Politique de protection des renseignements personnels du CCES

Numéro de la version : Version finale 1 approuvée par Jeremy Luke
Date d'entrée en vigueur : 1er janvier 2025

Table des matières

Aperçu

Ce document présente la politique de protection des renseignements personnels du Centre canadien pour l'éthique dans le sport (la « Politique de protection des renseignements personnels). Elle est divisée en quatre parties :

Partie 1	Présentation des politiques de protection des renseignements personnels qui s'appliquent au Centre canadien pour l'éthique dans le sport (CCES) en tant qu'organisme.
Partie 2 :	Présentation des politiques de protection des renseignements personnels qui s'appliquent précisément au Programme canadien antidopage du CCES.
Partie 3 :	Présentation des politiques de protection des renseignements personnels qui s'appliquent précisément au Programme canadien de sport sécuritaire du CCES.
Partie 4 :	Présentation des politiques connexes à la Politique de protection des renseignements personnels du CCES.

PARTIE 1 : POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS DU CCES

1.1 Introduction

Le Centre canadien pour l'éthique dans le sport est un organisme de réglementation. La présente politique de protection des renseignements personnels (la « Politique de protection des renseignements personnels ») présente le cadre général de protection de la vie privée qui s'applique à l'ensemble de l'organisme. On y distingue également les politiques qui s'appliquent au rôle du CCES dans le cadre du Programme canadien antidopage (le « **PCA** ») de celles qui s'appliquent au Programme canadien de sport sécuritaire (le « **PCSS** »).

La présente politique repose en partie sur le Standard international pour la protection des renseignements personnels (le « **SIPRP** ») de l'Agence mondiale antidopage (l'« **AMA** ») et elle est conforme aux politiques et aux principes énoncés dans la législation et la réglementation applicables. La raison d'être de la présente politique s'articule autour de quatre objectifs :

i. S'assurer que le PCA respecte en tous points les exigences de l'AMA en matière de protection de la vie privée;
ii. Se conformer pleinement aux lois et aux règlements canadiens applicables;
iii. Veiller au respect de l'ensemble des obligations contractuelles du CCES en matière de protection des données et de la vie privée découlant d'ententes avec des tierces parties;
iv. Faire en sorte que le CCES s'acquitte de ses responsabilités envers les personnes dont il recueille et conserve les renseignements personnels.

Le CCES s'engage également à prendre des mesures raisonnables pour s'assurer que les tierces parties qui reçoivent, collectent, conservent, sauvegardent, utilisent et détruisent des renseignements personnels au nom du CCES disposent de systèmes appropriés de protection de la vie privée et de gestion des données.

Se référer au SIPRP de l'AMA.

1.2 Définitions

Termes définis par le CCES

Employé, contractant ou bénévole du CCES : toute personne qui agit au nom du CCES dans le cadre de ses fonctions et qui participe au traitement de renseignements personnels.

Partenaire : un organisme tiers ou un client qui sollicite les services antidopage du CCES.

Renseignement personnel : toute information que le CCES obtient ou recueille et qui permet d'identifier la personne à qui elle appartient. Par souci de clarté, les rapports, les produits du travail et les renseignements générés par le CCES ne sont pas considérés comme des renseignements personnels.

Entente de service : tout arrangement ou contrat conclu avec une personne ou un organisme pour fournir au CCES un service nécessitant le traitement de renseignements personnels gérés

par le CCES ou un service antidopage nécessitant le traitement de renseignements personnels sur l'antidopage gérés par le CCES.

Sous-traitant : une entité dont les services fournis aux CCES impliquent le traitement de renseignements personnels dont le CCES est responsable.

D'autres définitions sont fournies dans le corps de la politique.

Les termes en italique dans la Partie 1 qui n'y sont pas autrement définis ont le sens qui leur est donné dans le SIPRP de l'AMA.

Termes définis dans le SIPRP de l'AMA qui s'appliquent au PCA :

Renseignements personnels liés à l'antidopage : Renseignements, y compris (sans s'y limiter) des *renseignements personnels sensibles*, relatifs à un *participant* identifié ou identifiable ou à une autre *personne* dont les renseignements sont traités uniquement dans le contexte d'*activités antidopage* d'une *organisation antidopage*. [Commentaire au sujet des *renseignements personnels liés à l'antidopage* : Il est entendu que les *renseignements personnels liés à l'antidopage* comprennent, sans s'y limiter, les renseignements relatifs au nom, à la date de naissance et aux coordonnées d'un *athlète*, ainsi que ses affiliations sportives, sa localisation, ses AUT (le cas échéant), ses résultats de contrôles du dopage et la *gestion des résultats* (y compris les audiences disciplinaires, les appels et les sanctions). Les *renseignements personnels liés à l'antidopage* comprennent en outre les coordonnées et les données personnelles relatives à d'autres *personnes*, telles que le personnel médical ou toute autre *personne* qui travaille avec l'*athlète*, le traite ou lui prête assistance dans le contexte des *activités antidopage*. De tels renseignements restent des *renseignements personnels liés à l'antidopage* et sont réglementés par le présent Standard international pendant toute la durée de leur *traitement*, que l'individu en question continue ou non d'être impliqué dans le sport organisé.] Par souci de clarté, les rapports, les produits du travail et les renseignements générés par le CCES ne sont pas considérés comme des *renseignements personnels liés à l'antidopage*.

Traitement (et termes apparentés tels que traiter ou traité(es)) : Collecte, accès, conservation, stockage, diffusion, transfert, transmission, modification, suppression ou toute autre utilisation de renseignements personnels.

Atteinte à la sécurité : Atteinte à la sécurité entraînant la perte, le vol, l'endommagement ou le *traitement* non autorisé et/ou illégal de *renseignements personnels liés à l'antidopage* sous forme électronique, imprimée ou autre, ou toute manipulation d'un système d'information de nature à compromettre la protection, la sécurité, la confidentialité, la disponibilité ou l'intégrité de *renseignements personnels liés à l'antidopage*.

Renseignements personnels sensibles : Renseignements personnels relatifs à l'origine raciale ou ethnique d'un *participant*, à des infractions (pénales ou autres) qu'il aurait pu commettre, à sa santé (notamment les renseignements tirés de l'analyse de prélèvements ou d'échantillons d'un *athlète*) et à ses informations biométriques et génétiques.

Tiers : Toute *personne* autre que la *personne* physique à laquelle se rapportent les *renseignements personnels liés à l'antidopage* pertinents, les *organisations antidopage* et les *tiers mandataires*.

Tiers mandataire : Toute *personne* qui *traite* des *renseignements personnels liés à l'antidopage* pour le compte d'une *organisation antidopage*, par délégation de celle-ci ou mandatée d'une autre façon par elle dans le contexte des *activités antidopage* de cette *organisation antidopage* y compris, mais sans s'y limiter, un *tiers délégué* et tout autre sous-traitant.

Définitions tirées du Standard international pour les contrôles et les enquêtes (SICE) de l'AMA

Autorité de contrôle : *Organisation antidopage* qui autorise les *contrôles* sur les *athlètes* relevant de sa compétence. Elle peut autoriser un *tiers délégué* à réaliser des *contrôles* en vertu de la compétence de l'*organisation antidopage* et conformément aux règles de celle-ci. Une telle autorisation doit être documentée. L'*organisation antidopage* qui autorise les *contrôles* demeure l'*autorité de contrôle* et en vertu du Code, il lui incombe en dernier ressort de veiller à ce que le *tiers délégué* effectue les *contrôles* dans le respect des exigences du Standard international pour les contrôles et les enquêtes.

1.3 Contexte

Agence antidopage du Canada, le CCES offre une foule de services antidopage. Il est responsable de la mise en œuvre du Programme canadien antidopage (le « **PCA** ») et fournit des services connexes à ses *partenaires* et ses clients, comme les fédérations sportives internationales et les grands jeux. La présente politique de protection des renseignements personnels porte en partie sur l'application du PCA et la prestation d'autres services antidopage.

Le CCES administre de façon indépendante le Code de conduite universel pour prévenir et contrer la maltraitance dans le sport (le « **CCUMS** ») à l'intention des organismes de sport de niveau national qui reçoivent des fonds fédéraux, et ce, par l'entremise du Programme canadien de sport sécuritaire (le « **PCSS** »). La présente politique de protection des renseignements personnels porte aussi en partie sur l'application du PCSS.

Dans le cadre du PCSS et du PCA, le CCES s'engage à gérer les *renseignements personnels* en conformité avec l'ensemble de la législation et de la réglementation applicables, des droits et obligations contractuels à l'égard de tiers en matière de confidentialité et de protection des données (notamment le consentement à la collecte, à l'utilisation ou à la divulgation de renseignements personnels), ainsi que ses responsabilités envers les personnes desquelles il recueille et conserve les *renseignements personnels*.

Le CCES s'engage également à traiter les *renseignements personnels liés à l'antidopage* et au PCA dans le respect du SIPRP de l'AMA. Il traite et gère différents types de *renseignements personnels liés à l'antidopage*, tantôt en tant qu'entité contrôlant les données (ou « responsable du contrôle des données »), tantôt pour le compte de *partenaires* et de clients (à titre de « responsable du traitement des données »). La partie II de la présente politique aborde ce sujet plus en détail.

1.4 Objectif et portée

La présente politique de confidentialité établit des politiques, des pratiques, des procédures et des systèmes permettant un traitement des *renseignements personnels* qui est conforme à la législation canadienne et, dans le cas du PCA, au SIPRP de l'AMA et aux exigences contenues dans les contrats conclus entre le CCES et ses divers *partenaires* (ensemble, les « obligations du CCES en matière de protection des renseignements personnels »). Dans les deux cas, le CCES souhaite

s'assurer qu'il a mis en place toutes les garanties appropriées pour protéger les informations personnelles dont il a la garde ou le contrôle. La présente politique, ou des parties de celle-ci :

- s'applique à l'ensemble des employés, des contractants et des bénévoles chargés de traiter des *renseignements personnels*;
- explique la façon dont ces personnes doivent traiter les *renseignements personnels* pour satisfaire aux *obligations du CCES en matière de protection des renseignements personnels*;
- régit la gestion et la destruction des *renseignements personnels*, définit les rôles et les responsabilités des employés, des contractants et des bénévoles du CCES tout au long du cycle de vie des renseignements et prévoit une procédure de traitement des plaintes concernant le traitement des *renseignements personnels*;
- s'applique aux *renseignements personnels* sous la garde ou le contrôle du CCES, y compris à ceux que le CCES transmet à des fournisseurs de services aux fins de traitement en son nom;
- s'applique aux *renseignements personnels* traités pour le compte de *partenaires*, même dans les cas où le CCES transfère ces renseignements à un *sous-traitant* aux fins de traitement;
- veille à ce que, pour le PCA, le CCES ne recueille que les *renseignements personnels* pertinents à sa mission de lutte contre le dopage, conformément au PCA et au Code mondial antidopage;
- veille à ce que, pour le PCSS et le CCUMS, le CCES ne recueille que les *renseignements personnels* pertinents à sa mission de promotion du sport sécuritaire, conformément au PCSS et au CCUMS.

Tous les employés, contractants et bénévoles qui traitent des *renseignements personnels* doivent se familiariser avec les aspects pertinents de la présente politique ou avec leurs procédures de travail précises pour connaître l'étendue de leurs responsabilités quant au *traitement* de *renseignements personnels* ou de documents connexes. Les employés, contractants ou bénévoles du CCES doivent traiter les *renseignements personnels* dans le respect de la présente politique. Les employés doivent être en mesure de guider les bénévoles, le conseil d'administration et les sous-traitants quant aux exigences en matière de *renseignements personnels* prévues dans leurs ententes avec le CCES. Les questions peuvent être adressées au responsable de la protection de la vie privée, qui s'appuiera sur l'expertise ou l'expérience appropriée pour guider les autres.

