la qualité des contrôles internes, la conformité réglementaire et l'efficacité des dispositifs de prévention des risques. Ce glossaire constitue un outil de référence destiné aux administrateurs, dirigeants, membres, salariés, bénévoles, partenaires, consultants, prestataires, auditeurs ainsi qu'à toute personne participant à la gouvernance ou aux activités de l'Organisation. Les définitions présentées ci-après doivent être interprétées conformément aux législations applicables, aux normes internationales ainsi qu'aux politiques institutionnelles d'AGCE International – AGCE Canada.

1. LBC (Lutte contre le blanchiment de capitaux)

Ensemble des mesures légales, réglementaires, organisationnelles et opérationnelles destinées à prévenir, détecter, signaler et empêcher l'utilisation de ressources financières provenant d'activités illicites ou criminelles.

2. FT (Financement du terrorisme)

Fourniture, collecte, gestion, transfert ou utilisation directe ou indirecte de ressources financières, matérielles ou numériques destinées à soutenir des activités terroristes ou des organisations impliquées dans le terrorisme, en violation des lois applicables.

3. Blanchiment de capitaux

Processus consistant à dissimuler l'origine illicite de fonds ou de biens afin de leur donner une apparence de légalité par l'intermédiaire de diverses opérations financières, commerciales ou patrimoniales.

4. Bénéficiaire effectif

Personne physique qui possède, contrôle ou bénéficie en dernier ressort d'une organisation, d'une opération financière, d'un compte, d'un contrat ou d'une relation d'affaires, même si elle n'apparaît pas officiellement comme titulaire.

5. KYC (Know Your Customer / Connaissance du client ou du partenaire)

Ensemble des procédures permettant d'identifier, de vérifier et de connaître les personnes physiques ou morales avec lesquelles l'Organisation établit une relation institutionnelle, financière ou contractuelle.

6. Diligence raisonnable (Due Diligence)

Processus d'évaluation préalable consistant à recueillir, vérifier et analyser les informations nécessaires afin d'apprécier le niveau de risque présenté par une personne, une organisation, un projet, un partenaire ou une transaction.

7. Évaluation des risques

Méthode permettant d'identifier, d'analyser, de hiérarchiser et de traiter les risques susceptibles d'affecter les activités, les ressources, la conformité ou la réputation de l'Organisation.

8. Opération suspecte

Toute transaction, activité ou comportement présentant des caractéristiques inhabituelles, incohérentes ou susceptibles de révéler une tentative de blanchiment de capitaux, de financement du terrorisme, de fraude ou de toute autre activité illicite.

9. Personne Politiquement Exposée (PPE)

Personne exerçant ou ayant exercé d'importantes fonctions publiques nationales, étrangères ou internationales, ainsi que les membres de sa famille et les personnes qui lui sont étroitement associées, lorsque la réglementation applicable prévoit leur prise en compte dans l'évaluation des risques.

10. Déclaration de soupçon

Communication effectuée auprès de l'autorité légalement compétente lorsqu'une opération ou un comportement présente des indices sérieux pouvant être liés au blanchiment de capitaux, au financement du terrorisme ou à une autre infraction financière, conformément aux obligations prévues par la législation applicable.

11. Contrôle interne

Ensemble des politiques, procédures, contrôles, responsabilités et mécanismes mis en œuvre afin d'assurer la conformité, la maîtrise des risques, la protection des ressources et l'efficacité des activités de l'Organisation.

12. Conformité (Compliance)

Dispositif permettant de garantir que les activités de l'Organisation sont réalisées conformément aux lois, règlements, politiques internes, engagements contractuels et principes éthiques applicables.

13. Audit

Examen méthodique, indépendant et documenté destiné à évaluer la conformité, l'efficacité et la performance des dispositifs de gouvernance, de contrôle interne et de gestion des risques.

14. Non-conformité

Tout écart constaté entre une exigence légale, réglementaire, contractuelle ou institutionnelle et les pratiques effectivement mises en œuvre au sein de l'Organisation.

15. Gel des avoirs

Mesure légale ou réglementaire consistant à empêcher temporairement la disposition, le transfert, la conversion ou l'utilisation de fonds, d'actifs ou d'autres ressources financières, lorsqu'une telle mesure est imposée par une autorité compétente ou requise par la réglementation applicable.

16. Traçabilité

Capacité à reconstituer de manière fiable l'ensemble des opérations, décisions, contrôles et actions réalisées grâce à une documentation complète, sécurisée et chronologique.

17. Gouvernance

Ensemble des structures, règles, responsabilités, processus décisionnels et mécanismes de contrôle assurant la direction, la supervision et le fonctionnement responsable de l'Organisation.

18. Partie prenante

Toute personne physique ou morale ayant un intérêt direct ou indirect dans les activités de l'Organisation, notamment les membres, bénéficiaires, donateurs, partenaires, bailleurs de fonds, autorités publiques, prestataires et communautés concernées.

19. Gestion documentaire

Ensemble des méthodes permettant de créer, classer, conserver, protéger, archiver et détruire les documents institutionnels conformément aux exigences légales et organisationnelles.

20. Amélioration continue

Démarche permanente consistant à renforcer progressivement les politiques, procédures, contrôles, formations et mécanismes de gouvernance afin d'accroître leur efficacité, leur conformité et leur capacité d'adaptation.

Ce **Glossaire LBC/FT** constitue un référentiel terminologique officiel de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il favorise une interprétation uniforme des concepts utilisés dans la présente politique, facilite les activités de formation, d'audit et de contrôle, et contribue au développement d'une culture institutionnelle fondée sur la conformité, l'intégrité, la transparence, la gestion responsable des risques et le respect des meilleures pratiques nationales et internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

ANNEXE B

Cartographie des risques

La présente **Cartographie des risques de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif d'identifier, d'analyser, de hiérarchiser, d'évaluer et de maîtriser les risques susceptibles d'affecter les activités de l'Organisation, ses ressources financières, ses partenaires, ses bénéficiaires, ses systèmes d'information et sa réputation institutionnelle. La cartographie des risques constitue un outil stratégique d'aide à la décision permettant aux instances de gouvernance de définir les priorités de contrôle, d'allouer les ressources de manière appropriée et de renforcer les dispositifs de prévention, de détection et de traitement des risques. Elle est régulièrement actualisée afin de tenir compte des évolutions réglementaires, des changements organisationnels, des nouvelles menaces, des résultats des audits, des incidents déclarés et des recommandations des autorités compétentes. Cette démarche s'inscrit dans une logique d'amélioration continue, de gouvernance responsable et de conformité aux meilleures pratiques nationales et internationales applicables aux organisations à but non lucratif.

1. Objectif de la cartographie des risques

La cartographie a pour finalité d'identifier les risques susceptibles de compromettre les missions, les ressources, la conformité réglementaire, la réputation et la pérennité de l'Organisation, afin de mettre en œuvre des mesures de prévention et de maîtrise adaptées.

2. Identification des risques

L'Organisation procède à un recensement systématique des risques liés notamment au blanchiment de capitaux, au financement du terrorisme, à la fraude, à la corruption, aux conflits d'intérêts, aux détournements de fonds, aux cyberattaques, aux violations de données, aux erreurs opérationnelles et aux défaillances organisationnelles.

3. Classification des risques

Les risques sont classés par catégories, notamment les risques stratégiques, financiers, juridiques, réglementaires, opérationnels, technologiques, humains, documentaires, réputationnels, environnementaux et liés aux partenariats ou aux activités internationales.

4. Analyse des causes

Chaque risque est analysé afin d'en déterminer les facteurs déclencheurs, les vulnérabilités internes, les causes externes ainsi que les circonstances susceptibles de favoriser sa survenance.

5. Évaluation du niveau de risque

Chaque risque est évalué selon sa probabilité de survenance, son niveau d'impact potentiel, sa criticité et son degré de maîtrise par les dispositifs existants. Cette évaluation permet de définir les priorités d'intervention.

6. Mesures de maîtrise

Pour chaque risque identifié, l'Organisation définit des mesures préventives, détectives et correctives telles que le renforcement des contrôles internes, les procédures KYC, les audits, les formations, les mécanismes d'autorisation, les contrôles financiers, les dispositifs de cybersécurité et les procédures de signalement.

7. Désignation des responsables

Chaque catégorie de risque est placée sous la responsabilité d'un ou plusieurs responsables clairement identifiés, chargés d'assurer la surveillance, la prévention, le suivi des indicateurs et la mise en œuvre des actions de maîtrise.

8. Suivi permanent

La cartographie des risques fait l'objet d'un suivi régulier au moyen d'indicateurs de performance, de rapports de conformité, de contrôles permanents, d'audits, d'inspections et de revues de gouvernance permettant d'apprécier l'évolution des risques et l'efficacité des dispositifs de contrôle.

9. Actualisation de la cartographie

La cartographie est révisée périodiquement et chaque fois qu'un changement majeur intervient, notamment en cas d'évolution réglementaire, de restructuration de l'Organisation, de lancement de nouveaux projets, d'incident significatif, de fraude, de cyberattaque ou de modification importante de l'environnement opérationnel.

10. Utilisation dans la gouvernance

La cartographie constitue un outil stratégique de pilotage permettant aux organes de gouvernance d'orienter les décisions, de définir les priorités institutionnelles, d'améliorer l'allocation des ressources, de renforcer les dispositifs de conformité et d'assurer une gestion proactive des risques.

11. Contribution à l'amélioration continue

Les résultats de la cartographie alimentent les processus d'audit, de contrôle interne, de révision des politiques, de planification stratégique, de formation et de gestion des risques, favorisant ainsi une amélioration permanente du dispositif LBC/FT.

12. Protection des intérêts de l'Organisation

En identifiant de manière précoce les risques émergents et les vulnérabilités, la cartographie contribue à protéger les actifs financiers, les données, les infrastructures numériques, les ressources humaines, les bénéficiaires, les partenaires, les donateurs ainsi que la réputation institutionnelle d'AGCE International – AGCE Canada.

Par cette **Cartographie des risques**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme sa volonté de mettre en œuvre une gestion intégrée, proactive et évolutive des risques. Véritable instrument de gouvernance, elle favorise une prise de décision éclairée, renforce la conformité réglementaire, améliore la résilience organisationnelle et consolide la confiance des membres, des autorités publiques, des bailleurs de fonds, des partenaires nationaux et internationaux ainsi que de l'ensemble des parties prenantes, conformément aux plus hauts standards de transparence, de responsabilité et de lutte contre le blanchiment de capitaux et le financement du terrorisme.

ANNEXE C

Grille KYC (Know Your Customer / Connaissance du Client, du Partenaire et du Bénéficiaire)

La présente **Grille KYC (Know Your Customer – Connaissance du Client, du Partenaire et du Bénéficiaire)** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle établit un cadre méthodologique harmonisé permettant d'identifier, de vérifier, d'évaluer et de documenter l'identité ainsi que le niveau de risque des personnes physiques, des personnes morales, des partenaires, des donateurs, des bénéficiaires, des fournisseurs, des prestataires, des bailleurs de fonds, des membres et de toute autre partie avec laquelle l'Organisation entretient une relation institutionnelle, financière ou contractuelle. Cette grille constitue un outil essentiel de prévention des risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de conflits d'intérêts et d'usurpation d'identité. Elle contribue à renforcer la transparence, la conformité réglementaire, la protection des ressources institutionnelles et la crédibilité de l'Organisation auprès des autorités de contrôle et des partenaires nationaux et internationaux.

1. Objet de la grille KYC

La grille KYC a pour objectif de garantir une connaissance suffisante des personnes et organisations avec lesquelles AGCE International – AGCE Canada établit ou maintient une relation, afin d'évaluer les risques de conformité et de protéger l'Organisation contre toute utilisation abusive de ses activités.

2. Identification de la personne ou de l'entité

La grille prévoit la collecte des informations d'identification essentielles, notamment le nom complet ou la dénomination sociale, la nationalité, l'adresse, les coordonnées, la date de naissance ou de création, les numéros d'identification officiels, ainsi que tout document justificatif permettant d'établir l'identité.

3. Vérification documentaire

Les informations recueillies font l'objet d'une vérification au moyen de documents officiels, fiables, valides et, lorsque cela est possible, de sources indépendantes permettant d'en confirmer l'authenticité.

4. Identification du bénéficiaire effectif

Lorsque la relation concerne une personne morale, une association, une fondation ou toute autre structure, la grille prévoit l'identification des personnes physiques exerçant un contrôle direct ou indirect ou bénéficiant effectivement des activités ou des ressources concernées.

5. Évaluation du profil de risque

Chaque personne ou organisation fait l'objet d'une analyse permettant de déterminer son niveau de risque selon différents critères, notamment la nature des activités, la zone géographique, la structure juridique, les modalités de financement, les volumes financiers, les partenaires impliqués et les antécédents connus.

6. Vérification des personnes à risque

La grille prévoit, lorsque la réglementation applicable l'exige, des vérifications adaptées concernant les Personnes Politiquement Exposées (PPE), les personnes soumises à des sanctions nationales ou internationales, ainsi que toute personne ou organisation présentant un risque particulier.

7. Classification des risques

À l'issue de l'évaluation, chaque dossier est classé selon un niveau de risque (faible, modéré, élevé ou critique), permettant de déterminer les mesures de vigilance et de contrôle à appliquer.

8. Mesures de vigilance adaptées

En fonction du niveau de risque identifié, l'Organisation applique des mesures de vigilance proportionnées pouvant inclure une surveillance renforcée, des vérifications complémentaires, une validation hiérarchique ou un suivi plus fréquent de la relation.

9. Documentation et conservation

Toutes les informations, analyses, documents justificatifs, décisions et évaluations KYC sont enregistrés, sécurisés et conservés conformément aux règles institutionnelles de gestion documentaire, de protection des données et aux exigences légales applicables.

10. Actualisation des informations

Les informations KYC sont réexaminées périodiquement ou chaque fois qu'un changement significatif intervient dans la situation de la personne, de l'organisation ou de la relation institutionnelle, afin de maintenir une évaluation des risques constamment actualisée.

11. Confidentialité et protection des données

Les données collectées dans le cadre de la grille KYC sont traitées dans le respect des principes de confidentialité, de sécurité, de proportionnalité et de protection des données personnelles. Leur accès est strictement limité aux personnes habilitées dans le cadre de leurs fonctions.

12. Contribution à la conformité institutionnelle

La grille KYC constitue un instrument de gouvernance permettant de renforcer la qualité des contrôles internes, de sécuriser les relations institutionnelles, d'améliorer la prévention des risques financiers et de démontrer la conformité de l'Organisation aux exigences nationales et internationales en matière de LBC/FT.

En adoptant cette **Grille KYC, ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** affirme son engagement à instaurer une culture institutionnelle fondée sur la vigilance, la transparence, l'intégrité et la responsabilité. Véritable outil opérationnel de gestion des risques, cette grille favorise une connaissance approfondie des parties prenantes, contribue à la sécurisation des activités humanitaires, sociales et économiques de l'Organisation et renforce durablement la confiance des membres, bénéficiaires, donateurs, partenaires, bailleurs de fonds et autorités de contrôle.

ANNEXE D

Fiche de vigilance renforcée

La présente **Fiche de vigilance renforcée** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle établit un cadre opérationnel destiné à renforcer les contrôles lorsqu'une personne physique, une personne morale, une opération financière, un projet, un partenariat ou toute autre relation institutionnelle présente un niveau de risque élevé ou inhabituel. Cette fiche permet de formaliser les investigations complémentaires, de documenter les analyses réalisées, de justifier les décisions prises et d'assurer une traçabilité complète des mesures de vigilance appliquées. Elle constitue un instrument essentiel de prévention des risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de fonds, de conflits d'intérêts, de cybercriminalité et de toute autre activité susceptible de compromettre les missions, les ressources ou la réputation de l'Organisation. Son utilisation s'inscrit dans une approche fondée sur les risques et respecte les principes de proportionnalité, de confidentialité, de conformité réglementaire et de bonne gouvernance.

1. Objet de la fiche de vigilance renforcée

La fiche a pour objet de formaliser les contrôles complémentaires applicables aux relations ou opérations présentant un risque élevé, afin de garantir une analyse approfondie avant toute décision institutionnelle.

2. Champ d'application

La vigilance renforcée peut être mise en œuvre à l'égard des membres, donateurs, bénéficiaires, partenaires, fournisseurs, prestataires, bailleurs de fonds, consultants, représentants, personnes politiquement exposées (PPE), personnes morales, projets, programmes, opérations financières ou toute autre relation jugée sensible.

3. Déclenchement de la vigilance renforcée

La procédure est engagée lorsqu'une évaluation des risques met en évidence des éléments inhabituels, une incohérence documentaire, une opération atypique, une exposition géographique sensible, un niveau de risque élevé ou tout autre indice nécessitant des investigations complémentaires.

4. Collecte d'informations complémentaires

La fiche prévoit la collecte de renseignements additionnels permettant d'approfondir la connaissance de la personne ou de l'entité concernée, notamment sur son identité, ses

activités, ses ressources, ses partenaires, ses bénéficiaires effectifs, l'origine des fonds et la finalité des opérations.

5. Vérification documentaire renforcée

Les documents fournis font l'objet de vérifications complémentaires afin d'en confirmer l'authenticité, la cohérence, la validité et la conformité avec les informations disponibles auprès de sources fiables et indépendantes, lorsque cela est possible et autorisé.

6. Analyse du niveau de risque

Les informations recueillies sont analysées afin d'apprécier la nature, la probabilité et les conséquences potentielles des risques identifiés. Cette analyse prend en considération les critères institutionnels de classification des risques ainsi que les obligations réglementaires applicables.

7. Validation hiérarchique

Toute décision relative à une relation ou une opération soumise à une vigilance renforcée est examinée et validée par les responsables ou instances compétentes désignés par les procédures internes de l'Organisation, selon les niveaux de délégation applicables.

8. Mesures de surveillance renforcée

Lorsque la relation est maintenue, un dispositif de suivi renforcé est mis en œuvre, comprenant notamment des contrôles plus fréquents, une actualisation régulière des informations, un suivi des opérations et une réévaluation périodique du niveau de risque.

9. Documentation et traçabilité

L'ensemble des informations collectées, des analyses réalisées, des décisions prises, des validations obtenues et des mesures appliquées est consigné dans un dossier sécurisé garantissant la traçabilité complète du processus de vigilance renforcée.

10. Confidentialité et protection des informations

Les données recueillies dans le cadre de la vigilance renforcée sont traitées dans le strict respect des règles de confidentialité, de protection des données personnelles, de sécurité de l'information et des obligations légales applicables. L'accès à ces informations est limité aux seules personnes habilitées.

11. Décision finale

À l'issue de l'analyse, l'Organisation peut décider d'accepter la relation, de l'accepter sous conditions, de mettre en œuvre des mesures complémentaires de contrôle, de suspendre

temporairement la relation, de la refuser ou d'y mettre fin, conformément à ses procédures internes et aux exigences légales en vigueur.

12. Contribution à la conformité et à l'amélioration continue

Les informations issues des fiches de vigilance renforcée alimentent les dispositifs de gestion des risques, les contrôles internes, les audits, les programmes de formation et les processus de révision de la politique LBC/FT, contribuant ainsi à l'amélioration continue du système de conformité de l'Organisation.

En adoptant cette **Fiche de vigilance renforcée, ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** réaffirme son engagement à appliquer une approche fondée sur les risques, conforme aux meilleures pratiques nationales et internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Cette annexe constitue un outil opérationnel essentiel permettant de renforcer la transparence, de sécuriser les relations institutionnelles, de protéger les ressources de l'Organisation et de préserver la confiance des membres, bénéficiaires, partenaires, bailleurs de fonds, autorités de contrôle et de l'ensemble des parties prenantes.

ANNEXE E

Formulaire de déclaration d'opération suspecte

Le présent **Formulaire de déclaration d'opération suspecte** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour objectif de fournir un cadre normalisé, confidentiel et sécurisé permettant aux administrateurs, dirigeants, membres, salariés, bénévoles, partenaires, consultants, prestataires et toute personne agissant pour le compte de l'Organisation de signaler, documenter et transmettre toute opération, transaction, comportement ou situation susceptible de présenter un risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de fonds ou de toute autre activité financière illicite. Ce formulaire constitue un outil essentiel du dispositif de vigilance de l'Organisation. Il favorise une détection précoce des risques, facilite l'analyse des situations suspectes, garantit la traçabilité des signalements et contribue au respect des obligations légales, réglementaires et institutionnelles applicables. Son utilisation s'effectue dans le respect des principes de confidentialité, de protection des données, de bonne foi, de présomption d'innocence et de coopération avec les autorités compétentes lorsque la législation l'exige.

1. Objet du formulaire

Le formulaire a pour finalité de recueillir de manière structurée les informations relatives à toute opération ou situation présentant des indices de risque afin de permettre une analyse objective et documentée par les responsables compétents.

2. Personnes habilitées à effectuer une déclaration

Peuvent compléter ce formulaire les administrateurs, dirigeants, membres, salariés, bénévoles, partenaires, prestataires, consultants, auditeurs ou toute personne ayant connaissance, dans le cadre de ses fonctions ou de sa relation avec l'Organisation, d'une opération susceptible de présenter un caractère suspect.

3. Identification du déclarant

Le formulaire prévoit l'identification du déclarant lorsque cette information est nécessaire au traitement du dossier, sous réserve des mécanismes de protection des lanceurs d'alerte et des dispositions garantissant la confidentialité des signalements effectués de bonne foi.

4. Identification de la personne ou de l'entité concernée

Le formulaire permet de recueillir les informations disponibles concernant la personne physique ou morale impliquée dans l'opération suspecte, notamment son identité, sa qualité, ses

coordonnées, son rôle dans la relation institutionnelle ainsi que toute autre information pertinente.

5. Description de l'opération suspecte

Le déclarant décrit avec précision les faits observés, la nature de l'opération, les montants concernés, les moyens de paiement utilisés, les dates, les circonstances, les documents disponibles ainsi que tout élément susceptible de faciliter l'analyse de la situation.