1.5 Responsable de la protection de la vie privée

Rôle du responsable de la protection de la vie privée : Le CCES désigne une personne responsable de la protection des *renseignements personnels* (le « **responsable de la protection de la vie privée** »). Son rôle consiste notamment à s'assurer que :

1. le CCES met en œuvre et respecte ses *obligations en matière de protection de la vie privée*;
2. la politique du CCES en matière de protection des renseignements personnels est conforme à la législation, à la réglementation et aux politiques de gouvernance applicables;
3. le CCES enquête sur les plaintes et les infractions, assure un suivi des dossiers et communique les résultats de ces enquêtes.

Les responsabilités précises liées au rôle sont énumérées ci-dessous.

Le *responsable de la protection de la vie privée* peut déléguer par écrit l'ensemble de ses fonctions ou une partie d'entre elles à d'autres employés du CCES. Les employés du CCES doivent transmettre toute demande ou plainte liée à la gestion des *renseignements personnels* au *responsable de la protection de la vie privée*, conformément à l'article 1.10 de la présente politique.

Le *responsable de la protection de la vie privée* supervise la mise en œuvre des autres politiques et procédures du CCES qui contribuent à la protection des *renseignements personnels*.

Toute demande ou plainte relative à la gestion des *renseignements personnels* doit être adressée au *responsable de la protection de la vie privée*. Les coordonnées du *responsable de la protection de la vie privée* sont indiquées ci-dessous.

Nomination du *responsable de la protection de la vie privée* : Le CCES doit désigner un *responsable de la protection de la vie privée* qui possède les qualifications, l'expertise et l'expérience requises en matière de protection de la vie privée et des données. Le *responsable de la protection de la vie privée* relève directement du président-directeur général.

Responsabilités du *responsable de la protection de la vie privée* :

1. Contrôle de la conformité :
    a. Veiller à ce que les politiques du CCES dans le cadre du PCA soient pleinement conformes aux exigences de l'AMA en matière de protection de la vie privée et à toutes les lois canadiennes applicables dans ce domaine.
    b. Faire le suivi des modifications apportées aux lois et règlements en matière de protection de la vie privée et mettre à jour la présente politique en conséquence.
2. Élaboration et mise en œuvre des politiques :
    a. Élaborer et mettre en œuvre des politiques, des procédures et des lignes directrices en matière de protection de la vie privée qui sont conformes à la présente politique, et les tenir à jour.
    b. Veiller à ce que toutes les politiques en matière de protection de la vie privée soient communiquées de manière efficace à l'ensemble du personnel concerné et comprises par celui-ci.
3. Analyses d'impact relatives à la protection des données :
    a. Réaliser des analyses d'impact relatives à la protection des données (« AIPD ») pour les nouveaux projets, systèmes ou processus qui impliquent le traitement de renseignements personnels.
    b. Identifier et atténuer les risques pour la vie privée associés aux activités de traitement des données.
4. Formation et sensibilisation :
    a. Créer des programmes de formation à la protection de la vie privée et les offrir aux employés, aux contractants et aux autres parties prenantes concernées.
    b. Promouvoir une culture de sensibilisation et de respect de la vie privée au sein de l'organisme.
5. Gestion des incidents et intervention en cas d'infraction :

   a. Établir des procédures pour repérer, signaler et gérer les fuites de données et les incidents de sécurité, et tenir ces procédures à jour.
   b. Diriger les enquêtes et les interventions en cas de fuite de données, et notamment informer les personnes touchées et les autorités réglementaires au besoin.
6. Gestion des demandes et des plaintes :
   a. Agir à titre de personne-ressource principale pour les demandes et les plaintes relatives à la protection de la vie privée formulées par des particuliers, des organismes de réglementation et d'autres parties prenantes.
   b. Veiller à ce que les demandes et les plaintes soient traitées rapidement et conformément aux procédures établies.
7. Tenue de dossiers et organisation :
   a. Tenir des registres précis des activités de traitement des données, des AIPD, des fuites de données et de toute autre documentation pertinente.
   b. Veiller à ce que les dossiers soient conservés conformément aux exigences légales et réglementaires.

Pouvoirs du *responsable de la protection de la vie privée* :

8. Accès à l'information :
   a. Accéder à l'ensemble de l'information et des ressources nécessaires pour s'acquitter efficacement de ses tâches.
   b. Effectuer des audits et des évaluations des activités de traitement des données afin de garantir le respect de la présente politique.
9. Prise de décisions :
   a. Prendre des décisions concernant la mise en œuvre de mécanismes et de mesures de protection de la vie privée visant à atténuer les risques repérés.
   b. Approuver les activités de traitement des données et rejeter celles qui ne sont pas conformes à la présente politique ou qui présentent des risques importants en matière de protection de la vie privée.
10. Rapports et responsabilité :
   a. Tenir à jour l'équipe de direction quant à la conformité en matière de protection de la vie privée, aux risques et aux incidents.
   b. Transmettre les problèmes importants liés à la protection de la vie privée à la haute direction et lui recommander des mesures correctives.

Soutien et ressources : Le CCES doit fournir au *responsable de la protection de la vie privée* le soutien et les ressources lui permettant de s'acquitter efficacement de ses responsabilités, notamment l'accès à de la formation, à des conseils juridiques et à des outils techniques nécessaires à la gestion de la vie privée.

Coordonnées du *responsable de la protection de la vie privée* : Les coordonnées du *responsable de la protection de la vie privée* sont accessibles en tout temps sur le site Web du CCES. Le personnel du CCES peut fournir aux personnes qui en font la demande les coordonnées du *responsable de la protection de la vie privée*.

On peut communiquer avec le *responsable de la protection de la vie privée* par courriel, à confidentialite@cces.ca.

L'aperçu de la présente politique doit être accessible au public sur le site Web du CCES et sur demande.

Le CCES doit rendre accessible, par le biais de la présente politique ou d'une autre manière :

i) une description du type de *renseignements personnels* recueillis et la raison de la collecte;
ii) les méthodes permettant aux *personnes* d'accéder à leurs *renseignements personnels* figurant dans les dossiers du CCES;
iii) les motifs justifiant la transmission de leurs renseignements personnels à des tiers, le cas échéant.

1.6 Contestation de la conformité

Réception des demandes et des plaintes : Toutes les demandes, préoccupations et plaintes relatives à la protection de la vie privée formulées par écrit doivent être transmises au *responsable de la protection de la vie privée* dès leur réception.

Gestion des demandes et des plaintes : Lorsqu'une *personne* fait une demande, signale une préoccupation ou dépose une plainte concernant une éventuelle violation de la vie privée commise par :

i) une partie – le *responsable de la protection de la vie privée* doit orienter la *personne* vers les dispositions pertinentes du PCA, du PCSS, du CCUMS ou de la présente politique;

ii) un contractant – le *responsable de la protection de la vie privée* doit orienter la *personne* vers la présente politique.

Le CCES est chargé d'enquêter sur les préoccupations soulevées et les plaintes déposées, à moins que le *responsable de la protection de la vie privée* estime qu'il existe des raisons suffisantes pour traiter la demande, la préoccupation ou la plainte d'une autre manière.

Le *responsable de la protection de la vie privée* doit procéder à l'examen initial des préoccupations et plaintes reçues dans un délai raisonnable. Dans tous les cas, le *responsable de la protection de la vie privée* doit informer la *personne* qui a formulé une préoccupation ou déposé une plainte de la progression de l'étude du dossier et de la date d'achèvement estimée.

Si la *personne* à l'origine de la préoccupation ou de la plainte juge que la résolution du cas est insatisfaisante, le CCES doit :

a) consigner le contenu non résolu de la préoccupation ou de la plainte dans les dossiers pertinents de la *personne*;
b) s'il y a lieu, informer les tiers ayant accès aux *renseignements personnels* concernés du fait que le cas est non résolu.

Atteinte à la vie privée : Sont notamment considérés comme une atteinte à la vie privée les vols et les pertes involontaires ou intentionnels de *renseignements personnels*, la collecte, l'utilisation ou la divulgation non autorisée de *renseignements personnels*, la modification ou la destruction non autorisée de renseignements personnels, ainsi que le non-respect de la présente politique.

Le *responsable de la protection de la vie privée* doit veiller, au minimum :

a) à limiter les dégâts, les vols et les pertes ainsi que l'utilisation ou la divulgation non autorisée de renseignements personnels;

b) à aviser rapidement les *personnes* touchées ou potentiellement touchées;

c) à enquêter sur les infractions, notamment en examinant les systèmes, les politiques, les pratiques et les procédures pertinentes;

d) à formuler des recommandations au président-directeur général pour remédier à la situation et, s'il y a lieu, pour imposer des mesures disciplinaires.

Le *responsable de la protection de la vie privée* doit tenir un registre des incidents et des signalements accompagnés des motifs et informer la *personne* à l'origine de la préoccupation ou de la plainte des résultats de l'enquête connexe.

Audit indépendant : Au besoin, le conseil d'administration du CCES peut lancer un audit indépendant de son propre respect de la politique.

1.7 Accès aux *renseignements personnels* et exactitude des données

Exactitude des données : Lorsqu'il agit en qualité de *responsable du contrôle des données*, le CCES doit veiller à ce que les *renseignements personnels* soient exacts, complets et à jour, dans la mesure où cela est nécessaire aux fins pour lesquelles les informations sont utilisées. Lorsque les *renseignements personnels* sont inexacts, incomplets ou obsolètes, le CCES doit les corriger et les mettre à jour, au besoin et sur demande. La modification des *renseignements personnels* dont il a la garde ou le contrôle doit advenir dans les plus brefs délais.

Réception des demandes d'accès : Les *personnes* qui interagissent avec le CCES seront informées de leurs droits d'accès indiqués dans la présente politique. Les employés du CCES qui reçoivent une demande d'une personne souhaitant obtenir des informations sur ses *renseignements personnels* détenus par le CCES ou y accéder doivent rediriger et transférer cette demande par courriel au *responsable de la protection de la vie privée*, qui traitera ladite demande conformément aux articles 1.5 et 1.10 de la présente politique.

Gestion des demandes d'accès : Le *responsable de la protection de la vie privée* ne traite que les demandes d'accès formulées par écrit et gère ces demandes selon la procédure décrite dans la présente section. Les demandes d'accès concernant le PCA doivent également être conformes aux articles 11.1 à 11.3 du SIPRP, qui contiennent des exigences détaillées selon le rôle.

- **En tant que *responsable du contrôle des données*** : Lorsque le *responsable de la protection de la vie privée* reçoit une demande d'accès en qualité de *responsable du contrôle des données*, il doit accuser réception de la demande dans un délai raisonnable et informer la personne derrière la demande de la manière dont il entend traiter le cas, et notamment de la méthode qu'il utilisera pour vérifier son identité, s'il y a lieu. L'accusé de réception doit demander :
    i) tout renseignement manquant pour identifier la personne derrière la demande (au besoin);

ii) toute précision permettant au CCES de trouver les renseignements demandés et de répondre adéquatement à la demande (p. ex., des détails sur les renseignements demandés).

- **En tant que *responsable du traitement des données* :** Lorsque le *responsable de la protection de la vie privée* reçoit une demande d'accès en qualité de *responsable du traitement des données*, il ne doit pas répondre à la demande, mais plutôt la transférer au *partenaire* concerné, puis informer la personne que sa demande a été transférée au *partenaire responsable du contrôle des données*.

- **Réponse aux demandes d'accès :** Le CCES doit transférer la demande à un *partenaire* ou y répondre et la traiter dans les 30 jours. S'il y a lieu, le *responsable de la protection de la vie privée* doit examiner les exigences et les considérations de l'article 11 (1-3) du SIPRP de l'AMA et fournir la réponse du CCES par écrit. Il examine si la demande peut être transférée à un *partenaire* ou acceptée ou refusée, en tout ou en partie, selon les circonstances détaillées dans le SIPRP de l'AMA, notamment dans le cas où divulguer ces renseignements à la personne qui en fait la demande révélerait :

  i) des *renseignements personnels* sur une tierce personne susceptibles de lui porter gravement préjudice;
  ii) des renseignements protégés par le privilège avocat-client ou le secret professionnel des avocats;
  iii) des renseignements susceptibles d'affecter une procédure judiciaire dans laquelle le CCES ou la personne qui fait la demande a un intérêt.