6. Motifs du soupçon

Le formulaire comporte une rubrique permettant d'exposer les éléments objectifs ayant conduit au signalement, notamment les incohérences constatées, les comportements inhabituels, les anomalies documentaires, les transactions atypiques, les risques identifiés ou tout autre indice laissant présumer une activité illicite.

7. Pièces justificatives

Le déclarant peut joindre tout document, copie, capture d'écran, relevé, contrat, correspondance, justificatif financier ou autre élément de preuve utile à l'instruction du dossier, dans le respect des règles de confidentialité et de protection des données.

8. Transmission sécurisée

Les déclarations sont adressées exclusivement par les canaux officiels définis par l'Organisation, garantissant la confidentialité, l'intégrité, la traçabilité et la sécurité des informations transmises.

9. Analyse et traitement

Chaque déclaration fait l'objet d'un enregistrement, d'un examen préliminaire, d'une évaluation des risques, d'investigations complémentaires lorsque nécessaire et d'une décision prise par les responsables ou instances compétentes conformément aux procédures internes.

10. Protection du déclarant

Toute personne effectuant un signalement de bonne foi bénéficie des mesures de protection prévues par la politique relative aux lanceurs d'alerte, sans subir de discrimination, de représailles ou de préjudice en raison de sa démarche.

11. Conservation des dossiers

Les formulaires, pièces justificatives, analyses, décisions et suites données sont conservés dans un système documentaire sécurisé conformément aux règles institutionnelles de gestion documentaire, aux obligations légales de conservation et aux exigences relatives à la protection des données personnelles.

12. Coopération avec les autorités compétentes

Lorsque la législation applicable l'impose ou que la gravité des faits le justifie, les informations issues du formulaire peuvent servir de fondement à un signalement adressé aux autorités administratives, judiciaires, financières ou de contrôle compétentes, dans le strict respect des obligations légales et des droits des personnes concernées.

En adoptant ce **Formulaire de déclaration d'opération suspecte**, **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** renforce son dispositif de vigilance, de transparence et de maîtrise des risques. Cette annexe constitue un instrument opérationnel essentiel permettant de détecter précocement les situations à risque, de documenter les investigations, de favoriser une prise de décision éclairée et de contribuer efficacement à la prévention du blanchiment de capitaux, du financement du terrorisme, de la fraude et de toute autre activité financière illicite, conformément aux meilleures pratiques internationales de gouvernance, de conformité et de responsabilité institutionnelle.

ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE- NUMÉRIQUE (AGCE INTERNATIONAL – AGCE CANADA)

POLITIQUE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME (LBC/FT)

ANNEXE E

FORMULAIRE OFFICIEL DE DÉCLARATION D'OPÉRATION SUSPECTE (DOS)

Référence : AGCE-FRM-LBCFT-001

Version : V1.0

Classification : Strictement Confidentiel – Diffusion Restreinte

Date de déclaration : ____ / ____ / ____

Numéro de dossier : _____

***Important :** Ce formulaire est destiné à signaler toute opération, tentative d'opération, comportement, transaction ou activité susceptible de présenter un risque de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de fonds, de falsification documentaire ou de toute autre activité illicite. Toute déclaration effectuée de bonne foi bénéficie des protections prévues par les politiques internes de l'Organisation ainsi que par les dispositions légales applicables.*

I. IDENTIFICATION DU DÉCLARANT

Nom et prénom : _____

Fonction : _____

Direction / Service : _____

Statut :

☐ Administrateur

☐ Dirigeant

☐ Salarié

☐ Bénévole

☐ Partenaire

☐ Prestataire

☐ Consultant

☐ Auditeur

☐ Membre

☐ Autre : _____

Téléphone : _____

Adresse électronique : _____

Souhaitez-vous que votre identité demeure confidentielle ?

☐ Oui

☐ Non

II. PERSONNE OU ORGANISATION CONCERNÉE

Nom complet / Raison sociale :

Nationalité / Pays :

Adresse :

Téléphone :

Adresse électronique :

Type de relation avec AGCE :

☐ Membre

☐ Donateur

☐ Partenaire

☐ Fournisseur

☐ Prestataire

☐ Bénéficiaire

☐ Employé

☐ Banque

☐ Institution

☐ Autre :

Numéro de dossier interne :

III. NATURE DE L'OPÉRATION SUSPECTE

Date de l'opération :

____ / ____ / ____

Heure :

Lieu :

Nature de l'opération :

- ☐ Paiement
- ☐ Virement bancaire
- ☐ Don
- ☐ Retrait
- ☐ Dépôt
- ☐ Transfert international
- ☐ Paiement numérique
- ☐ Cryptomonnaie
- ☐ Contrat
- ☐ Achat
- ☐ Vente
- ☐ Autre :

Montant :

Devise :

Mode de paiement :

- ☐ Espèces
- ☐ Banque
- ☐ Carte bancaire
- ☐ PayPal
- ☐ SeerBit

☐ Orange Money

☐ Mobile Money

☐ Chèque

☐ Autre :

IV. DESCRIPTION DÉTAILLÉE DES FAITS

Décrivez précisément les circonstances observées.

V. INDICES AYANT MOTIVÉ LE SIGNALEMENT

Cochez les éléments observés.

☐ Identité douteuse

☐ Faux documents

☐ Documents incohérents

☐ Refus de fournir des informations

☐ Montant inhabituel

☐ Multiplication d'opérations

☐ Transactions fractionnées

☐ Origine des fonds inconnue

☐ Destination inhabituelle

- ☐ Pays à risque
 - ☐ Personne politiquement exposée (PPE)
 - ☐ Société écran
 - ☐ Utilisation de prête-noms
 - ☐ Pression pour accélérer la transaction
 - ☐ Comportement inhabituel
 - ☐ Suspicion de fraude
 - ☐ Suspicion de corruption
 - ☐ Suspicion de financement du terrorisme
 - ☐ Suspicion de blanchiment de capitaux
 - ☐ Cybercriminalité
 - ☐ Usurpation d'identité
 - ☐ Autre :
-
-

VI. DOCUMENTS OU ÉLÉMENTS DISPONIBLES

Pièces jointes :

- ☐ Copie de pièce d'identité
- ☐ Contrat
- ☐ Facture
- ☐ Capture d'écran
- ☐ Courriel
- ☐ Relevé bancaire
- ☐ Justificatif de paiement

☐ Enregistrement

☐ Photographie

☐ Vidéo

☐ Rapport

☐ Témoignage

☐ Autres :

Nombre de pièces :

VII. ÉVALUATION INITIALE DU RISQUE

Niveau estimé :

☐ Faible

☐ Modéré

☐ Élevé

☐ Critique

Nature principale du risque :

☐ Blanchiment

☐ Financement du terrorisme

☐ Fraude

☐ Corruption

☐ Conflit d'intérêts

☐ Cyberattaque

☐ Détournement de fonds

☐ Violation documentaire

☐ Autre :

VIII. MESURES DÉJÀ PRISES

☐ Suspension de l'opération

☐ Demande d'informations complémentaires

☐ Blocage temporaire

☐ Information du supérieur hiérarchique

☐ Signalement au Responsable Conformité

☐ Conservation des preuves

☐ Aucune

☐ Autres :

IX. OBSERVATIONS COMPLÉMENTAIRES

X. DÉCLARATION DU DÉCLARANT

Je soussigné(e), certifie que les informations communiquées dans le présent formulaire sont exactes, sincères et établies de bonne foi sur la base des éléments dont j'ai eu connaissance dans l'exercice de mes fonctions.

Je reconnais que toute fausse déclaration volontaire est susceptible d'engager ma responsabilité conformément aux lois applicables et aux règlements internes de l'Organisation.

Nom :

Signature :

Date : ____ / ____ / ____

XI. RÉSERVÉ AU RESPONSABLE CONFORMITÉ LBC/FT

Date de réception : ____ / ____ / ____

Numéro de référence :

Nom du responsable :

Analyse préliminaire :

- ☐ Recevable
- ☐ Informations complémentaires requises
- ☐ Sans suite
- ☐ Investigation interne
- ☐ Transmission à la Direction Générale
- ☐ Signalement à l'autorité compétente

Niveau de risque retenu :

- ☐ Faible
- ☐ Modéré
- ☐ Élevé

☐ Critique

Décision finale :

Mesures décidées :

☐ Clôture

☐ Surveillance renforcée

☐ Suspension

☐ Résiliation de la relation

☐ Audit

☐ Contrôle complémentaire

☐ Déclaration officielle

☐ Autre :

Nom :

Fonction :

Signature :

Date : ____ / ____ / ____

XII. TRAÇABILITÉ ET ARCHIVAGE

Référence documentaire : _____

Date d'archivage : ____ / ____ / ____

Durée de conservation : Conformément à la Politique LBC/FT, à la politique de gestion documentaire et aux exigences légales applicables.

Classification :

- ☐ Strictement confidentiel
- ☐ Confidentiel
- ☐ Diffusion restreinte
- ☐ Archivé

Mentions institutionnelles

Le présent formulaire est un document officiel de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il est utilisé exclusivement dans le cadre de la prévention, de la détection, de l'analyse et du traitement des opérations suspectes conformément aux politiques internes de gouvernance, aux procédures de conformité LBC/FT, aux exigences réglementaires applicables et aux meilleures pratiques internationales en matière de lutte contre le blanchiment de capitaux, le financement du terrorisme, la fraude et la criminalité financière. Les informations recueillies sont strictement confidentielles, protégées par les règles de sécurité de l'information et accessibles uniquement aux personnes dûment habilitées.

ANNEXE F

Procédure d'escalade

La présente **Procédure d'escalade** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle définit le cadre institutionnel applicable à l'identification, au signalement, au traitement et à l'escalade des situations présentant un risque élevé de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de détournement de fonds, de cybercriminalité ou de toute autre atteinte susceptible de compromettre la conformité, la sécurité ou la réputation de l'Organisation. Cette procédure garantit que toute anomalie, tout incident ou toute opération suspecte fasse l'objet d'un traitement rapide, documenté, proportionné et conforme aux exigences légales ainsi qu'aux règles internes de gouvernance. Elle précise les niveaux de responsabilité, les circuits de décision, les délais d'intervention et les modalités de communication entre les différents acteurs impliqués. Véritable mécanisme de gouvernance, la procédure d'escalade favorise une prise de décision coordonnée, limite les conséquences des incidents et renforce la capacité de l'Organisation à prévenir, maîtriser et résoudre efficacement les situations critiques.

1. Objet de la procédure d'escalade

La procédure a pour objet d'établir un processus structuré permettant d'assurer le traitement progressif et sécurisé des incidents, alertes et opérations présentant un niveau de risque nécessitant une intervention hiérarchique ou spécialisée.

2. Champ d'application

La procédure s'applique à l'ensemble des activités, programmes, projets, opérations financières, systèmes d'information, partenariats, ressources humaines, fournisseurs, prestataires, membres, bénéficiaires et parties prenantes de l'Organisation susceptibles d'être concernés par un risque LBC/FT.