1.8 Externalisation du *traitement* des *renseignements personnels*

Externalisation : Dans les circonstances appropriées, le CCES peut transférer des *renseignements personnels* à des fournisseurs de services ou, lorsqu'il traite des *renseignements personnels* au nom d'un *partenaire*, à des *sous-traitants*. Le CCES doit protéger les *renseignements personnels* par voie contractuelle lorsqu'ils sont traités par des fournisseurs de services ou des *sous-traitants*, conformément à la présente section. Toutes les *ententes de services* impliquant le traitement de *renseignements personnels* par une tierce partie doivent être approuvées par le *responsable de la protection de la vie privée* du CCES.

Exigences contractuelles minimales/utilisation d'un modèle d'addenda sur le traitement des données : L'*entente de service* entre le CCES et le fournisseur de services ou le *sous-traitant* doit être conclue par écrit et contenir au minimum les éléments suivants : (i) l'obligation de respecter la législation applicable en matière de protection de la vie privée, ainsi qu'une description des mesures prises par le fournisseur de services ou le *sous-traitant* pour assurer la confidentialité des *renseignements personnels* (p. ex., la description des mécanismes de sécurité en place); (ii) l'obligation pour le fournisseur de services ou le *sous-traitant* de n'utiliser les *renseignements personnels* qu'aux fins de la prestation de services au CCES, de ne pas conserver ces informations après l'expiration ou la fin du contrat et de fournir au CCES, sur demande, une confirmation écrite du respect de cette exigence; (iii) l'obligation pour le fournisseur de services ou le *sous-traitant* d'aviser sans délai le *responsable de la protection de la vie privée* du CCES de toute violation réelle

ou tentative de violation de la sécurité et de permettre au *responsable de la protection de la vie privée* de vérifier le respect des exigences en matière de sécurité des données. S'il y a lieu, et dans la mesure du possible, le CCES doit conclure un addenda sur le traitement des données avec les fournisseurs de services ou les *sous-traitants* en qualité de *responsable du contrôle des données*.

Exigences en matière de sous-traitance : Avant de transmettre des *renseignements personnels* à un *sous-traitant*, le CCES doit s'assurer qu'il est autorisé à le faire en vertu de son contrat avec le *partenaire* concerné. Même si la sous-traitance est autorisée, il se peut que le contrat avec le *partenaire* concerné exige du CCES qu'il ajoute des protections supplémentaires (en plus des exigences contractuelles minimales mentionnées ci-dessus) dans ses contrats avec les *sous-traitants*.

Surveillance continue : Le CCES peut s'octroyer divers droits de contrôle et de surveillance dans le cadre d'un accord contractuel avec un fournisseur de services ou un *sous-traitant*, tel que le droit de demander au fournisseur de services de fournir des rapports, de l'information et des certifications, ainsi que le droit de mener des audits ou des enquêtes sur le fournisseur de services. L'employé du CCES responsable d'élaborer de l'*entente de service* doit régulièrement tirer parti de ces droits pour évaluer la conformité du fournisseur de services ou du *sous-traitant* et pour signaler immédiatement au *responsable de la protection de la vie privée* tout incident ou événement ayant affecté, ou étant susceptible d'affecter, la sécurité, la confidentialité, l'intégrité ou la disponibilité de tout *renseignement personnel*.

Résiliation d'une entente d'externalisation : Au terme de l'*entente de service*, l'employé du CCES qui supervise le contrat doit s'assurer que le fournisseur de services renvoie tous les *renseignements personnels* au CCES, qu'il supprime ou détruise sécuritairement tout enregistrement des données du CCES en sa possession ou sous son contrôle et qu'il remette une confirmation écrite de sa conformité aux exigences du CCES. L'employé doit en outre prendre des mesures pour gérer les risques liés à la sécurité des renseignements lorsqu'une *entente de service* prend fin, y compris, par exemple, l'annulation des identifiants d'un fournisseur de services lui permettant d'accéder à distance aux systèmes et aux *renseignements personnels* du CCES.

1.9 Sécurité des renseignements et *atteinte à la sécurité*

Sécurité des renseignements : Le CCES doit adopter des mesures de sécurité appropriées pour protéger les *renseignements personnels* dont il a la garde ou le contrôle. Tous les employés, contractants et bénévoles du CCES doivent faire preuve de prudence et d'attention lors du traitement des *renseignements personnels* et adopter des mesures de sécurité appropriées (physiques, organisationnelles et technologiques) pour les protéger conformément à la présente politique et aux autres politiques et procédures pertinentes du CCES. Précisément, l'accès des employés, des contractants et des bénévoles du CCES aux *renseignements personnels* est limité à ce qui est nécessaire pour exécuter leurs tâches, et dans le cas des fournisseurs de services, des *sous-traitants*, des conseillers ou des autres *tiers* auxquels le CCES est autorisé à transmettre ces renseignements, l'accès est limité aux personnes qui en ont véritablement besoin dans le cadre de leur mandat pour le CCES et uniquement dans la mesure nécessaire à l'accomplissement de ce mandat.

Atteinte à la sécurité : Il y a *atteinte à la sécurité* en cas de perte, de destruction ou d'altération des *renseignements personnels*, ou en cas d'accès non autorisé ou de divulgation des *renseignements personnels*. Exemples :

- **Divulgation accidentelle :** Les *renseignements personnels* sont divulgués à quelqu'un par accident. Par exemple : (i) un courriel ou une lettre contenant des *renseignements personnels* est envoyé à une mauvaise adresse en raison d'une erreur mécanique ou humaine; (ii) des renseignements personnels sont publiés en ligne par le CCES à la suite d'un problème technique.
- **Perte :** Les *renseignements personnels* sont perdus. Par exemple, un employé du CCES perd son ordinateur portable, son appareil mobile ou son sac à dos contenant des *renseignements personnels*.
- **Accès ou divulgation non autorisés :** Une personne non autorisée consulte ou reçoit des *renseignements personnels*, ou les renseignements sont divulgués d'une manière non autorisée ou à des fins non autorisées, notamment en violation des politiques, des procédures ou des contrats de partenariat applicables du CCES.

Signalement des *atteintes à la sécurité* au sein du CCES : Les employés, les contractants et les bénévoles du CCES doivent faire preuve de vigilance quant aux failles des mécanismes de sécurité et signaler immédiatement toute faille réelle ou raisonnablement suspectée au *responsable de la protection de la vie privée*. Le signalement immédiat d'une *atteinte à la sécurité* réelle ou suspectée permettra à ce dernier d'enquêter et de réagir rapidement à la violation, afin de protéger le CCES et l'ensemble des personnes et organismes concernés. Plus le CCES agira rapidement en cas d'*atteinte de la sécurité*, plus il sera en mesure de contenir efficacement l'atteinte ainsi que d'éviter et d'atténuer les dommages qui en résultent.

Confirmation de l'*atteinte à la sécurité* : Le *responsable de la protection de la vie privée* doit examiner tout rapport d'*atteinte à la sécurité* porté à son attention en menant sur-le-champ une évaluation globale de la situation pour déterminer si l'incident suspecté constitue réellement une *atteinte à la sécurité*. Si l'*atteinte à la sécurité* est confirmée, il faut prendre les mesures suivantes :

- **Étape 1 : Créer une équipe de gestion de l'atteinte.** Le *responsable de la protection de la vie privée* doit former une équipe de gestion de l'atteinte idéalement constituée de membres ayant des connaissances ou une expertise pertinentes au mandat de l'équipe. Parallèlement, l'avocat général du CCES et la direction générale des services généraux aviseront les assureurs du CCES.

- **Étape 2 : Contenir les dommages.** L'équipe de gestion de l'atteinte doit contenir sur-le-champ l'*atteinte à la sécurité* par les mesures suivantes : (i) corriger la faille, y compris, le cas échéant, en mettant fin à l'activité non autorisée, en récupérant tous les documents concernés, en arrêtant le système ou en bloquant l'accès au système lié à l'atteinte, en révoquant ou modifiant les codes d'accès informatiques, en colmatant les failles de sécurité physique ou électronique, ou en prenant toute autre mesure corrective appropriée; (ii) protéger l'enquête en conservant en lieu sûr tous les éléments de preuve qui pourraient servir à déterminer la cause de l'atteinte, y compris, le cas échéant, en

clonant les appareils électroniques, en sauvegardant les courriels et en envoyant un avis de mise en suspens pour litige ou de conservation de documents aux *employés* concernés.

- **Étape 3 : Enquêter.** L'équipe de gestion de l'atteinte doit coordonner l'enquête et confirmer les risques posés par la faille, établir un plan d'action pour l'enquête, coordonner la mise en œuvre du plan d'action et superviser la rédaction du rapport d'enquête. Elle doit également superviser le processus de résolution, gérer tous les risques associés à l'atteinte, examiner le rapport d'enquête, et s'assurer que l'*atteinte à la sécurité* a fait l'objet d'une enquête approfondie, qu'elle est suffisamment documentée et que l'affaire a été résolue adéquatement.

- **Étape 4 : Trouver les parties à aviser.** Le *responsable de la protection de la vie privée* doit déterminer s'il a l'obligation légale (ou s'il est autrement approprié) d'envoyer une déclaration aux autorités de réglementation en matière de protection de la vie privée ainsi qu'un avis aux personnes concernées, en examinant si l'*atteinte à la sécurité* présente un risque réel de préjudice important (ou un critère similaire en vertu du droit applicable) pour les personnes concernées et en tenant compte de la sensibilité des informations concernées, des conséquences potentielles de leur utilisation et de la probabilité que ces informations soient utilisées à des fins préjudiciables. Le *responsable de la protection de la vie privée* doit également déterminer s'il a l'obligation légale ou contractuelle d'aviser des parties externes, notamment (i) des *partenaires* (en cas d'*atteinte à la sécurité* touchant les *renseignements personnels* auxquels le CCES a eu accès en tant que *responsable du traitement des données*), des fournisseurs de services ou des *sous-traitants*, selon le cas (si cela est requis par contrat); (ii) les forces de l'ordre (si l'on présume un vol ou un autre délit); (iii) les assureurs ou d'autres parties (si le contrat l'exige ou si l'atteinte est assurable); (iv) des ordres professionnels ou autres organismes de réglementation (le cas échéant); (v) le commissaire à la protection de la vie privée, si le CCES l'estime nécessaire.

- **Étape 5 : Documenter la décision en matière d'avis.** Le *responsable de la protection de la vie privée* doit documenter ses décisions en matière d'avis, comme indiqué à l'étape 4 ci-dessus. Il doit notamment exposer les grandes lignes de sa décision d'aviser ou non une personne concernée ou de signaler l'atteinte à un tiers, aux forces de l'ordre, aux assureurs ou à d'autres parties, à des ordres professionnels ou à d'autres organismes de réglementation, ainsi qu'au commissaire à la protection de la vie privée.

Consignation de l'atteinte : Le *responsable de la protection de la vie privée* doit veiller à ce que toutes les *atteintes à la sécurité* soient documentées et enregistrées dans un système centralisé, quelle que soit la cause ou la source de l'atteinte. Il peut rassembler tous les cas dans la base de données des *atteintes à la sécurité* et utiliser le modèle de consignation des atteintes, lequel est disponible sur demande auprès du CCES.

1.10 Organismes de réglementation, forces de l'ordre/gouvernement et procédure judiciaire

Organismes de réglementation : Les employés du CCES qui reçoivent d'un organisme de réglementation un message au sujet de la gestion de *renseignements personnels* doivent immédiatement en informer le *responsable de la protection à la vie privée* afin qu'il prenne les

mesures appropriées au nom du CCES. Le *responsable de la protection de la vie privée* est le point de contact unique pour toute correspondance et communication avec l'organisme de réglementation. Il peut consulter et solliciter l'aide d'autres employés du CCES au besoin, conformément aux politiques et aux lignes directrices applicables du CCES. Sauf indication contraire du *responsable de la protection de la vie privée*, les employés du CCES ne sont pas autorisés à répondre à des communications avec des organismes de réglementation.

Forces de l'ordre, gouvernement et procédure judiciaire : Les employés du CCES qui reçoivent des communications des forces de l'ordre ou d'une agence gouvernementale demandant l'accès à des *renseignements personnels*, ou bien une citation à comparaître ou une demande judiciaire similaire d'accès à des *renseignements personnels*, doivent immédiatement en informer le *responsable de la protection de la vie privée*, qui est chargé de répondre à ce type de demandes. Sauf indication contraire du *responsable de la protection de la vie privée*, les employés du CCES ne sont pas autorisés à répondre à des communications avec les forces de l'ordre ou une agence gouvernementale concernant l'accès à des *renseignements personnels*.

Demandes ou plaintes déposées auprès du CCES

Les personnes qui estiment qu'il y a eu violation de la présente politique ou du SIPRP, selon le cas, sont invitées à envoyer au *responsable de la protection de la vie privée* une lettre confidentielle (par la poste ou sous forme de pièce jointe à un courriel protégée par un mot de passe), avec les détails de leur préoccupation ou de leur plainte, aux adresses suivantes :

Courriel : confidentialite@cces.ca
Numéro sans frais : 1 800 672 7775
Adresse postale : 201-2723, chemin Lancaster
Ottawa (Ontario) K0B 0B1

En outre, les employés du CCES qui reçoivent une demande de renseignements ou une plainte relative au traitement de renseignements personnels doivent rapidement signaler ladite plainte au *responsable de la protection de la vie privée* en y indiquant le nom de la personne et ses coordonnées (le cas échéant). Sauf indication contraire du *responsable de la protection de la vie privée*, les employés du CCES ne sont pas autorisés à répondre à des communications avec une personne à l'origine d'une plainte.

Soutien et sanctions

Soutien et conseils : Les employés, contractants ou bénévoles du CCES qui ont des doutes sur l'application de la présente politique – ou du SIPRP dans le cadre du PCA – ou qui se demandent si une pratique va à l'encontre de la présente politique doivent demander conseil au *responsable de la protection de la vie privée*.

Sanctions : Tous les employés du CCES qui ont affaire avec le PCA sont tenus de se conformer au SIPRP de l'AMA en plus de la présente politique. Tout employé du CCES qui enfreint la présente politique, ou le SIPRP s'il a affaire avec le PCA, s'expose à des mesures disciplinaires pouvant aller jusqu'au congédiement.

1.11 Modifications à la présente politique

La présente politique doit être revue et mise à jour régulièrement afin de garantir sa pertinence et son efficacité. Cela permet d'assurer une gestion des changements claire et structurée, d'assurer la participation des parties prenantes et de maintenir la conformité avec la législation, la réglementation et les politiques d'autres organismes, comme l'AMA, en matière de protection de la vie privée. La présente politique, qui fait régulièrement l'objet d'une révision et occasionnellement l'objet de changements, est accessible sur le réseau du CCES.

Participation des parties prenantes : Diverses parties prenantes prennent part au processus de révision et de mise à jour, notamment :

- le *responsable de la protection de la vie privée*;
- les équipes juridiques et de conformité concernées;
- l'équipe de sécurité des renseignements;
- la direction des services concernés;
- des spécialistes externes de la protection de la vie privée (au besoin).

Processus de gestion des modifications : Le processus de mise à jour de la présente politique suit les étapes suivantes :

1. **Détermination des modifications à apporter :** Les changements à effectuer peuvent découler de mises à jour législatives, de directives réglementaires, d'audits internes, d'évaluations des risques ou de rétroaction de la part des parties prenantes.
2. **Analyse d'impact :** Une analyse d'impact doit être réalisée afin d'évaluer les effets potentiels des modifications proposées sur les pratiques de l'organisme en matière de protection de la vie privée et sur ses obligations de conformité.
3. **Rédaction des modifications :** Le *responsable de la protection de la vie privée*, en collaboration avec les parties prenantes concernées, doit rédiger les modifications proposées à la présente politique. Dans cette version provisoire, les changements doivent être justifiés et accompagnés de la documentation connexe pertinente.
4. **Examen et approbation :** Les modifications proposées sont ensuite examinées par le président-directeur général afin de s'assurer qu'ils sont conformes aux lois et aux règlements applicables. La version finale doit aussi être soumise au président-directeur général pour approbation.
5. **Communication et formation :** Une fois approuvée, la politique mise à jour est transmise à l'ensemble du personnel concerné. Des séances de formation doivent être organisées pour veiller à ce que tout le monde comprenne les changements et s'y conforme.
6. **Documentation et tenue de dossiers :** Toutes les modifications apportées à la présente politique doivent être documentées, notamment au moyen des justifications de ces changements, des analyses d'impact et des processus d'approbation. Il est important de conserver ces dossiers aux fins d'audit et de conformité.

Mises à jour urgentes : En cas de changements juridiques ou réglementaires importants qui nécessitent une action immédiate, le *responsable de la protection de la vie privée* est autorisé à apporter des modifications temporaires à la présente. Le président-directeur général doit ensuite examiner et ratifier ces mises à jour urgentes dans les plus brefs délais.

Contrôle de version : Chaque version de la présente politique de protection des renseignements personnels doit être clairement numérotée et datée. Un historique des versions contenant la date d'entrée en vigueur et un sommaire des changements doit être créé, de façon à suivre les modifications apportées.

Amélioration continue : Le CCES s'engage à améliorer continuellement ses pratiques en matière de protection de la vie privée. La rétroaction à la suite des audits, les évaluations des risques et les commentaires des parties prenantes permettent de cerner les points à améliorer et de guider les mises à jour subséquentes de la présente politique.

Politiques, procédures et lignes directrices connexes du CCES

Veuillez également tenir compte des politiques et procédures suivantes, en plus des annexes :

- SIPRP de l'AMA
- Délais de conservation (annexe A du SIPRP de l'AMA, index des fichiers qualité, activités de l'organisme)

La présente politique a été mise à jour le 1er janvier 2025.

PARTIE 2 : POLITIQUE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS PROPRE AU PCA

2.1 Compétence et application

À titre d'agence antidopage nationale du Canada, le CCES est responsable d'administrer le Programme canadien antidopage (PCA). Ce faisant, le CCES doit s'assurer que les *renseignements personnels liés à l'antidopage* traités dans le cadre de ses activités antidopage sont protégés conformément aux lois, aux principes et aux normes de protection des données applicables.

Le CCES doit également se conformer aux dispositions du SIPRP de l'AMA comme intégrées au PCA.

La présente politique établit, en termes généraux, la façon dont les renseignements personnels aux fins de la lutte contre le dopage sont traités par le CCES dans le cadre de l'administration et de la mise en œuvre du PCA.

2.2 Définitions propres au PCA

Responsable du contrôle des données : lorsque le CCES traite et gère des renseignements personnels pour son propre compte. Pour en savoir plus, consultez la Politique de protection des renseignements personnels du CCES.

Responsable du traitement des données : lorsque le CCES fournit à un *partenaire* ou à un client (comme des fédérations sportives internationales ou de grands jeux) des services de traitement et de gestion des *renseignements personnels*.

2.3 Types de *renseignements personnels liés à l'antidopage*

Voici certains types de *renseignements personnels liés à l'antidopage* :

- l'identité (à savoir, le nom, la nationalité, la date de naissance, le genre, l'événement, le niveau de compétition, les affiliations, les noms et les coordonnées d'autres personnes, comme les professionnels de la santé qui travaillent, de loin ou de près, avec la personne dans un contexte sportif ou de lutte contre le dopage);
- les renseignements sur la localisation;
- les exemptions médicales, y compris les autorisations d'usage à des fins thérapeutiques (AUT) et les évaluations du dossier médical;
- les contrôles du dopage (incluant la planification de la répartition des contrôles, le prélèvement et la manipulation des échantillons, les résultats des contrôles du dopage, les analyses en laboratoire, la gestion des résultats, les audiences, les sanctions et les appels).

Les *renseignements personnels liés à l'antidopage* peuvent aussi comprendre des renseignements personnels délicats, notamment ceux qui ont trait à la race, à l'ethnie, à la génétique, à la médecine ou à la biologie (y compris des renseignements provenant de l'analyse des échantillons ou des spécimens) et la commission d'infractions.

2.4 Entité de collection

Le CCES, un autre organisme ou un organisme antidopage auquel le CCES aura conféré l'autorité d'effectuer des *contrôles* du dopage et de prélever des échantillons conformément au PCA ou qui détient l'autorité nécessaire pour effectuer des contrôles du dopage et prélever des échantillons chez une personne recueillera des *renseignements personnels liés à l'antidopage* de différents types.

2.5 Fins pour lesquelles vos *renseignements personnels liés à l'antidopage* peuvent être traités

Le CCES et ses agents traiteront uniquement les *renseignements personnels liés à l'antidopage* recueillis quand il est nécessaire et approprié de réaliser des activités de lutte contre le dopage en vertu du PCA et des standards internationaux de l'AMA ou quand une loi applicable l'exige et aucun conflit n'existe entre les lois de protection de la confidentialité et des données applicables. Ces renseignements seront notamment traités pour :

- déterminer l'admissibilité à une AUT;
- effectuer des contrôles du dopage, y compris des contrôles ciblés, et pour documenter les résultats de ces contrôles;
- mener des enquêtes visant à déterminer les violations potentielles des règles du PCA;
- gérer les résultats en vertu du PCA, y compris les audiences, les appels et les décisions disciplinaires connexes, et pour publier les résultats.

2.6 Divulgations

Le CCES peut divulguer des *renseignements personnels liés à l'antidopage* à des agents, y compris les fournisseurs de services autorisés, liés aux activités de lutte contre le dopage du CCES comme indiqué dans le PCA.

Les *renseignements personnels liés à l'antidopage* ne seront pas divulgués à d'autres organismes antidopage, sauf si de telles divulgations sont nécessaires pour permettre à ces organismes d'effectuer leurs activités de lutte contre le dopage en vertu du PCA ou du Code mondial antidopage (Code) et conformément aux lois de protection de la confidentialité et des données applicables.

Les *renseignements personnels liés à l'antidopage* ne seront pas divulgués à des tierces parties autres que celles indiquées ci-dessus, sauf si de telles divulgations sont :

- prescrites par la loi;
- faites avec un consentement éclairé, exprès ou écrit;
- nécessaires pour aider les organismes d'application de la loi ou les autorités gouvernementales dans la détermination, l'analyse ou la poursuite d'un délit criminel ou d'une violation des règles du PCA, à condition que les *renseignements personnels liés à l'antidopage* exigés soient directement liés au délit ou à la violation en question et qu'ils ne puissent être obtenus autrement par les autorités.

2.7 Transferts internationaux

Le CCES peut mettre des *renseignements personnels liés à l'antidopage* à la disposition de tiers, y compris des fournisseurs de services autorisés, l'AMA et les organismes antidopage, dont certains peuvent être situés à l'extérieur du Canada.

Transferts transfrontaliers : Avant de transférer des *renseignements personnels liés à l'antidopage* à l'extérieur du Canada, le CCES doit :

- s'il agit à titre de *responsable du traitement des données*, s'assurer que son contrat avec le *partenaire* n'interdit pas un tel transfert;
- s'il agit à titre de *responsable du contrôle des données*, s'assurer que les personnes concernées sont au courant que leurs *renseignements personnels liés à l'antidopage* pourraient être transférés à l'extérieur du Canada;
  dans tous les cas, s'assurer que les mesures de sécurité techniques utilisées pour transférer les *renseignements personnels liés à l'antidopage* sont adaptées au degré de sensibilité des renseignements, à la procédure du CCES sur la sécurité de l'information et au SIPRP.