3. Détection de l'événement déclencheur

L'escalade peut être initiée à la suite d'un contrôle interne, d'un audit, d'une déclaration d'opération suspecte, d'un signalement de lanceur d'alerte, d'un incident de sécurité, d'une fraude présumée, d'une cyberattaque ou de tout autre événement révélant un risque significatif.

4. Qualification initiale du risque

Le responsable ayant reçu l'information procède à une première évaluation afin de qualifier la nature de l'incident, son degré de gravité, son impact potentiel, son urgence et les mesures conservatoires pouvant être immédiatement nécessaires.

5. Notification des responsables compétents

Lorsque le risque est confirmé ou nécessite une expertise complémentaire, l'information est transmise sans délai aux responsables compétents, notamment au Responsable Conformité LBC/FT, à la Direction Générale ou à toute autre instance désignée par les procédures internes.

6. Mesures conservatoires immédiates

Selon la gravité de la situation, des mesures temporaires peuvent être décidées afin de limiter les risques, notamment la suspension d'une opération, le gel d'un paiement, la restriction d'accès à un système, la sécurisation des preuves ou la mise sous surveillance renforcée d'une relation.

7. Analyse approfondie et investigations

Les responsables désignés conduisent les investigations nécessaires afin de recueillir les éléments de preuve, d'évaluer les causes, de mesurer les conséquences et de déterminer les actions appropriées dans le respect des principes d'impartialité, de confidentialité et de traçabilité.

8. Décision d'escalade supérieure

Lorsque les investigations révèlent un risque majeur, une violation réglementaire ou une menace pour les intérêts de l'Organisation, le dossier est porté au niveau décisionnel supérieur ou, lorsque la loi l'impose, transmis aux autorités administratives, judiciaires ou financières compétentes.

9. Communication et coordination

Tout au long de la procédure, une communication sécurisée est assurée entre les acteurs concernés afin de garantir la cohérence des décisions, la confidentialité des informations et la bonne coordination des mesures de gestion de crise.

10. Documentation et traçabilité

Chaque étape de la procédure fait l'objet d'un enregistrement précis comprenant les dates, les décisions prises, les responsables impliqués, les actions réalisées, les pièces justificatives et les suites données, afin d'assurer une traçabilité complète du processus.

11. Clôture de la procédure et retour d'expérience

Une fois les mesures mises en œuvre, le dossier est formellement clôturé après validation des responsables compétents. Un retour d'expérience est réalisé afin d'identifier les enseignements tirés, les éventuelles faiblesses du dispositif et les améliorations à apporter aux procédures internes.

12. Révision et amélioration continue

La procédure d'escalade est régulièrement évaluée et actualisée afin de tenir compte des évolutions réglementaires, des nouveaux risques, des résultats des audits, des incidents observés, des recommandations des autorités compétentes et des meilleures pratiques internationales en matière de conformité et de gestion des risques.

La présente **Procédure d'escalade** constitue un élément fondamental du dispositif de gouvernance, de contrôle interne et de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En définissant des mécanismes clairs de remontée de l'information, de prise de décision et de gestion des situations sensibles, elle contribue à renforcer la transparence, la réactivité, la responsabilité et la résilience institutionnelle. Son application rigoureuse permet d'assurer une protection durable des ressources, des bénéficiaires, des partenaires, des donateurs et de la réputation de l'Organisation, tout en garantissant le respect des obligations nationales et internationales relatives à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la criminalité financière.

ANNEXE G

Liste des responsabilités

La présente **Liste des responsabilités** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle définit de manière claire, structurée et transparente les rôles, obligations et niveaux de responsabilité des organes de gouvernance, des dirigeants, des responsables opérationnels, des membres, des salariés, des bénévoles, des partenaires, des prestataires et de toute personne intervenant dans les activités de l'Organisation. Cette répartition des responsabilités constitue un pilier essentiel du dispositif de gouvernance, de contrôle interne et de conformité. Elle vise à garantir une séparation adéquate des fonctions, une responsabilisation de chaque acteur, une prise de décision documentée et une application uniforme des exigences en matière de prévention du blanchiment de capitaux, du financement du terrorisme, de la fraude, de la corruption et de toute autre forme de criminalité financière. La présente annexe favorise également la coordination entre les différents niveaux hiérarchiques, renforce la culture de conformité et facilite les opérations de contrôle, d'audit et d'amélioration continue.

1. Responsabilités du Collège Central et des organes de gouvernance

Les organes de gouvernance définissent les orientations stratégiques en matière de conformité LBC/FT, approuvent les politiques institutionnelles, assurent la supervision générale du dispositif de contrôle interne et veillent à la disponibilité des ressources humaines, techniques et financières nécessaires à son fonctionnement.

2. Responsabilités de la Présidence Générale

La Présidence Générale garantit la mise en œuvre effective de la politique LBC/FT, veille à son intégration dans les activités de l'Organisation, soutient les responsables chargés de la conformité et s'assure du respect des obligations légales, réglementaires et institutionnelles.

3. Responsabilités de la Direction Générale et des responsables opérationnels

Les responsables de direction assurent l'application quotidienne des procédures, supervisent les contrôles relevant de leur domaine de compétence, identifient les risques, mettent en œuvre les mesures correctives et rendent compte régulièrement aux instances de gouvernance.

4. Responsabilités du Responsable Conformité LBC/FT

Le Responsable Conformité coordonne le dispositif LBC/FT, réalise les évaluations des risques, supervise les procédures KYC, analyse les opérations suspectes, assure la veille réglementaire, accompagne les services opérationnels et formule des recommandations destinées à renforcer la conformité de l'Organisation.

5. Responsabilités des responsables financiers et comptables

Les responsables financiers veillent à la régularité des opérations financières, au respect des procédures de validation, à la traçabilité des flux, à la conservation des justificatifs et à la détection des anomalies susceptibles de révéler un risque financier ou réglementaire.

6. Responsabilités des salariés, bénévoles et collaborateurs

Chaque salarié, bénévole ou collaborateur est tenu de respecter les politiques internes, d'appliquer les procédures LBC/FT, de participer aux formations obligatoires, de signaler toute situation inhabituelle et de contribuer activement à la prévention des risques dans le cadre de ses missions.

7. Responsabilités des partenaires, fournisseurs et prestataires

Les partenaires institutionnels, fournisseurs et prestataires sont tenus de respecter les engagements contractuels, les principes d'intégrité, les exigences de conformité et les mesures de vigilance définies par l'Organisation. Ils coopèrent aux vérifications nécessaires et fournissent les informations requises dans le cadre des procédures de contrôle.

8. Responsabilités des membres et bénéficiaires

Les membres et bénéficiaires doivent communiquer des informations exactes, fournir les documents demandés, respecter les règles de transparence, coopérer lors des contrôles et signaler toute situation susceptible de compromettre les intérêts de l'Organisation.

9. Responsabilités en matière de signalement

Toute personne intervenant dans les activités de l'Organisation a la responsabilité de signaler sans délai, par les canaux officiels, toute opération suspecte, toute fraude présumée, tout conflit d'intérêts, toute violation des procédures ou toute situation présentant un risque pour la conformité ou la sécurité institutionnelle.

10. Responsabilités en matière de confidentialité et de protection des données

Chaque acteur est responsable de la confidentialité des informations auxquelles il a accès. Les données personnelles, financières, administratives et documentaires doivent être protégées conformément aux politiques internes, aux exigences de sécurité de l'information et aux dispositions légales applicables.

11. Responsabilités en matière de coopération, d'audit et d'amélioration continue

Tous les acteurs de l'Organisation sont tenus de coopérer avec les équipes de contrôle, les auditeurs internes ou externes, les autorités compétentes et les responsables de la conformité. Ils participent activement aux actions d'amélioration continue, à la mise en œuvre des recommandations et au renforcement permanent du dispositif LBC/FT.

12. Responsabilité individuelle et obligation de redevabilité

Chaque personne demeure personnellement responsable des décisions, actions ou omissions relevant de ses fonctions. Elle doit pouvoir démontrer le respect des procédures applicables, justifier les décisions prises et répondre de ses actes dans le cadre des mécanismes de contrôle, d'audit et de gouvernance prévus par l'Organisation.

La présente **Liste des responsabilités** constitue un référentiel de gouvernance indispensable au bon fonctionnement du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En définissant avec précision les rôles et obligations de chaque acteur, elle favorise la responsabilisation individuelle et collective, renforce la coordination institutionnelle, améliore l'efficacité des contrôles internes et consolide la confiance des membres, des bénéficiaires, des partenaires, des bailleurs de fonds et des autorités de contrôle. Son application rigoureuse participe pleinement à la promotion d'une gouvernance exemplaire, fondée sur l'intégrité, la transparence, la conformité réglementaire et la gestion responsable des risques.

ANNEXE H

Schéma du processus LBC/FT

Le présent **Schéma du processus de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme de ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il présente, sous une forme logique, chronologique et structurée, l'ensemble des étapes constituant le dispositif institutionnel de prévention, de détection, d'analyse, de traitement, de contrôle et d'amélioration continue des risques liés au blanchiment de capitaux et au financement du terrorisme. Ce schéma constitue un référentiel opérationnel permettant à l'ensemble des organes de gouvernance, des responsables, des collaborateurs, des membres, des bénévoles, des partenaires, des prestataires et des auditeurs de comprendre clairement les interactions entre les différentes procédures internes. Il facilite la coordination des acteurs, renforce la traçabilité des décisions, améliore l'efficacité des contrôles et garantit une application cohérente des exigences légales, réglementaires et institutionnelles. Il contribue également à la diffusion d'une culture de conformité fondée sur la transparence, la responsabilité, la vigilance et la gestion proactive des risques, conformément aux meilleures pratiques nationales et internationales en matière de LBC/FT.

1. Identification de la relation ou de l'opération

Le processus débute par l'identification de toute personne physique, personne morale, partenaire, membre, bénéficiaire, fournisseur, donateur, bailleur de fonds ou opération financière entrant dans le périmètre d'application de la politique LBC/FT. Cette première étape permet d'ouvrir un dossier de conformité et d'engager les contrôles préalables requis.

2. Collecte des informations et procédures KYC

Les informations d'identification, les documents justificatifs et les renseignements relatifs aux activités, à l'origine des fonds, aux bénéficiaires effectifs et à la finalité de la relation sont recueillis conformément aux procédures de connaissance du client, du partenaire ou du bénéficiaire (KYC).

3. Vérification et validation documentaire

Les informations collectées sont vérifiées afin d'en confirmer l'exactitude, la cohérence, la validité et l'authenticité. Cette étape comprend également les contrôles documentaires, les vérifications internes et, lorsque cela est autorisé, le recours à des sources fiables et indépendantes.

4. Évaluation et classification des risques

Les données recueillies sont analysées afin de déterminer le niveau de risque présenté par la relation ou l'opération. Cette évaluation repose sur une approche fondée sur les risques prenant en compte les critères institutionnels, financiers, géographiques, opérationnels et réglementaires.

5. Décision d'acceptation, de refus ou de vigilance renforcée

Selon les résultats de l'évaluation, l'Organisation décide soit d'établir la relation, soit de la refuser, soit de mettre en œuvre une procédure de vigilance renforcée impliquant des contrôles complémentaires et une validation hiérarchique.