2.8 Droits relatifs au respect des *renseignements personnels liés à l'antidopage*

Droit d'accéder aux *renseignements personnels liés à l'antidopage* : Les personnes ont le droit de solliciter auprès du CCES des *renseignements personnels liés à l'antidopage* les concernant (les catégories de renseignements, les raisons pour lesquelles ces renseignements sont recueillis et les tiers ou les catégories de tiers à qui ils sont transmis), de savoir si ces renseignements sont en cours de traitement ou non et de recevoir dans un délai raisonnable (un mois suivant la demande) une copie des *renseignements personnels* pertinents dans un format facilement lisible, à moins qu'un cas en particulier compromette la capacité du CCES à planifier ou à effectuer des contrôles du dopage en vertu du PCA (incluant les contrôles ciblés) ou à enquêter sur des violations des règles antidopage ou à les établir.

Le CCES peut refuser de répondre aux demandes d'accès aux *renseignements personnels liés à l'antidopage* si leur envergure ou leur fréquence est excessive ou si elles imposent un fardeau disproportionné au CCES en matière de coût ou d'effort étant donné la nature des renseignements en question. Si le CCES refuse l'accès aux *renseignements personnels liés à l'antidopage*, il devra en aviser le demandeur et lui expliquer par écrit les motifs de son refus dans les meilleurs délais.

Droit de modifier les *renseignements personnels liés à l'antidopage* : Les *renseignements personnels liés à l'antidopage* que le CCES traite seront précis, complets et à jour. Si le CCES réalise que les *renseignements personnels liés à l'antidopage* qu'il traite sont imprécis ou incomplets, il les rectifiera, modifiera, complétera, mettra à jour ou supprimera dès que possible. Le cas échéant, si les *renseignements personnels liés à l'antidopage* en question ont été divulgués à un tiers qui semble continuer de les traiter, le tiers devra être informé des modifications dès que possible.

Droit de s'opposer au traitement des *renseignements personnels liés à l'antidopage* : Les personnes ont le droit de s'opposer au traitement de leurs *renseignements personnels liés à l'antidopage*, même si, dans un tel cas, le CCES ou des tiers peuvent devoir continuer de traiter

(y compris de retenir) certains de ces renseignements afin de remplir leurs obligations et leurs responsabilités en vertu du PCA ou des lois applicables.

S'opposer à la divulgation ou au traitement des *renseignements personnels liés à l'antidopage* peut être interprété comme un refus de participation et peut entraîner une violation des règles antidopage. Le refus de permettre au CCES de traiter convenablement les *renseignements personnels liés à l'antidopage* recueillis pourrait faire en sorte que la personne ne se conforme pas au PCA et doive faire face aux conséquences y étant liées.

Droit de porter plainte : Les personnes peuvent porter plainte si elles ont de bonnes raisons de croire que le CCES ne se conforme pas au PCA, au Standard international de l'AMA ou à toute loi applicable liée à la protection de la confidentialité. La plainte doit être déposée auprès du CCES, à l'adresse confidentialite@cces.ca.

2.9 Traitement des *renseignements personnels liés à l'antidopage*

Traitement des *renseignements personnels liés à l'antidopage* à titre de *responsable du contrôle des données*

Cette section énonce les règles fondamentales que le CCES doit suivre quant au traitement de *renseignements personnels liés à l'antidopage* lorsqu'il agit en qualité de *responsable du contrôle des données*.

Transparence : Le CCES doit adopter et mettre en œuvre une politique externe de protection des renseignements personnels (la Politique de confidentialité et de protection des renseignements personnels du PCA) qui précise les éléments suivants dans un langage clair et simple :

(i) Les objectifs de la collecte de *renseignements personnels liés à l'antidopage* auprès des personnes qui interagissent avec le CCES par le biais du PCA ou d'autres programmes antidopage conformes à l'AMA;
(ii) La manière dont les renseignements sont recueillis;
(iii) Les droits pour les personnes visées par la collecte d'accéder à leurs renseignements personnels et de les corriger;
(iv) Le droit de refuser que les *renseignements personnels liés à l'antidopage* recueillis soient communiqués ou utilisés;
(v) S'il y a lieu, les tierces parties pour lesquelles le CCES recueille les *renseignements personnels* ainsi que l'indication que les renseignements pourraient être transférés à l'extérieur du Canada. La Politique de confidentialité et de protection des renseignements personnels du PCA doit être accessible facilement et en tout temps sur le site Web du CCES.

Consentement : Conformément à la présente politique, le CCES n'utilisera ou ne divulguera les *renseignements personnels liés à l'antidopage* qu'aux fins pour lesquelles ils ont été recueillis, à moins que la personne concernée n'ait donné son consentement ou que les lois pertinentes sur la protection des données ou le Code mondial antidopage ne l'autorisent. Le CCES doit obtenir le consentement exprès pour traiter des *renseignements personnels délicats liés à l'antidopage*.

Fins du traitement : Conformément à la présente politique, le CCES n'utilisera les *renseignements personnels liés à l'antidopage* qu'aux fins lui permettant de respecter ses obligations en matière de protection de la vie privée.

Partage de *renseignements personnels liés à l'antidopage* : Les parties prenantes du CCES ne communiqueront les *renseignements personnels liés à l'antidopage* à un *sous-traitant* ou à un fournisseur de services que si le traitement des renseignements par ce sous-traitant ou fournisseur de services est régi par un contrat approprié, conformément à l'article 1.8 de la présente politique. Toute demande émanant d'un organisme de réglementation, d'une autorité gouvernementale, des forces de l'ordre ou d'un autre tiers pour accéder à des *renseignements personnels liés à l'antidopage* détenus par le CCES sera immédiatement transmise au *responsable de la protection de la vie privée*, qui répondra à cette demande conformément aux articles 1.5 et 1.10 de la présente politique.

Traitement des *renseignements personnels liés à l'antidopage* à titre de *responsable du traitement des données*

Entente sur le *traitement* des données : Le CCES ne *traitera* que les *renseignements personnels liés à l'antidopage* confiés par des *partenaires* (qui sont généralement des *autorités de contrôle* selon le Standard international pour les contrôles et les enquêtes de l'AMA) pour des projets précis faisant l'objet d'un accord écrit qui prévoit au minimum (i) l'obligation pour le CCES de n'utiliser les *renseignements personnels liés à l'antidopage* qu'aux fins de la prestation de services au *partenaire*, et de ne pas conserver ces informations après l'expiration ou la résiliation du contrat, sous réserve des exigences légales en matière de conservation des données; (ii) l'obligation pour le CCES de protéger ces *renseignements personnels liés à l'antidopage* par des mesures de sécurité adéquates (voir l'article 1.9); et (iii) l'obligation pour le CCES d'aviser sans délai le *partenaire* de toute atteinte à la sécurité.

Utilisation du modèle : Les *ententes de services* conclues avec les *partenaires* doivent être accompagnées du modèle d'addenda sur le traitement des données. L'équipe interne du CCES responsable de l'entente avec le *partenaire* exigera que cet addenda sur le traitement des données soit conclu ou autrement, qu'un document équivalent préparé par le *partenaire* et acceptable pour le CCES soit signé par les parties.

2.10 Conservation et destruction des *renseignements personnels*

Exigences générales en matière de conservation : Les *renseignements personnels liés à l'antidopage* que le CCES gère en qualité de *responsable du traitement des données* doivent être conservés selon les modalités du contrat en vigueur et des directives fournies par le *partenaire*. Les *renseignements personnels liés à l'antidopage* que le CCES gère en qualité de *responsable du contrôle des données* doivent être conservés selon les modalités de la présente section et de la partie 2 de la présente politique.

Délais de conservation du PCA : Le CCES conserve les *renseignements personnels liés à l'antidopage* aussi longtemps que nécessaire pour atteindre les objectifs du SIPRP de l'AMA pour lesquels il les a initialement recueillis et conformément à l'annexe A du SIPRP. Plus précisément, sous réserve de la sous-section « Suspension de la destruction ou de l'élimination des dossiers », les dossiers comprenant des *renseignements personnels liés à l'antidopage* ne doivent pas être conservés au-delà du délai prescrit.

- ***Partenaires* :** Les *renseignements liés à l'antidopage* des *partenaires* sont généralement conservés pendant au moins trois ans après la fin du partenariat.

- ***Atteinte à la sécurité*** **:** les données en lien avec une *atteinte à la sécurité* (pour en savoir plus, voir l'article 1.9 de la présente politique) doivent être conservées pendant au moins deux ans après l'incident.
- **Demandes d'accès :** Après avoir traité une demande d'accès et y avoir répondu conformément à l'article 1.7, le CCES conservera les données suivantes pour une période minimale de trois ans : la date et la nature de la demande, la manière dont la demande a été soumise, la date et la nature de la réponse du CCES et, le cas échéant, la raison pour laquelle la demande a été rejetée en tout ou en partie. Si le CCES rejette en tout ou en partie une demande d'accès ou de modification, il doit conserver les données connexes, sous réserve de toute période de conservation plus longue prévue par la présente politique, pendant le temps nécessaire pour permettre à la personne qui a fait la demande d'épuiser les ressources prévues par la loi, ce qui, dans la plupart des cas, est de 30 jours.

Destruction : En vertu du PCA, le CCES doit détruire ou effacer en toute sécurité ou bien anonymiser les *renseignements personnels liés à l'antidopage* qu'il n'est plus tenu de conserver. La direction générale des services généraux doit prendre les dispositions nécessaires pour que les dossiers contenant des *renseignements personnels liés à l'antidopage* qui ont atteint la durée de conservation prescrite dans la présente politique au cours de l'année civile précédente soient, selon le format des dossiers, effacés de manière sécurisée par écrasement avec l'aide du service de l'informatique ou déchiquetés. Les employés du CCES doivent se conformer à ces exigences, notamment en employant des méthodes sécurisées pour procéder à la destruction autorisée de *renseignements personnels liés à l'antidopage*. (Annexe A du SIPRP de l'AMA)

Suspension de la destruction ou de l'élimination des documents : Dans certains cas, les dossiers contenant des *renseignements personnels liés à l'antidopage* seront conservés au-delà de la période de conservation prescrite en raison d'une plainte contre le CCES, d'une demande de protection de la vie privée, d'un audit, d'un litige en cours, d'une sanction en cours ou de la possibilité d'un litige impliquant ou susceptible d'impliquer le CCES. Le CCES doit suspendre sur-le-champ l'application du délai de conservation et la destruction d'un document ou d'une catégorie de documents dans les cas suivants :

i) Lorsqu'il prend connaissance, par quelconque moyen, d'une allégation, d'une réclamation, d'un audit, d'une enquête ou d'une procédure, potentiel, en vigueur ou en attente contre le CCES, qui vise notamment un membre du personnel ou de la direction du CCES pour des actions effectuées dans le cadre de ses fonctions, à condition que la réclamation, l'audit, l'enquête ou la procédure ait été lancé ou semble sur le point de l'être;

ii) Lorsque la loi ou une ordonnance du tribunal l'exige;

iii) Lorsque nécessaire pour permettre au CCES d'exercer les recours à sa disposition ou de limiter les dommages qu'il pourrait subir. La suspension de la destruction sera levée au terme de l'enquête, conformément au délai de prescription applicable, qui est de deux ans dans la plupart des cas.

2.11 Sécurité

Le *responsable de la protection de la vie privée* doit assurer la conformité au SIPRP.

Le CCES protégera en tout temps les *renseignements personnels liés à l'antidopage* en appliquant toutes les mesures de sécurité nécessaires, y compris les mesures physiques, organisationnelles, techniques, environnementales et autres pour prévenir la perte, le vol ou l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation (y compris la divulgation à l'aide des réseaux électroniques) des *renseignements personnels liés à l'antidopage*.

Le CCES appliquera les mesures de sécurité qui tiennent compte des risques liés au traitement des *renseignements personnels liés à l'antidopage* et à la vulnérabilité des *renseignements personnels liés à l'antidopage* qu'il doit protéger.

Quand le CCES divulgue des *renseignements personnels liés à l'antidopage* à des agents associés à ses activités de lutte contre le dopage en vertu du PCA ou du Code, il est responsable de prendre toutes les mesures raisonnables pour s'assurer que ces agents utilisent les renseignements conformément aux lois du pays en question ou, si aucune loi n'est en vigueur, au SIPRP.