6. Réalisation et surveillance des opérations

Les opérations autorisées sont exécutées dans le respect des procédures internes de contrôle, de validation, de séparation des fonctions et de sécurité financière. Elles font l'objet d'un suivi permanent afin de détecter toute anomalie ou évolution du niveau de risque.

7. Détection des anomalies et opérations suspectes

Les dispositifs de contrôle permanent, les audits, les signalements internes et les mécanismes automatisés de surveillance permettent d'identifier rapidement toute opération inhabituelle, incohérente ou susceptible de révéler un risque de blanchiment de capitaux, de financement du terrorisme, de fraude ou d'autres activités illicites.

8. Déclaration, analyse et procédure d'escalade

Toute opération suspecte fait l'objet d'une déclaration selon les procédures internes. Une analyse approfondie est conduite par les responsables compétents, pouvant conduire à une escalade hiérarchique, à la mise en œuvre de mesures conservatoires ou, lorsque la loi l'impose, à un signalement aux autorités compétentes.

9. Décision, mesures correctives et suivi

À l'issue des investigations, l'Organisation adopte les mesures appropriées pouvant comprendre la poursuite de la relation, une surveillance renforcée, la suspension ou la résiliation de la relation, ainsi que toute autre mesure corrective destinée à protéger les intérêts institutionnels et à assurer la conformité réglementaire.

10. Documentation et conservation des preuves

L'ensemble des informations, contrôles, analyses, décisions, validations et pièces justificatives est enregistré dans un système documentaire sécurisé garantissant la traçabilité complète des opérations et le respect des durées légales de conservation.

11. Contrôle, audit et amélioration continue

Le processus est régulièrement évalué au moyen de contrôles permanents, d'audits internes et externes, d'indicateurs de conformité, de revues de gouvernance et d'analyses de risques permettant d'identifier les axes d'amélioration et de renforcer l'efficacité du dispositif LBC/FT.

12. Révision de la politique et retour d'expérience

Les enseignements tirés des incidents, des audits, des contrôles, des évolutions réglementaires et des recommandations des autorités sont intégrés dans le processus de révision de la politique. Cette démarche garantit une adaptation permanente du dispositif aux nouveaux risques et aux meilleures pratiques internationales.

Le présent **Schéma du processus LBC/FT** constitue un outil stratégique de gouvernance permettant à **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)** de disposer d'une vision globale, cohérente et intégrée de son dispositif de conformité. En représentant de manière structurée les différentes étapes du processus, les responsabilités associées et les interactions entre les mécanismes de contrôle, il facilite l'appropriation des procédures par l'ensemble des parties prenantes, renforce la qualité des décisions, améliore la réactivité face aux risques et consolide la transparence, la redevabilité et la confiance des membres, des partenaires, des bailleurs de fonds, des autorités de contrôle et de toutes les personnes impliquées dans les activités de l'Organisation. Ce schéma illustre l'engagement permanent d'AGCE International – AGCE Canada en faveur d'une gouvernance exemplaire, d'une gestion responsable des risques et d'une conformité durable aux normes nationales et internationales relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

ANNEXE I

CHARTRE D'ENGAGEMENT DES COLLABORATEURS EN MATIÈRE DE LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX ET LE FINANCEMENT DU TERRORISME (LBC/FT)

Référence : AGCE-CHR-LBCFT-001

Version : V1.0

Classification : Document institutionnel – Engagement obligatoire

Applicable à : L'ensemble des administrateurs, dirigeants, membres, salariés, bénévoles, consultants, partenaires, prestataires, stagiaires et toute personne intervenant pour le compte de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**.

PRÉAMBULE

La présente **Charte d'engagement des collaborateurs** constitue une annexe officielle de la **Politique de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle traduit l'engagement collectif de l'Organisation à promouvoir une culture de conformité, d'intégrité, de transparence et de responsabilité dans toutes ses activités humanitaires, sociales, éducatives, économiques et numériques.

Chaque collaborateur, quel que soit son statut ou son niveau de responsabilité, contribue directement à la prévention des risques de blanchiment de capitaux, de financement du terrorisme, de fraude, de corruption, de conflits d'intérêts et de toute autre activité illicite susceptible de porter atteinte aux intérêts de l'Organisation ou de ses parties prenantes.

Par la signature de la présente Charte, chaque collaborateur reconnaît avoir pris connaissance de la Politique LBC/FT d'AGCE International – AGCE Canada et s'engage à en respecter l'ensemble des dispositions.

I. MES ENGAGEMENTS

Je m'engage à :

1. Respecter les lois et règlements

Appliquer en permanence les lois nationales et internationales ainsi que les politiques internes relatives à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

2. Agir avec intégrité

Exercer mes fonctions avec honnêteté, impartialité, loyauté, professionnalisme et dans le respect des principes éthiques de l'Organisation.

3. Respecter les procédures internes

Appliquer rigoureusement toutes les procédures relatives au contrôle interne, au KYC, à la vigilance, à la sécurité financière, à la gestion documentaire et à la conformité.

4. Vérifier les informations

M'assurer que les informations et documents recueillis auprès des membres, partenaires, bénéficiaires, fournisseurs ou donateurs sont complets, cohérents et fiables.

5. Signaler toute situation suspecte

Informier immédiatement les responsables compétents de toute opération inhabituelle, fraude présumée, falsification documentaire, conflit d'intérêts ou comportement susceptible de présenter un risque LBC/FT.

6. Préserver la confidentialité

Garantir la confidentialité des informations auxquelles j'ai accès et ne communiquer aucune donnée sensible à des personnes non autorisées.

7. Coopérer aux contrôles

Participer pleinement aux audits, inspections, contrôles internes, enquêtes et investigations réalisés dans le cadre des obligations de conformité.

8. Protéger les ressources de l'Organisation

Veiller à une utilisation responsable, transparente et conforme des ressources financières, matérielles, numériques et documentaires mises à ma disposition.

9. Déclarer tout conflit d'intérêts

Informier immédiatement l'Organisation de toute situation susceptible de compromettre mon impartialité ou l'indépendance de mes décisions.

10. Participer aux formations

Suivre les formations obligatoires relatives à la conformité, à la gouvernance, à l'éthique, à la cybersécurité et à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

11. Favoriser l'amélioration continue

Contribuer activement au renforcement permanent des procédures, des contrôles et des bonnes pratiques de gouvernance par des propositions constructives et un retour d'expérience.

12. Représenter dignement AGCE International

Adopter en toutes circonstances un comportement conforme aux valeurs de transparence, de responsabilité, de solidarité, de respect des droits humains et de bonne gouvernance défendues par l'Organisation.

II. MES INTERDICTIONS

Je m'interdis notamment de :

- participer directement ou indirectement à une opération illicite ;
- accepter ou proposer un avantage indu ;
- falsifier un document ou une information ;
- contourner les procédures de contrôle interne ;
- divulguer des informations confidentielles ;
- utiliser les ressources de l'Organisation à des fins personnelles ou frauduleuses ;
- exercer des représailles contre un lanceur d'alerte agissant de bonne foi ;
- ignorer volontairement une situation présentant un risque de conformité.

III. ENGAGEMENT EN MATIÈRE DE RESPONSABILITÉ

Je reconnais que le respect de la présente Charte constitue une obligation professionnelle et institutionnelle.

Je comprends que tout manquement pourra entraîner, selon sa gravité :

- une mesure corrective ;
- un rappel à l'ordre ;
- une formation complémentaire ;
- une sanction disciplinaire ;
- une suspension temporaire ;
- une résiliation de ma collaboration ;
- un signalement aux autorités compétentes lorsque la législation applicable l'exige.

IV. DÉCLARATION D'ENGAGEMENT

Je soussigné(e), déclare :

- ☐ avoir reçu un exemplaire de la Politique LBC/FT ;
- ☐ avoir pris connaissance de la présente Charte ;
- ☐ comprendre les responsabilités qui me sont confiées ;
- ☐ m'engager à respecter toutes les procédures internes de conformité ;
- ☐ signaler toute opération suspecte conformément aux procédures de l'Organisation ;
- ☐ protéger les intérêts, les ressources et la réputation de **AGCE International – AGCE Canada**.

V. IDENTIFICATION DU COLLABORATEUR

Nom et prénom :

Fonction :

Direction / Service :

Statut :

- ☐ Administrateur
- ☐ Dirigeant
- ☐ Salarié
- ☐ Bénévole
- ☐ Consultant
- ☐ Prestataire

☐ Partenaire

☐ Stagiaire

☐ Autre : _____

Téléphone :

Adresse électronique :

Lieu :

Date : ____ / ____ / ____

VI. SIGNATURE

Le Collaborateur

Nom :

Signature :

Date : ____ / ____ / ____

Le Responsable hiérarchique

Nom :

Fonction :

Signature :

Date : ____ / ____ / ____

Responsable Conformité LBC/FT

Nom :

Signature :

Date : ____ / ____ / ____

VII. CLAUSE FINALE

La présente **Charte d'engagement des collaborateurs** entre en vigueur dès sa signature et demeure applicable pendant toute la durée de la relation entre le collaborateur et **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle complète les politiques de gouvernance, le Code d'éthique et d'intégrité, les procédures de contrôle interne et l'ensemble des dispositifs institutionnels de conformité de l'Organisation.

En adhérant à cette Charte, chaque collaborateur participe activement au maintien d'un environnement de travail fondé sur l'intégrité, la transparence, la responsabilité et la prévention des risques. Il contribue ainsi à protéger les ressources, les bénéficiaires, les partenaires, les bailleurs de fonds et la réputation d'AGCE International – AGCE Canada, tout en renforçant la confiance des parties prenantes et le respect des meilleures pratiques nationales et internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme.

ANNEXE J

REGISTRE DES CONTRÔLES

Description

Le **Registre des contrôles** constitue un document officiel de gouvernance, de conformité et de traçabilité intégré au dispositif de **lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour finalité d'enregistrer, de manière chronologique, exhaustive et sécurisée, l'ensemble des activités de contrôle réalisées dans le cadre de la prévention, de la détection, de l'évaluation et du traitement des risques liés au blanchiment de capitaux, au financement du terrorisme, à la fraude, à la corruption, aux conflits d'intérêts, aux violations réglementaires et aux autres risques de conformité.

Ce registre constitue un instrument essentiel de pilotage permettant d'assurer la traçabilité complète des contrôles effectués, des anomalies constatées, des décisions prises, des mesures correctives mises en œuvre et des résultats obtenus. Il favorise la transparence, facilite les audits internes et externes, améliore le suivi des recommandations et permet aux organes de gouvernance de disposer d'une vision consolidée de l'efficacité du dispositif de contrôle interne.

Le Registre des contrôles doit être tenu à jour de façon continue par les responsables habilités. Il est conservé dans un environnement sécurisé garantissant l'intégrité, la confidentialité, la disponibilité et l'archivage des informations, conformément aux politiques institutionnelles de gestion documentaire, de protection des données et aux exigences légales applicables.

Actions nécessaires

1. Enregistrer chaque contrôle réalisé

Consigner systématiquement tous les contrôles préventifs, détectifs, correctifs ou de conformité effectués dans le cadre des activités de l'Organisation.

2. Identifier le contrôle

Attribuer à chaque contrôle un numéro de référence unique, une date d'exécution, un intitulé précis et une catégorie de contrôle (financier, KYC, documentaire, informatique, opérationnel, etc.).

3. Identifier les responsables

Mentionner le nom, la fonction, le service et les personnes ayant réalisé, supervisé ou validé le contrôle.

4. Décrire l'objet du contrôle

Préciser l'activité, le processus, le projet, la transaction, le partenaire, le membre ou le document ayant fait l'objet du contrôle.

5. Documenter les constats

Enregistrer les observations, anomalies, écarts, non-conformités, incidents ou bonnes pratiques identifiés lors du contrôle.

6. Évaluer le niveau de risque

Qualifier les risques détectés selon leur criticité (faible, modéré, élevé ou critique) ainsi que leur impact potentiel sur l'Organisation.

7. Définir les actions correctives

Préciser les mesures décidées pour corriger les anomalies, réduire les risques, renforcer les contrôles ou améliorer les procédures existantes.

8. Désigner les responsables du suivi

Identifier les personnes chargées de mettre en œuvre les actions correctives ainsi que les échéances prévues pour leur réalisation.

9. Vérifier l'efficacité des mesures

Contrôler que les actions décidées ont été effectivement réalisées et qu'elles ont permis de supprimer ou de réduire les risques identifiés.

10. Produire des rapports périodiques

Utiliser les informations du registre pour élaborer les rapports de conformité, les tableaux de bord de gouvernance, les rapports d'audit et les rapports destinés aux organes décisionnels.

11. Garantir la traçabilité documentaire

Conserver l'ensemble des pièces justificatives, rapports, procès-verbaux, formulaires, décisions et documents associés à chaque contrôle afin d'assurer une traçabilité complète.

12. Actualiser régulièrement le registre

Mettre à jour le registre après chaque contrôle, audit, inspection, incident, révision réglementaire ou mise en œuvre d'une mesure corrective afin de maintenir une vision fidèle et actualisée du niveau de conformité de l'Organisation.

Contenu minimal du Registre des contrôles

Le registre devrait comprendre au minimum les rubriques suivantes :

- Numéro du contrôle
- Date du contrôle
- Type de contrôle
- Service ou activité concerné
- Objet du contrôle
- Responsable du contrôle
- Références des procédures applicables
- Constats réalisés
- Niveau de risque
- Non-conformités identifiées
- Mesures correctives décidées
- Responsable de la mise en œuvre
- Échéance de réalisation
- Date de vérification du suivi
- Résultat du contrôle de suivi
- Statut (Ouvert – En cours – Clôturé)
- Observations complémentaires
- Signature du contrôleur
- Validation du Responsable Conformité LBC/FT

Finalité du registre

Le **Registre des contrôles** constitue une preuve permanente de l'application effective du dispositif LBC/FT d'**AGCE International – AGCE Canada**. Il permet de démontrer aux autorités de contrôle, aux auditeurs, aux partenaires institutionnels et aux bailleurs de fonds que l'Organisation applique des mécanismes de surveillance, de contrôle interne et d'amélioration continue conformes aux meilleures pratiques nationales et internationales. En renforçant la traçabilité, la responsabilité et la redevabilité, ce registre contribue directement à la protection des ressources de l'Organisation, à la maîtrise des risques et au maintien d'une gouvernance exemplaire fondée sur la transparence, l'intégrité et la conformité réglementaire.

ANNEXE K

REGISTRE DES INCIDENTS

Description

Le **Registre des incidents** constitue un document officiel de gouvernance, de conformité et de gestion des risques intégré au dispositif de **lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour objectif d'assurer l'enregistrement, le suivi, l'analyse et la traçabilité de tous les incidents, événements indésirables, anomalies, violations de procédures, tentatives de fraude, opérations suspectes, cyberattaques, incidents de sécurité, erreurs opérationnelles et toute situation susceptible de compromettre la conformité, les ressources, les activités ou la réputation de l'Organisation.

Ce registre constitue un outil essentiel de pilotage permettant d'identifier les causes profondes des incidents, d'évaluer leur niveau de gravité, de mettre en œuvre les mesures correctives appropriées et de prévenir leur récurrence. Il contribue au renforcement du contrôle interne, de la sécurité financière, de la gestion des risques et de l'amélioration continue du système de conformité LBC/FT.

Chaque incident doit être déclaré, documenté, classifié, analysé, traité et clôturé selon une procédure formalisée. Les informations consignées dans ce registre sont protégées par les règles de confidentialité, de sécurité de l'information et de protection des données applicables au sein de l'Organisation. Le registre est régulièrement examiné par les responsables compétents afin d'orienter les décisions de gouvernance, les actions de prévention et les programmes de formation.

Actions nécessaires

1. Enregistrer systématiquement chaque incident

Consigner sans délai tout incident, anomalie, opération suspecte, violation de procédure ou événement susceptible d'avoir un impact sur la conformité, les activités ou les ressources de l'Organisation.

2. Attribuer une référence unique

Affecter à chaque incident un numéro d'identification unique permettant d'assurer son suivi, son archivage et sa traçabilité tout au long de son cycle de traitement.

3. Identifier les personnes concernées

Préciser les personnes, services, partenaires, bénéficiaires, fournisseurs ou autres parties prenantes impliqués ou affectés par l'incident, dans le respect des règles de confidentialité.

4. Décrire précisément l'incident

Documenter la nature de l'incident, les circonstances de sa découverte, la date, l'heure, le lieu, les faits observés ainsi que les éléments ayant conduit à son identification.

5. Classifier la nature de l'incident

Qualifier l'incident selon sa catégorie, notamment : fraude, blanchiment de capitaux, financement du terrorisme, cyberattaque, violation documentaire, conflit d'intérêts, corruption, erreur opérationnelle, incident informatique, fuite de données ou tout autre risque de conformité.

6. Évaluer le niveau de gravité

Apprécier l'impact réel ou potentiel de l'incident sur les activités, les ressources financières, les données, les bénéficiaires, les partenaires, la conformité réglementaire et la réputation de l'Organisation.

7. Déclencher les mesures immédiates

Mettre en œuvre, lorsque cela est nécessaire, les mesures conservatoires appropriées telles que la suspension d'une opération, le blocage d'un accès, la sécurisation des preuves, la protection des données ou l'activation de la procédure d'escalade.

8. Désigner un responsable du traitement

Nommer la personne ou l'équipe chargée de conduire les investigations, de coordonner les actions correctives, d'assurer le suivi du dossier et de rendre compte aux instances compétentes.

9. Définir et suivre les actions correctives

Identifier les causes de l'incident, établir un plan d'action, fixer les échéances, attribuer les responsabilités et vérifier la mise en œuvre effective des mesures destinées à supprimer ou réduire le risque.

10. Clôturer officiellement le dossier

Prononcer la clôture de l'incident uniquement après validation que les investigations sont terminées, que les actions correctives ont été réalisées et que le risque est maîtrisé.

11. Produire des analyses et des statistiques

Exploiter les données du registre afin d'établir des tableaux de bord, des rapports de conformité, des indicateurs de performance et des analyses des tendances permettant d'améliorer la gestion des risques.

12. Capitaliser les retours d'expérience

Utiliser les enseignements tirés de chaque incident pour renforcer les politiques internes, améliorer les procédures, adapter les formations, actualiser la cartographie des risques et consolider le dispositif global de lutte contre le blanchiment de capitaux et le financement du terrorisme.

Contenu minimal du Registre des incidents

Le registre devrait comprendre au minimum les rubriques suivantes :

- Numéro de référence de l'incident
- Date et heure de déclaration
- Date de survenance
- Service ou activité concerné
- Déclarant
- Personnes ou entités concernées
- Catégorie de l'incident
- Description détaillée des faits
- Niveau de gravité (Faible, Modéré, Élevé, Critique)
- Niveau de risque LBC/FT
- Conséquences constatées
- Mesures conservatoires appliquées
- Responsable du traitement
- Résultats des investigations
- Actions correctives mises en œuvre
- Date de mise en œuvre
- Contrôle de l'efficacité des actions
- Décision finale
- Date de clôture
- Statut (Nouveau – En cours – Sous investigation – Clôturé)
- Observations complémentaires
- Signature du responsable
- Validation du Responsable Conformité LBC/FT

Finalité du registre

Le **Registre des incidents** constitue un instrument central du système de gouvernance et de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il permet d'assurer une gestion méthodique, transparente et documentée de tous les incidents susceptibles d'affecter l'Organisation, tout en renforçant la prévention, la détection et la maîtrise des risques. Véritable outil de redevabilité, il facilite les audits, démontre l'efficacité du dispositif de contrôle interne et contribue à instaurer une culture institutionnelle de vigilance, d'amélioration continue et de conformité durable aux exigences nationales et internationales relatives à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la criminalité financière.

ANNEXE L

REGISTRE DES FORMATIONS

Description

Le **Registre des formations** constitue un document officiel de gestion des compétences, de conformité et de gouvernance intégré au dispositif de **lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour objet de planifier, enregistrer, suivre, évaluer et archiver l'ensemble des activités de formation, de sensibilisation, de perfectionnement et de renforcement des capacités organisées au profit des administrateurs, dirigeants, responsables, salariés, bénévoles, membres, consultants, partenaires, prestataires et toute autre personne intervenant dans les activités de l'Organisation.

Ce registre constitue un outil stratégique permettant de démontrer que l'Organisation veille au maintien et au développement des compétences nécessaires à la mise en œuvre efficace de sa politique LBC/FT. Il assure une traçabilité complète des formations suivies, des participants, des contenus pédagogiques, des évaluations, des certifications obtenues et des actions de recyclage. Il contribue ainsi au renforcement de la culture de conformité, à la prévention des risques, à l'amélioration des performances opérationnelles et au respect des exigences des autorités de contrôle, des partenaires institutionnels et des bailleurs de fonds.

Le Registre des formations est mis à jour de manière continue par les responsables désignés. Il constitue une source d'information essentielle pour les audits internes et externes, les évaluations de conformité, les plans de développement des compétences et les revues de gouvernance. Les informations qui y sont consignées sont conservées dans un environnement sécurisé garantissant leur intégrité, leur confidentialité, leur disponibilité et leur conservation conformément aux exigences réglementaires et aux politiques institutionnelles de gestion documentaire.

Actions nécessaires

1. Enregistrer chaque action de formation

Consigner systématiquement toute formation, séance de sensibilisation, atelier, séminaire, webinaire, exercice pratique ou programme de renforcement des capacités organisé dans le cadre du dispositif LBC/FT.

2. Identifier la formation

Attribuer à chaque action de formation un numéro de référence unique en précisant son intitulé, son objectif, son thème principal, sa durée, son format (présentiel, distanciel ou hybride) et sa date de réalisation.

3. Identifier les participants

Enregistrer les informations relatives aux participants, notamment leur identité, leur fonction, leur service, leur statut au sein de l'Organisation ainsi que leur niveau de responsabilité.

4. Identifier les formateurs

Préciser les noms, qualifications, organismes d'appartenance et responsabilités des formateurs, intervenants ou experts ayant animé la session.