2.12 Conservation

Le CCES s'assurera que les *renseignements personnels liés à l'antidopage* seront uniquement conservés le temps nécessaire pour remplir ses obligations en vertu du PCA ou si la loi applicable l'exige. Le CCES respectera les délais de rétention pour les différents types de *renseignements personnels liés à l'antidopage* déterminés à l'occasion par l'AMA, à moins qu'un tel délai viole une loi applicable. Dans le cas des AUT, les certificats seront conservés 10 ans après leur expiration pour s'assurer qu'ils seront préservés pour tout échantillon entreposé à des fins de contrôle du dopage ultérieures.

Dès que les *renseignements personnels liés à l'antidopage* ne servent plus aux fins indiquées ci-dessus, ils seront supprimés, détruits ou dépersonnalisés de façon permanente.

PARTIE 3 : Politique de protection des renseignements personnels du Programme canadien de sport sécuritaire (PCSS)

3.1 Résumé

Le Centre canadien pour l'éthique dans le sport (CCES) s'engage à ce que toute personne puisse effectuer un Signalement (voir la définition ci-dessous) de maltraitance en toute confiance. Cela signifie, entre autres, de comprendre comment nous protégeons vos renseignements sensibles. La présente politique porte sur vos droits relatifs à vos renseignements.

Lorsque le CCES reçoit un Signalement de maltraitance, il collecte des renseignements personnels sur la personne qui effectue le Signalement (si elle les fournit), la personne faisant l'objet du Signalement et, parfois, les parties concernées. Il peut arriver que ces personnes soient mineures. En outre, si nous avons besoin de vos renseignements personnels, nous nous engageons à :

- conserver vos renseignements en sécurité;
- vous expliquer pourquoi nous avons besoin de vos renseignements avant que vous nous les donniez;
- n'utiliser vos renseignements personnels qu'aux fins pour lesquelles vous nous les avez fournis;
- ne pas vendre vos renseignements;
- ne pas communiquer vos renseignements personnels sans votre consentement, à moins que ce soit nécessaire, par exemple pour des raisons de sécurité, pour faire respecter une Mesure provisoire, pour enquêter sur un Comportement prohibé, pour faire respecter une sanction ou à moins d'indication contraire de la loi;
- utiliser vos renseignements dans une base de données anonymisées pour suivre l'évolution de nos travaux et, plus largement, de la question de la maltraitance dans le sport au Canada.

L'un des moyens d'assurer la sécurité de vos renseignements est de veiller à ce que vous et nous comprenions pourquoi vous nous fournissez vos renseignements personnels, comment ces renseignements sont utilisés et comment nous les protégeons. La présente politique explique en détail comment le CCES collecte, utilise, conserve, protège, divulgue et élimine vos Renseignements personnels dans le cadre du Programme canadien de sport sécuritaire (PCSS), et devrait être lue et interprétée dans ce contexte et en parallèle avec le PCSS lui-même. Les termes définis dans la présente partie ont le sens qui leur est attribué dans le PCSS, à moins d'indications contraires expresses.

Pour communiquer avec le responsable de la protection de la vie privée, envoyer un courriel à confidentialite@cces.ca.

3.2 Champ d'application

La présente politique s'applique à toutes les Personnes participantes assujetties aux Règlements du PCSS et à leur mise en application.

3.3 Avis

Le CCES informera les Parties (voir la définition ci-dessous) et les témoins sur les exigences en matière de confidentialité du PCSS et du Code de conduite universel pour prévenir et contrer la maltraitance dans le sport (CCUMS). Toutefois, le CCES ne peut être tenu responsable de la conduite des Parties ou témoins impliqués dans le processus du PCSS qui pourrait entraîner la divulgation illicite des Renseignements personnels faisant partie du dossier de preuve présenté au CCES.

Dans le cadre des services qu'il fournit en ligne, le CCES prend des moyens raisonnables pour prévenir les accès non autorisés aux Renseignements personnels qu'il stocke, sous forme numérique, dans ses propres serveurs; cela dit, le CCES ne peut être tenu responsable de tout manquement causé par les fournisseurs de services de courriel ou d'Internet des destinataires prévus.

3.4 Contexte

Le CCUMS formalise l'engagement du secteur du sport canadien à promouvoir une culture du sport respectueuse qui procure des expériences sportives de qualité, inclusives, accessibles, accueillantes et sécuritaires. Le PCSS s'engage lui aussi à promouvoir cet objectif fondamental.

Le PCSS confie au CCES le mandat d'administrer le CCUMS et de le faire respecter par les Organismes de sport, en recevant et en traitant les Signalements de Comportement prohibé ainsi qu'en élaborant et en mettant en œuvre des activités de sensibilisation et de prévention, de même que des politiques, dont des évaluations du milieu sportif. La présente politique se fonde sur les dix principes énoncés dans le Code type sur la protection des renseignements personnels du Groupe CSA, également énoncés dans les principes relatifs à l'équité dans le traitement de l'information de la Loi sur la protection des renseignements personnels et les documents électroniques.

La présente politique vise à décrire comment le CCES collecte, utilise, conserve, protège, divulgue et élimine les Renseignements personnels dans le cadre de son mandat tel que défini dans le PCSS. Le CCES peut modifier ou actualiser la présente politique de temps à autre pour quelque raison que ce soit, y compris pour refléter l'introduction de nouvelles technologies, de nouvelles pratiques opérationnelles, de nouveaux besoins des parties prenantes ou de nouvelles lois ou exigences réglementaires.

3.5 Définitions

Les termes qui portent la majuscule dans les présentes sans y être autrement définis ont le sens qui leur est donné dans les Règlements du PCSS.

Représentant autorisé : tout avocat ou toute autre personne désignée par écrit par la Personne ou, si la Personne est mineure et non émancipée, par tout parent, tuteur légal ou représentant autorisé d'une partie prenante au processus du PCSS.

Système de gestion des documents : la plateforme logicielle utilisée par le CCES pour la gestion des documents dans le cadre de ses activités ou des procédures du PCSS.

Signalement : un formulaire de signalement soumis ou de l'information soumise que le CCES

considère expressément comme un signalement.

Système de gestion des dossiers du PCSS : la plateforme logicielle utilisée par le CCES pour la gestion des Signalements, c'est-à-dire le partage d'information à l'interne et la réception de l'information que lui transmettent les Sous-traitants.

Sous-traitant : toute personne dont le CCES retient les services pour effectuer des tâches relatives à ses activités en échange d'une compensation monétaire ou de crédits d'éducation coopérative; ce terme désigne aussi les personnes à l'emploi du CCES.

Consentement exprès : consentement qui est donné par une Personne, sous forme électronique, écrite ou verbale, si nécessaire, qui est toujours sans équivoque et qui ne nécessite aucune inférence de la part du CCES.

Consentement tacite : consentement qui s'infère raisonnablement d'actes ou d'omissions d'une Personne.

Personne : une personne dont les Renseignements personnels sont collectés, utilisés, divulgués et conservés par le CCES. Il peut s'agir, entre autres, d'une Partie.

Partie(s) : une Personne à l'origine du signalement, une Partie intimée ou une Personne touchée aux termes des Règlements du PCSS.

La présente politique s'applique, quel que soit le mode d'enregistrement des Renseignements personnels utilisé (par exemple, électronique ou papier). Elle exclut les renseignements sur plus d'une personne où l'identité des personnes n'est pas connue et ne peut être inférée (les « Renseignements agrégés »). Le CCES se réserve le droit d'utiliser des renseignements agrégés de toutes les façons qu'il juge raisonnablement appropriées. En outre, la présente politique ne s'applique pas aux renseignements concernant des entreprises ou autres entités juridiques.

3.6 Responsabilité

Dans le cadre de son engagement à protéger les Renseignements personnels, le CCES requiert de tous les Sous-traitants, employés et autres fournisseurs qui contribuent à la prestation de ses services de respecter les obligations énoncées dans les présentes.

3.7 Objet de la collecte et types de renseignements collectés

Types de renseignements collectés

i) Le CCES collecte des Renseignements personnels qui sont raisonnablement nécessaires au déroulement de ses activités ou qui sont requis par la loi. Cela comprend les catégories de renseignements décrites ci-dessous, de même que tous autres Renseignements personnels fournis volontairement au CCES.
ii) Dans le cadre de ses activités, le CCES requiert le nom de famille, le prénom et les coordonnées (adresse courriel et/ou numéro de téléphone), ainsi que la confirmation de l'identité ou de l'autorité des Sous-traitants, des Parties et, s'il y a lieu, de leurs Représentants autorisés.
iii) Le CCES obtient de la part des Parties ou de leurs Représentants autorisés les Renseignements personnels par voie de plainte initiale/Signalement, d'enquête, de dossier de preuve, de soumission et autres mesures et documents reçus dans le cadre des

processus définis par les Règlements du PCSS. Ces renseignements peuvent comprendre, entre autres, des renseignements sur la santé, les infractions criminelles, le nom de famille, le prénom et les coordonnées, ainsi que les renseignements relatifs aux Signalements effectués contre les personnes et les sanctions connexes. Les Renseignements personnels fournis par les Parties ou leurs Représentants autorisés, notamment les renseignements financiers, les renseignements sur la santé, le nom de famille, le prénom, les coordonnées et les renseignements relatifs aux Signalements ou à d'autres procédures devant le CCES, peuvent aussi être collectés en vue d'établir l'admissibilité à certains programmes offerts par le CCES (ex. : aiguillage en santé mentale) et d'offrir ces programmes aux Parties admissibles.

iv) Le CCES collecte des renseignements personnels de ses Sous-traitants, notamment des renseignements financiers, les noms de famille, les prénoms et les coordonnées.

v) Le Système de gestion des dossiers du PCSS peut collecter des témoins de navigation contenant des renseignements sur les utilisateurs, dont l'adresse IP, les sections du portail consultées et l'information téléchargée.

vi) Les sites Web du CCES peuvent également collecter des renseignements non identificatoires, comme des témoins de navigation, y compris, entre autres, les adresses IP, les sections du site Web consultées et l'information téléchargée.

vii) Dans certains cas, le CCES obtient des Renseignements personnels de la part d'organismes de réglementation et d'application de la loi, d'autres organisations traitant avec le CCES ou les Personnes – par exemple, des organismes gouvernementaux, des agences de notation du crédit, des agences de recrutement et des fournisseurs d'information ou de services –, et aussi à partir de documents accessibles au public. Le CCES peut aussi obtenir des renseignements de la part de tiers ou à partir de sources publiques dans le contexte d'une enquête ou d'un processus du PCSS.

3.8 Objet

Les fins pour lesquelles le CCES collecte des Renseignements personnels sont énumérées à l'annexe A.

Le CCES informe la Personne des raisons de la collecte et de l'utilisation de ses Renseignements personnels en la renvoyant à la présente politique au moment de la collecte ou avant celle-ci.

Le CCES ne vend pas les renseignements personnels obtenus.

3.9 Obtention d'un consentement éclairé valable

Quand demander le consentement

À l'exception des cas d'urgence, des cas où il est raisonnable de penser que la Personne a donné son consentement tacite, ou des cas où le consentement n'est pas prescrit par la loi, le CCES obtient le consentement de la Personne, ou de son Représentant autorisé, pour l'utilisation et la divulgation de ses Renseignements personnels, le tout avant leur collecte ou au moment de celle-ci.

Sauf exception prévue par la loi, le CCES, advenant qu'il ait à utiliser les Renseignements personnels à d'autres fins que celles auxquelles la Personne avait initialement consenti, avise la Personne et obtient son consentement pour l'utilisation de ces renseignements à toute

nouvelle fin.