5. Décrire le contenu pédagogique

Documenter les modules abordés, les objectifs pédagogiques, les supports de formation utilisés, les études de cas, les exercices pratiques ainsi que les références réglementaires et institutionnelles présentées.

6. Évaluer les acquis

Mettre en œuvre des évaluations permettant de mesurer le niveau de compréhension des participants, les compétences acquises et leur aptitude à appliquer les procédures LBC/FT dans leurs activités professionnelles.

7. Délivrer les attestations ou certifications

Enregistrer les attestations de participation, certificats de réussite ou autres reconnaissances délivrés à l'issue des formations, lorsque les conditions requises sont remplies.

8. Identifier les besoins complémentaires

Analyser les résultats des évaluations afin d'identifier les besoins de perfectionnement, de recyclage ou de formation spécialisée pour certaines catégories de collaborateurs.

9. Assurer le suivi des formations obligatoires

Contrôler que chaque collaborateur concerné a bien suivi les formations obligatoires et programmer les sessions de mise à niveau lorsque cela est nécessaire.

10. Élaborer des rapports périodiques

Exploiter les données du registre afin de produire des statistiques, des tableaux de bord et des rapports destinés aux organes de gouvernance, aux responsables de la conformité et aux auditeurs.

11. Conserver les preuves documentaires

Archiver l'ensemble des feuilles de présence, convocations, programmes, supports pédagogiques, évaluations, attestations, certificats et autres documents justificatifs relatifs à chaque formation.

12. Actualiser régulièrement le registre

Mettre à jour le registre après chaque nouvelle formation, chaque recyclage, chaque évolution réglementaire ou chaque modification du plan annuel de formation afin de garantir la disponibilité permanente d'informations exactes et à jour.

Contenu minimal du Registre des formations

Le registre devrait comprendre au minimum les rubriques suivantes :

- Numéro de référence de la formation
- Intitulé de la formation
- Objectifs pédagogiques
- Domaine concerné (LBC, FT, KYC, conformité, audit, cybersécurité, gouvernance, etc.)
- Date de la formation
- Durée
- Lieu ou plateforme de formation
- Mode de formation (présentiel, distanciel, hybride)
- Nom du formateur ou de l'organisme formateur
- Liste des participants
- Fonction et service des participants
- Nombre de participants
- Supports pédagogiques utilisés
- Résultats des évaluations
- Attestations ou certifications délivrées
- Besoins de formation complémentaires
- Date prévue du recyclage
- Observations
- Signature du formateur
- Validation du Responsable Formation
- Validation du Responsable Conformité LBC/FT

Finalité du registre

Le **Registre des formations** constitue un instrument fondamental de gouvernance et de développement des compétences de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il permet de démontrer que l'Organisation assure une formation continue, structurée et documentée de l'ensemble de ses collaborateurs en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. En garantissant la traçabilité des actions de formation, l'évaluation des compétences et le suivi des obligations de sensibilisation, ce registre renforce la culture de conformité, améliore l'efficacité opérationnelle, favorise l'amélioration continue et consolide la confiance des autorités de contrôle, des partenaires institutionnels, des bailleurs de fonds et de l'ensemble des parties prenantes dans la capacité de l'Organisation à prévenir et maîtriser les risques de criminalité financière.

ANNEXE M

TABLEAU DES NIVEAUX DE RISQUES

Description

Le **Tableau des niveaux de risques** constitue un document officiel d'évaluation, de classification et de gestion des risques intégré au dispositif de **lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Il a pour vocation de fournir un cadre méthodologique uniforme permettant d'apprécier, de classer et de hiérarchiser les risques auxquels l'Organisation est exposée dans le cadre de ses activités institutionnelles, humanitaires, sociales, financières, numériques et internationales.

Ce tableau constitue un outil d'aide à la décision destiné aux organes de gouvernance, au Responsable Conformité LBC/FT, aux responsables opérationnels, aux auditeurs et aux contrôleurs internes. Il facilite l'application d'une approche fondée sur les risques en permettant d'identifier les situations nécessitant des mesures de vigilance normale, renforcée ou exceptionnelle. Grâce à une évaluation harmonisée de la probabilité de survenance, de l'impact potentiel, du niveau de maîtrise des contrôles existants et de la criticité globale, il contribue à orienter les décisions de contrôle, les priorités d'intervention et l'allocation des ressources.

Le **Tableau des niveaux de risques** est utilisé dans toutes les étapes du dispositif LBC/FT, notamment lors des procédures KYC, de la sélection des partenaires, de l'analyse des opérations financières, de la surveillance des activités, des audits, des investigations, de la gestion des incidents et de la révision périodique de la cartographie des risques. Il est actualisé régulièrement afin d'intégrer les évolutions réglementaires, les nouveaux risques émergents, les résultats des audits, les retours d'expérience et les recommandations des autorités compétentes. Son utilisation garantit une approche cohérente, objective, documentée et proportionnée de la gestion des risques conformément aux meilleures pratiques nationales et internationales.

Actions nécessaires

1. Définir les critères d'évaluation des risques

Établir des critères objectifs permettant d'apprécier chaque risque selon sa nature, sa probabilité de survenance, son impact potentiel, sa fréquence et son niveau de maîtrise.

2. Identifier les risques à évaluer

Recenser les risques liés aux opérations financières, aux partenaires, aux bénéficiaires, aux donateurs, aux fournisseurs, aux projets, aux systèmes d'information, aux ressources humaines et à toute activité susceptible d'exposer l'Organisation à un risque LBC/FT.

3. Classifier les niveaux de risques

Attribuer à chaque risque un niveau de criticité, généralement réparti en quatre catégories :

- Faible
- Modéré
- Élevé
- Critique

afin d'assurer une lecture homogène des évaluations.

4. Évaluer la probabilité de survenance

Analyser la possibilité qu'un risque se réalise en tenant compte des données historiques, des vulnérabilités identifiées, du contexte opérationnel et des facteurs externes.

5. Évaluer l'impact potentiel

Mesurer les conséquences financières, juridiques, opérationnelles, réputationnelles, organisationnelles, humaines et réglementaires que pourrait entraîner la réalisation du risque.

6. Déterminer les mesures de maîtrise

Identifier les contrôles existants et définir les actions préventives, détectives et correctives nécessaires pour réduire la probabilité de survenance ou limiter les conséquences du risque.

7. Associer un responsable à chaque niveau de risque

Désigner le responsable chargé du suivi, de la surveillance, de la mise en œuvre des mesures de maîtrise et du reporting relatif à chaque risque identifié.

8. Déterminer les actions à entreprendre selon le niveau de risque

Prévoir les mesures applicables pour chaque catégorie de risque, notamment la vigilance standard, la vigilance renforcée, les contrôles complémentaires, la validation hiérarchique, la suspension d'une opération ou l'activation de la procédure d'escalade.

9. Assurer un suivi régulier

Réexaminer périodiquement les risques identifiés afin de vérifier leur évolution, l'efficacité des mesures de maîtrise mises en œuvre et la nécessité d'adapter les contrôles existants.

10. Documenter toutes les évaluations

Conserver les résultats des analyses, les décisions prises, les justifications des niveaux attribués ainsi que les mesures correctives engagées afin de garantir une parfaite traçabilité.

11. Exploiter les résultats pour le pilotage de la conformité

Utiliser le tableau comme support de décision pour les audits, les revues de gouvernance, les plans de contrôle, les formations, la cartographie des risques et les rapports destinés aux organes de gouvernance.

12. Actualiser périodiquement le tableau

Réviser le tableau des niveaux de risques lors de chaque évolution réglementaire, changement organisationnel, incident majeur, lancement d'un nouveau projet, partenariat stratégique ou à la suite des recommandations issues des audits et contrôles.

Contenu minimal du Tableau des niveaux de risques

Le tableau devrait comporter au minimum les rubriques suivantes :

- Numéro de référence du risque
- Catégorie de risque
- Description du risque
- Activité ou processus concerné
- Probabilité de survenance
- Niveau d'impact
- Niveau de criticité
- Contrôles existants
- Niveau de maîtrise actuel
- Niveau de risque résiduel
- Mesures préventives
- Mesures correctives
- Responsable du suivi
- Fréquence de surveillance
- Date de la dernière évaluation
- Date de la prochaine révision
- Statut du risque (Accepté – Sous surveillance – À traiter – Clos)
- Observations

- Validation du Responsable Conformité LBC/FT
- Validation de la Direction Générale

Échelle recommandée des niveaux de risques

Niveau	Couleur	Signification	Action requise
Faible	 Vert	Risque maîtrisé, impact limité	Surveillance courante et contrôles standards
Modéré	 Jaune	Risque nécessitant une vigilance accrue	Renforcement des contrôles et suivi périodique
Élevé	 Orange	Risque important pouvant affecter les activités	Vigilance renforcée, validation hiérarchique et plan d'action immédiat
Critique	 Rouge	Risque majeur susceptible de compromettre l'Organisation	Suspension de l'opération, procédure d'escalade, investigation approfondie et, si nécessaire, signalement aux autorités compétentes

Finalité du tableau

Le **Tableau des niveaux de risques** constitue un référentiel décisionnel indispensable au système de gouvernance et de conformité de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En offrant une méthode normalisée d'évaluation et de hiérarchisation des risques, il permet d'améliorer la qualité des décisions, de renforcer l'efficacité des contrôles internes, d'optimiser l'allocation des ressources et de favoriser une gestion proactive des risques. Il démontre également l'engagement permanent de l'Organisation en faveur d'une gouvernance exemplaire, d'une transparence accrue et d'une conformité durable aux exigences nationales et internationales relatives à la lutte contre le blanchiment de capitaux, le financement du terrorisme et la criminalité financière.

ANNEXE N

MATRICE DES RESPONSABILITÉS (RACI)

Description

La **Matrice des responsabilités (RACI)** constitue un document officiel de gouvernance, d'organisation et de contrôle interne intégré au dispositif de **lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle a pour objectif de définir de manière claire, précise et harmonisée les rôles et les responsabilités des différents acteurs impliqués dans la mise en œuvre, le suivi, le contrôle et l'amélioration continue du dispositif LBC/FT.

Fondée sur la méthodologie internationale **RACI** (*Responsible, Accountable, Consulted, Informed*), cette matrice permet d'éviter les ambiguïtés organisationnelles, les chevauchements de responsabilités, les omissions et les conflits de compétences. Elle facilite la coordination entre les organes de gouvernance, la Direction Générale, le Responsable Conformité LBC/FT, les responsables opérationnels, les équipes financières, les auditeurs, les collaborateurs, les partenaires et les autres parties prenantes.

La Matrice RACI constitue un outil essentiel de pilotage permettant de déterminer, pour chaque processus, activité ou décision relevant de la conformité LBC/FT :

- la personne qui réalise effectivement l'action (**Responsible**) ;
- l'autorité qui valide et assume la responsabilité finale (**Accountable**) ;
- les personnes devant être consultées avant toute décision (**Consulted**) ;
- les personnes devant être informées des décisions prises (**Informed**).