3.10 Consentements exprès et tacite

En fournissant au CCES des renseignements personnels, la Personne ou son représentant autorisé consent à leur collecte, à leur utilisation et à leur divulgation aux termes des présentes. Si ces personnes n'acceptent pas les présentes dispositions, elles ne doivent pas fournir de renseignements personnels au CCES. Toutefois, bien que la fourniture de certains Renseignements personnels au CCES soit facultative, le CCES pourrait ne pas être en mesure de fournir à la Personne les services qui requièrent ces Renseignements personnels si la Personne choisit de ne pas les transmettre.

Le consentement peut être exprès ou tacite et être fourni par la Personne ou un Représentant autorisé. Pour déterminer le type de consentement requis, le CCES tient compte de la nature sensible des Renseignements personnels et des attentes raisonnables de la Personne. Malgré ce qui précède, sauf exception prévue par la loi, le CCES doit obtenir le consentement exprès lorsqu'on peut raisonnablement penser que les Renseignements personnels sont de nature sensible.

3.11 Procédures de consentement détaillées

Formulaires de consentement normalisés : le CCES élabore et utilise des formulaires normalisés pour obtenir le consentement exprès. Ces formulaires sont disponibles en version numérique et papier et doivent être acceptés par la Personne ou son Représentant autorisé.

Mécanismes de consentement numériques : En ce qui concerne les interactions numériques, le CCES met en place des mécanismes de consentement numériques sécurisés, par exemple des signatures électroniques ou des cases à cocher, pour veiller à ce que le consentement exprès soit correctement consigné.

Révocation du consentement : les Personnes ont le droit de révoquer leur consentement en tout temps; toutefois, une demande de révocation de consentement ne met pas fin à un processus du PCSS en cours. Le CCES fournit un processus de révocation clair, ce qui comprend un formulaire normalisé et un point de contact dédié à la soumission des demandes de révocation.

3.12 Limitation de la collecte

Collecte

Le CCES ne collecte les Renseignements personnels que par des moyens honnêtes et licites raisonnablement nécessaires aux fins déterminées.

3.13 Limitation de l'utilisation : utilisation et divulgation

Principes généraux

Le CCES utilise et divulgue les Renseignements personnels aux fins déterminées seulement, et ces fins se limitent, dans la mesure où cela est raisonnablement nécessaire, à l'exécution des obligations du CCES aux termes du PCSS.

3.14 Applications du principe

Le nom de famille et le prénom peuvent être transmis aux Parties concernées par le même différend ou processus du PCSS ainsi qu'à leurs Représentants autorisés durant des procédures du PCSS.

Les Renseignements personnels décrits à l'article 3.7(iii) peuvent, à l'entière discrétion du CCES et/ou de tout Sous-traitant dans le cadre d'un processus d'enquête, d'arbitrage, d'appel, de médiation ou autre du PCSS, être divulgués dans le rapport d'enquête et/ou la décision de l'arbitre lorsqu'il s'avère raisonnablement nécessaire d'étayer les décisions rendues ou les conclusions présentées.

Tout Renseignement personnel décrit à l'article 3.7(iii) qui se trouve dans une décision rendue par le CCES autorisant l'identification d'une Personne visée par une allégation d'infraction est publié, conservé et distribué conformément aux Règlements du PCSS.

Les Renseignements personnels décrits à l'article 3.7(iv) sont utilisés strictement aux fins de gestion des ressources humaines, de gouvernance et de fonctionnement du CCES, respectivement.

Les Renseignements personnels décrits aux articles 3.7(v) et 3.7(vi) sont utilisés sous forme agrégée lorsque cela est possible et peut servir aux mêmes fins.

En dehors du CCES, l'accès aux Renseignements personnels, leur utilisation et leur divulgation sont restreints aux Sous-traitants du CCES selon le cadre raisonnablement nécessaire à l'exécution de leurs obligations envers le CCES.

Les Renseignements personnels faisant l'objet d'une demande d'une Personne ou de son Représentant autorisé sont conservés aussi longtemps que raisonnablement nécessaire pour permettre à la Personne d'épuiser tous les recours qu'elle peut avoir, pourvu que la demande soit faite avant leur suppression.

Tout Renseignement personnel collecté par le CCES est géré conformément aux normes et mécanismes de sécurité énoncés à l'article 3.17.

3.15 Conservation

Les Renseignements personnels collectés dans le cadre du PCSS sont conservés pour une période minimale de deux ans et aussi longtemps seulement qu'ils sont raisonnablement nécessaires et pertinents aux fins pour lesquelles ils ont été recueillis.

3.16 Exactitude des renseignements

Le CCES prend des moyens raisonnables pour s'assurer que les Renseignements personnels sont exacts, complets et aussi à jour que l'exigent les fins ayant étayé leur collecte.

Le CCES exige de chaque Personne qu'elle fournisse des Renseignements personnels exacts et le tienne rapidement informé de tout changement.

Le CCES n'est pas responsable des pertes de services et d'avantages découlant de l'omission, par les Personnes, d'aviser par écrit le CCES de tout changement aux Renseignements personnels à leur dossier.

3.17 Normes et mécanismes de sécurité

Dispositions générales

Le CCES a mis en place des mécanismes de sécurité afin de protéger de la perte et du vol, ainsi que de l'accès, de la divulgation, de la duplication, de l'utilisation ou de la modification non autorisés les Renseignements personnels. Le CCES s'engage à maintenir en place ces mesures ou des mesures 6 équivalentes, lesquelles peuvent être modifiées de temps à autre.

Les méthodes de sécurité qu'emploie le CCES sont décrites dans sa politique sur la sécurité des TI.

Dispositions particulières

L'autorisation d'accès aux Renseignements personnels stockés dans le Système de gestion des dossiers du PCSS et le Système de gestion des documents du CCES varie selon les responsabilités et les besoins de l'employé ou du Sous-traitant.

Le Système de gestion des dossiers du PCSS et le Système de gestion des documents du CCES déploient les mesures de protection des données énoncées dans la partie IV de la politique sur la sécurité des TI du CCES.

Tout transfert nécessaire de Renseignements personnels détenus par le CCES s'effectue par le Système de gestion des dossiers du PCSS et le Système de gestion des documents ou par un mécanisme sécurisé de transmission de fichiers. Dans la mesure du possible, la transmission de Renseignements personnels ne se fait pas par courriel. Les documents envoyés par courriel ou par un mécanisme sécurisé de transmission de fichiers sont protégés par un mot de passe. Le mot de passe est envoyé dans un courriel distinct de celui auquel est joint le document protégé par mot de passe.

Conscientisation, formation et ententes en matière de protection des renseignements personnels

Le CCES met tous ses employés et ses Sous-traitants au courant de l'importance du maintien de la sécurité et de la confidentialité des Renseignements personnels.

Tous les employés et Sous-traitants doivent signer une entente qui les lie à la présente politique et aux dispositions pertinentes de la politique encadrant l'administration du ou des Signalements qu'ils traitent.

Les Parties et leurs Représentants autorisés sont liés aux dispositions des Règlements du PCSS et du CCUMS, qui prévoient qu'ils et que toutes les autres personnes assistant aux procédures en leur nom doivent s'abstenir de divulguer tout renseignement ou document obtenu dans le cadre de leur participation au processus de résolution, conformément à la loi.

Tous les employés et Sous-traitants du CCES doivent suivre la formation obligatoire sur la protection des renseignements personnels au moment de leur intégration et une fois par année par la suite. Cette formation traite des plus récentes menaces à la sécurité, des bonnes pratiques en matière de protection des données ainsi que des politiques et procédures de sécurité du CCES.

Le CCES tient des dossiers sur toutes les séances de formation sur la sécurité, y compris un relevé des présences et le matériel de formation. Ces dossiers font l'objet d'une vérification

périodique pour en assurer la conformité et l'efficacité.

3.18 Destruction, suppression ou dépersonnalisation

Les Renseignements personnels sont détruits, supprimés, anonymisés de façon permanente ou, dans le cas de dossiers papier, déchiquetés lorsqu'ils ne sont plus pertinents ni nécessaires aux fins pour lesquelles ils ont été collectés.

3.19 Transparence

Modifications

Les modifications à la présente politique sont mises à la disposition du public après leur adoption, au moins un (1) mois avant leur entrée en vigueur, sur le site Web du CCES ou à la demande. Nous recommandons aux Personnes qui fournissent des Renseignements personnels au CCES de vérifier régulièrement si la présente politique a été modifiée ou mise à jour.

Divergences

Dans le cas de divergences ou d'incohérences entre la législation sur la protection des renseignements personnels applicable et la présente politique, la législation applicable prévaut.

3.20 Accès individuel et correction des renseignements

Accès aux renseignements et corrections

Sous réserve de l'article 3.18 ci-dessus :

- Toute Personne a droit d'accéder à ses Renseignements personnels sur présentation d'une demande écrite au Responsable de la protection des renseignements personnels.
- Le CCES fournit également, sur présentation d'une demande écrite, des renseignements de base sur l'utilisation des Renseignements personnels de la Personne, dont leur communication à des tiers, sous réserve des modalités des Règlements du PCSS.
- La Personne a le droit de demander, par écrit, la correction de toute erreur démontrable relativement à ses Renseignements personnels.
- Le CCES transmet, lorsque cela s'avère nécessaire à ses activités ou au maintien des services et avantages fournis à la Personne, les Renseignements personnels rectifiés aux Sous-traitants et aux tiers détenteurs d'une autorisation d'accès.

Identification

Seules les demandes faites par écrit (par des Personnes ayant adéquatement donné leur identité ou les Représentants autorisés par ces Personnes à obtenir les Renseignements personnels demandés) seront traitées.

L'identification adéquate du demandeur comprend deux pièces d'identité délivrées par le gouvernement (passeport, permis de conduire, certificat de naissance, etc.), dont au moins une comportant la photo du demandeur.

Délai de réponse à une demande

Le CCES répond au plus tard 30 jours après la date de réception d'une demande faite par écrit par une personne admissible ou son Représentant autorisé.

Dans certaines circonstances raisonnables, notamment les demandes impliquant de nombreux renseignements, les demandes difficiles à traiter ou celles requérant une conversion de renseignements, le CCES peut avoir besoin d'une prolongation. Dans de tels cas, le demandeur est avisé par écrit, avant l'expiration du délai de 30 jours, des raisons de la prolongation et de son droit de déposer une plainte au Responsable de la protection des renseignements personnels relativement à cette prolongation.

Coût

Le CCES peut exiger le paiement de frais de réponse à la Personne effectuant la demande. Le cas échéant, le CCES informe la Personne du coût approximatif; le CCES fournira les renseignements demandés une fois le paiement effectué.

Refus d'une demande

Le CCES peut refuser, brefs motifs à l'appui, une demande de correction dans certains cas seulement, y compris, sans s'y limiter, ceux où la Personne omet de fournir une preuve suffisante de l'inexactitude des renseignements, ou ceux où la divulgation des renseignements contreviendrait aux dispositions et aux fins du PCSS. Lorsqu'il est impossible de modifier un document, la correction prend la forme d'une note ajoutée au dossier.

Malgré un droit général d'accéder à des Renseignements personnels sur demande, le CCES peut refuser, à son entière discrétion, une demande d'accès; le cas échéant, il fournit les motifs de sa décision, qui est finale et contraignante et ne peut faire l'objet d'une révision ni d'un appel à l'interne.

Le CCES peut refuser une demande d'accès notamment dans les cas suivants :

i) satisfaire à la demande pourrait causer un préjudice à la Personne ou à une autre Personne;

ii) satisfaire à la demande pourrait compromettre l'administration, le processus d'enquête ou les préparatifs d'arbitrage d'un Signalement;

iii) satisfaire à la demande divulguerait les Renseignements personnels d'une autre Personne sans son consentement, ces renseignements étant indissociables, à moins que leur divulgation soit nécessaire pour éviter à cette autre Personne un préjudice;

iv) un doute raisonnable subsiste quant à l'identité ou l'autorité du demandeur, qu'il s'agisse de la Personne ou d'une autre alléguant avoir l'autorité d'agir au nom de la Personne.