Cette matrice favorise une gouvernance efficace, renforce la redevabilité, améliore la rapidité des prises de décision, facilite les audits et garantit une parfaite traçabilité des responsabilités au sein de l'Organisation. Elle est régulièrement révisée afin de tenir compte des évolutions organisationnelles, réglementaires et opérationnelles.

Actions nécessaires

1. Identifier les processus concernés

Recenser l'ensemble des activités relevant du dispositif LBC/FT, notamment les procédures KYC, les contrôles internes, les audits, la surveillance des opérations, la gestion documentaire, la déclaration des opérations suspectes, les formations, les investigations, les incidents et les plans d'amélioration.

2. Identifier les fonctions et acteurs

Lister les organes de gouvernance, les directions, les responsables de conformité, les services opérationnels, les collaborateurs, les partenaires et toute autre partie prenante participant aux processus concernés.

3. Désigner le Responsable opérationnel (Responsible – R)

Attribuer à chaque activité la ou les personnes chargées de réaliser concrètement les tâches, d'exécuter les procédures et de produire les résultats attendus.

4. Désigner le Responsable décisionnaire (Accountable – A)

Identifier l'autorité qui approuve les décisions, valide les résultats, assume la responsabilité finale des actions entreprises et rend compte aux organes de gouvernance.

5. Identifier les personnes à consulter (Consulted – C)

Préciser les experts, responsables ou services dont l'avis technique, juridique, financier ou opérationnel doit être sollicité avant toute décision importante.

6. Identifier les personnes à informer (Informed – I)

Déterminer les personnes, services ou organes devant être informés des décisions prises, des résultats obtenus, des incidents ou des évolutions du dispositif de conformité.

7. Formaliser la matrice RACI

Présenter les responsabilités sous forme de tableau normalisé permettant une lecture rapide des rôles attribués à chaque acteur pour chaque processus.

8. Valider la répartition des responsabilités

Soumettre la matrice à la Direction Générale et aux organes de gouvernance afin de confirmer officiellement la répartition des responsabilités et d'assurer sa cohérence avec l'organisation interne.

9. Diffuser la matrice

Mettre la matrice à la disposition de tous les collaborateurs concernés afin qu'ils connaissent précisément leurs responsabilités et leurs obligations dans le cadre du dispositif LBC/FT.

10. Contrôler son application

Vérifier régulièrement que les responsabilités attribuées sont effectivement exercées, que les validations sont respectées et que les circuits décisionnels fonctionnent conformément aux procédures établies.

11. Réviser périodiquement la matrice

Actualiser la matrice lors de toute évolution organisationnelle, création d'un nouveau service, modification des responsabilités, évolution réglementaire ou amélioration des processus.

12. Archiver les différentes versions

Conserver les différentes versions validées de la matrice afin d'assurer la traçabilité des évolutions organisationnelles, de faciliter les audits et de démontrer la conformité du dispositif de gouvernance.

Contenu minimal de la Matrice RACI

La matrice devrait comporter au minimum les rubriques suivantes :

- Numéro du processus
- Activité ou procédure concernée
- Description de l'activité
- Responsable d'exécution (**R**)
- Responsable décisionnaire (**A**)
- Personnes consultées (**C**)
- Personnes informées (**I**)
- Direction ou service concerné
- Documents de référence
- Niveau de risque associé
- Fréquence d'exécution
- Date de validation
- Responsable de la mise à jour
- Observations
- Validation de la Direction Générale
- Validation du Responsable Conformité LBC/FT

Légende de la Matrice RACI

Sigle	Signification	Rôle
R	Responsable (Responsable d'exécution)	Réalise l'activité, exécute les tâches et produit les livrables attendus.
A	Accountable (Responsable décisionnaire)	Valide les décisions, approuve les résultats et assume la responsabilité finale du processus.
C	Consulted (Consulté)	Fournit un avis, une expertise ou une recommandation avant la prise de décision.
I	Informed (Informé)	Est tenu informé des décisions, de l'avancement ou des résultats, sans intervenir directement dans l'exécution.

Finalité de la matrice

La **Matrice des responsabilités (RACI)** constitue un référentiel de gouvernance indispensable au bon fonctionnement du dispositif LBC/FT de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. En clarifiant les responsabilités, les niveaux d'autorité et les circuits de communication, elle améliore la coordination entre les acteurs, renforce la transparence des processus décisionnels, réduit les risques d'erreur ou de duplication des tâches et favorise une meilleure redevabilité institutionnelle. Véritable outil de management et de contrôle interne, elle contribue à l'efficacité opérationnelle, à la qualité des audits, au respect des exigences réglementaires et à l'amélioration continue de la gouvernance, consolidant ainsi la confiance des membres, des partenaires, des bailleurs de fonds, des autorités de contrôle et de l'ensemble des parties prenantes.

ANNEXE O

LISTE DES DOCUMENTS DE RÉFÉRENCE

Description

La **Liste des documents de référence** constitue un document officiel de gouvernance documentaire intégré au dispositif de **lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT)** de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle recense l'ensemble des textes juridiques, réglementaires, normatifs, institutionnels, contractuels et opérationnels servant de fondement à l'élaboration, à l'application, au contrôle et à l'amélioration continue de la présente Politique LBC/FT.

Cette annexe a pour objectif de garantir que tous les collaborateurs disposent d'un référentiel documentaire unique, fiable et régulièrement actualisé. Elle facilite l'interprétation uniforme des exigences de conformité, favorise la cohérence des décisions et assure l'application harmonisée des règles de gouvernance, de contrôle interne, de gestion des risques et de sécurité financière au sein de l'Organisation.

La Liste des documents de référence comprend notamment les lois nationales applicables, les conventions internationales, les recommandations des organismes internationaux spécialisés, les procédures internes, les politiques institutionnelles, les manuels de gouvernance, les codes d'éthique, les guides opérationnels, les formulaires, les registres et tout autre document indispensable à la mise en œuvre du dispositif LBC/FT.

Elle constitue également un outil essentiel pour les audits, les inspections, les contrôles de conformité, les formations, les évaluations des risques et les missions de supervision. Son actualisation régulière permet d'intégrer les évolutions législatives, réglementaires, organisationnelles et techniques, garantissant ainsi la conformité permanente des activités de **AGCE International – AGCE Canada** avec les meilleures pratiques nationales et internationales.

Actions nécessaires

1. Identifier les documents applicables

Recenser l'ensemble des documents légaux, réglementaires, normatifs et institutionnels applicables aux activités de l'Organisation en matière de LBC/FT.

2. Classifier les documents

Organiser les documents par catégories afin d'en faciliter la consultation, notamment :

- Textes législatifs et réglementaires ;
- Normes internationales ;
- Politiques institutionnelles ;
- Procédures internes ;
- Manuels de gouvernance ;
- Registres et formulaires ;
- Guides opérationnels ;
- Contrats et conventions.

3. Attribuer une référence documentaire

Affecter à chaque document un numéro de référence, une version, une date d'approbation et un responsable de sa gestion afin d'assurer une identification unique et une traçabilité complète.

4. Vérifier la validité des documents

S'assurer que chaque document est en vigueur, officiellement approuvé, authentique et conforme aux exigences légales et institutionnelles applicables.

5. Assurer la disponibilité des documents

Mettre les documents de référence à la disposition des personnes habilitées au moyen d'un système documentaire sécurisé, organisé et facilement accessible.

6. Contrôler les versions

Mettre en œuvre un système de gestion des versions permettant d'éviter l'utilisation de documents obsolètes et de garantir que seule la version en vigueur est utilisée.

7. Diffuser les mises à jour

Informar rapidement les collaborateurs concernés de toute modification, création, suppression ou révision d'un document de référence ayant un impact sur les procédures ou les obligations de conformité.

8. Former les utilisateurs

Sensibiliser les collaborateurs à l'utilisation des documents de référence et à leur importance dans l'application quotidienne des politiques, procédures et contrôles internes.

9. Archiver les versions antérieures

Conserver les anciennes versions des documents conformément aux règles de gestion documentaire afin d'assurer la traçabilité des évolutions et de répondre aux besoins des audits ou des contrôles.

10. Réviser périodiquement la liste

Mettre à jour régulièrement la liste afin d'intégrer les nouveaux textes légaux, les nouvelles politiques internes, les procédures révisées et les documents récemment approuvés.

11. Contrôler la conformité documentaire

Vérifier que les documents référencés sont cohérents entre eux, correctement appliqués et conformes aux exigences réglementaires ainsi qu'aux objectifs de gouvernance de l'Organisation.

12. Assurer un suivi documentaire permanent

Désigner un responsable chargé du suivi de la documentation, de la veille réglementaire, de la mise à jour du registre documentaire et du contrôle de la diffusion des documents officiels.

Contenu minimal de la Liste des documents de référence

La liste devrait comprendre au minimum les rubriques suivantes :

- Numéro de référence du document
- Intitulé officiel du document
- Catégorie du document
- Objet ou finalité
- Version en vigueur
- Date d'approbation
- Date d'entrée en vigueur
- Date de la dernière révision
- Responsable du document
- Organe d'approbation
- Niveau de confidentialité
- Service utilisateur
- Fréquence de révision
- Localisation ou système d'archivage
- Statut (En vigueur – En révision – Archivé – Abrogé)
- Observations
- Validation du Responsable Conformité LBC/FT
- Validation de la Direction Générale

Catégories recommandées de documents de référence

La liste peut notamment inclure les catégories suivantes :

- Lois et règlements nationaux applicables à la LBC/FT ;
- Conventions et normes internationales ;
- Statuts et Règlement intérieur de l'Organisation ;
- Code d'éthique et d'intégrité ;
- Politique LBC/FT ;
- Manuel de contrôle interne ;
- Politique de gestion des risques ;
- Politique de protection des données ;
- Procédures KYC et de vigilance renforcée ;
- Procédures de déclaration des opérations suspectes ;
- Politique de protection des lanceurs d'alerte ;
- Charte des collaborateurs ;
- Registres institutionnels (contrôles, incidents, formations, audits) ;
- Rapports d'audit et de conformité ;
- Plans d'action et documents de gouvernance.

Finalité de la liste

La **Liste des documents de référence** constitue un référentiel documentaire essentiel au système de gouvernance de **ACTION GLOBALE CARITATIVE ET ÉCONOMIQUE-NUMÉRIQUE (AGCE International – AGCE Canada)**. Elle garantit une gestion rigoureuse des documents stratégiques, renforce la sécurité documentaire, facilite les audits et assure une application cohérente des exigences légales, réglementaires et institutionnelles. En offrant un accès structuré à l'ensemble des textes de référence, cette annexe favorise la transparence, la maîtrise des risques, la qualité des décisions et l'amélioration continue du dispositif de lutte contre le blanchiment de capitaux et le financement du terrorisme, tout en consolidant la confiance des autorités de contrôle, des partenaires, des bailleurs de fonds et de l'ensemble des parties prenantes.

Fait pour servir et faire valoir ce que de droit:

Fait à Douala le 20 Juillet 2026



Pour Action Globale Caritative et Economique-Numérique
(AGCE International - AGCE Canada)



Le Président Général

JOSUÉ SAMPA NKWENDJEU
PRÉSIDENT
(COORDINATEUR GÉNÉRAL)