Le CCES peut donner accès aux Renseignements personnels, lorsque c'est possible et raisonnable, sous une forme caviardée afin d'éviter tout préjudice. Le CCES est réputé avoir refusé une demande d'accès s'il n'a pas répondu au terme du délai de 30 jours.

Annexe A à PARTIE III : Politique de protection des renseignements personnels du PCSS

Le CCES collecte des Renseignements personnels sur les Personnes aux fins énoncées dans le PCSS et les Règlements du PCSS ainsi qu'aux fins suivantes :

Renseignements obtenus de toutes Personnes, sur toutes Personnes

- offrir aux Personnes du soutien administratif ou technique dans le cadre de leur utilisation du Système de gestion des documents du CCES et des services et du Système de gestion des dossiers du PCSS;
- recueillir les opinions et commentaires des Personnes au sujet des activités du CCES;
- le cas échéant, procéder à toutes autres collectes et utilisations de Renseignements personnels pour lesquelles le CCES obtient le consentement;
- agir selon ce qui est par ailleurs requis ou autorisé par la loi.

Renseignements obtenus de Personnes autres que des Sous-traitants

- répondre aux Signalements ou demandes de renseignements des Personnes;
- recevoir les Signalements, les traiter, les administrer, ainsi que mener les processus connexes d'enquête, de médiation, de décision et d'application des décisions prises aux termes du PCSS. Cela peut comprendre l'inscription des Renseignements personnels au registre public;
- conseiller les Personnes au sujet des nouveaux programmes et services qui pourraient répondre à leurs besoins ou à ceux de leurs organisations;
- surveiller l'utilisation du Système de gestion des dossiers du PCSS et du Système de gestion des documents et détecter toute tentative d'utilisation frauduleuse;
- produire des rapports statistiques.

Renseignements obtenus de Sous-traitants :

- tenir des événements auxquels ils participent;
- pourvoir des postes au CCES;
- administrer les politiques et procédures du CCES relativement à la formation, à la rétention et à l'évaluation des Sous-traitants;
- mener des activités d'accompagnement, de mentorat et de développement professionnel;
- gérer la productivité, ce qui comprend les mesures d'accommodement et les autorisations;
- rembourser les dépenses admissibles engagées par les Sous-traitants sous forme de factures, de reçus ou de renseignements sur les déplacements;
- à partir des renseignements de tiers fournisseurs d'avantages sociaux, de régimes de

retraite et d'assurance et autres services connexes, fournir lesdits services ainsi que de la rémunération, et satisfaire aux exigences fiscales à cet égard;

- se conformer à d'autres exigences prescrites par les lois applicables, notamment les lois sur la santé et la sécurité au travail et celles sur la sécurité professionnelle et l'assurance contre les accidents du travail.

PARTIE 4 : AUTRES POLITIQUES DU CCES

Politique sur la sécurité des TI

4.1 Politique sur la sécurité des TI – présentation

La présente politique sur la sécurité des TI s'applique à l'ensemble des employés permanents et temporaires, y compris les employés contractuels (collectivement, le « personnel »).

4.2 Conformité à la politique

Le personnel est responsable du respect de la politique, comme indiqué à l'article 4.3 ci-dessous, mais c'est au CCES de s'assurer que l'ensemble du personnel prend connaissance du contenu et de l'objectif de la présente politique, les passe en revue et les comprend.

Quiconque enfreint la présente politique s'expose à des mesures disciplinaires pouvant aller jusqu'au congédiement.

4.3 Responsabilités

La direction générale des services généraux (ou son délégué) doit veiller à ce que le CCES respecte la présente politique, remplisse ses engagements en matière de technologies de l'information (TI) contenus dans ses addendas relatifs au traitement des données et qu'il offre la formation nécessaire à son personnel.

Le personnel est responsable de ce qui suit :

- Se tenir à jour sur ses responsabilités en matière de sécurité et suivre les formations nécessaires sur l'utilisation des systèmes informatiques.
- Suivre des procédures qui minimisent l'exposition du CCES à la fraude, au vol ou à la perturbation de ses systèmes informatiques, telles que la séparation des tâches au besoin (par exemple entre les activités antidopage et le service des finances).
- Veiller à ce que ses actions n'entraînent aucune faille de sécurité.
- Signaler sans délai au *responsable de la protection de la vie privée* toute *atteinte à la sécurité* réelle ou suspectée.
- S'assurer que les renseignements auxquels il a accès sont sécurisés.
- Coopérer à toute enquête.

4.4 Assurer la sécurité des renseignements

Fuite de données et incidents liés à la sécurité des renseignements

Le CCES doit traiter les fuites de données et les incidents liés à la sécurité conformément à la Politique de protection des renseignements personnels et à la législation applicable.

Contrôle de l'accès

L'accès du personnel aux systèmes informatiques est accordé en fonction du rôle, selon le principe du moindre privilège ou du besoin de savoir. Par défaut, les privilèges d'accès sont

limités au degré d'accès le plus bas nécessaire à l'exécution de son rôle et de ses tâches. Le personnel ne peut accéder qu'aux systèmes pour lesquels il a l'autorisation. L'authentification multifactorielle doit être mise en place dans la mesure du possible.

Le CCES dispose de procédures pour contrôler l'accès à ses systèmes. Les privilèges d'accès sont modifiés en fonction des mutations et révoqués à distance lorsqu'une personne quitte le CCES. Les cadres doivent informer sans délai l'équipe informatique et le *responsable de la protection de la vie privée* de toute demande de changement nécessitant une telle modification ou révocation.

Quiconque quitte le CCES doit remettre l'ensemble de ses dispositifs d'identification personnelle, cartes d'accès, clés, laissez-passer, manuels et documents à son départ.

Lorsqu'un employé quitte le CCES, les administrateurs des systèmes (internes et externes, notamment l'accès aux comptes bancaires et les approbations) doivent supprimer ou désactiver tous ses identifiants et ses mots de passe.

Les cadres doivent aussi s'assurer qu'à son départ, la personne ne copie pas, n'efface pas ou ne supprime pas de façon inappropriée des renseignements sur les disques durs ou les serveurs. Les accès de cette personne seront supprimés immédiatement à son départ, afin d'éviter tout dommage à l'équipement du CCES et tout accès non autorisé aux renseignements du CCES, ou toute divulgation ou perte de renseignements du CCES.

Une personne qui visite les bureaux du CCES doit être accompagnée en tout temps. Si elle a besoin de mots de passe temporaires pour accéder à des systèmes confidentiels, ceux-ci seront désactivés après son départ. Elle ne devrait en aucun cas avoir la possibilité de consulter sans autorisation des écrans d'ordinateur ou des documents imprimés produits par un système d'information. On ne lui fournira que le réseau Wi-Fi pour les invités, qui ne permet pas d'accéder aux lecteurs partagés du CCES.

Les bureaux du CCES doivent être physiquement protégés par un système de contrôle des accès.

Sécurité de l'équipement

Les ordinateurs portables et les appareils mobiles doivent être dotés d'une protection d'accès appropriée, par exemple des mots de passe et du chiffrement. Les appareils ne doivent jamais être laissés sans surveillance dans un lieu public, y compris à la vue de tous dans un véhicule.

Le personnel en télétravail doit mettre en place des mesures de sécurité appropriées sur son lieu de travail pour protéger adéquatement l'équipement et les renseignements du CCES (par exemple, verrouiller les portes, faire en sorte que les autres personnes sur le lieu ne voient ni n'aient accès à l'équipement et aux renseignements).

Le matériel fourni par le CCES ne peut être utilisé que par le personnel du CCES.

Il est important de se défaire des ordinateurs portables et des appareils mobiles de manière appropriée afin de garantir la destruction irrémédiable et sécurisée de tout renseignement confidentiel.

Les employés et contractants du CCES sont tenus d'utiliser le réseau privé virtuel (RPV) du CCES en tout temps. Les réseaux Wi-Fi publics sont à éviter, et l'utilisation de points d'accès personnels sans fil doit être limitée, afin d'empêcher tout accès non autorisé aux appareils.

Sécurité et stockage de renseignements

Tous les renseignements, qu'ils soient électroniques ou non, doivent être stockés de manière sécurisée en fonction de leur degré de sensibilité. Chaque équipe doit déterminer le degré de sensibilité des renseignements qu'elle possède et le mode de stockage approprié.

Politique de bureau propre

À la fin de chaque journée de travail, le personnel doit retirer de son bureau, de son espace de travail et de ses étagères les documents de travail privés ou confidentiels, les dossiers ouverts et les documents administratifs pour les placer en lieu sûr dans les tiroirs et les classeurs du bureau, le cas échéant.

Envoi de renseignements par la poste ou par courriel

Sauf si des circonstances exceptionnelles ne le permettent pas, il faut toujours envisager et adopter la méthode de transmission la plus sûre, en particulier pour les renseignements sensibles et confidentiels comme les renseignements personnels. Les renseignements transmis, physiquement ou électroniquement, doivent toujours être limités au strict minimum. Les procédures suivantes doivent être adoptées selon les besoins et en fonction de la sensibilité de l'information, et peuvent être adaptées en cas d'urgence.

Envoi de renseignements par courriel :

- Prenez le temps de vérifier l'adresse électronique du destinataire avant d'appuyer sur « Envoyer », en particulier lorsque le champ « À » se remplit automatiquement.
- Si vous devez envoyer régulièrement des renseignements confidentiels, personnels ou sensibles par courriel, envisagez de désactiver la fonction de saisie semi-automatique et de vider régulièrement la liste des destinataires suggérés. Ces deux fonctions se trouvent dans Outlook, sous « Fichier », « Options » et « Courrier ».
- Utilisez la fonction « Répondre à tous » avec prudence et assurez-vous que vous connaissez l'ensemble des destinataires et que chacune de ces personnes a besoin de l'information que vous vous apprêtez à lui envoyer.
- S'il y a lieu, servez-vous de mots de passe, de technologies de chiffrement et de canaux sécurisés pour transmettre des renseignements sensibles à des parties externes (p. ex., en utilisant ShareFile).
- Vérifiez que tous les renseignements privés ou confidentiels qui devraient être supprimés l'ont été.

Envoi de renseignements par la poste :

- Assurez-vous d'avoir la bonne adresse.
- Assurez-vous que seuls les renseignements pertinents figurent dans l'enveloppe et qu'une autre lettre n'y a pas été incluse par inadvertance.
- Apposez la mention « Confidentiel » sur l'enveloppe.

- Si les renseignements sont particulièrement sensibles ou confidentiels, envisagez le recours à une méthode de livraison plus sûre (par exemple, par courrier recommandé ou service de messagerie).

Impression, photocopie et numérisation :

- Le personnel doit veiller à retirer des imprimantes, des photocopieuses et des numériseurs tout document contenant des renseignements confidentiels, et à ne jamais laisser de tels documents sans surveillance dans ces appareils.
- Après avoir numérisé un document, il est important de le couper du serveur S: et de le coller vers le bon dossier du lecteur partagé, et ce, le plus rapidement possible. Avant d'envoyer un fichier numérisé à l'externe, il faut toujours vérifier qu'il s'agit du bon document.

Rétention et destruction des renseignements

Pour la destruction de renseignements, le CCES doit suivre la présente politique.

Les documents papier qui contiennent des renseignements confidentiels doivent être déchiquetés. Les renseignements électroniques doivent quant à eux être détruits de façon permanente, c'est-à-dire effacés de manière à empêcher leur récupération dans un contexte autre que judiciaire.

4.5 Sécurité des renseignements et des technologies de la communication

Solutions de stockage infonuagiques

Il est interdit au personnel de stocker des renseignements du CCES dans son propre outil infonuagique (comme Skydrive, OneDrive personnel, Dropbox, iCloud, etc.).

Mise en place et développement de systèmes

Il faut toujours tenir compte des enjeux de sécurité associés à la mise en place et au développement de systèmes. Au besoin, il convient de consulter le gestionnaire principal de la technologie.

Il est possible de demander une évaluation indépendante avant d'acheter un nouveau système permettant de stocker des renseignements personnels et d'y accéder.

Sécurité du réseau

Le CCES met en place des mesures de contrôle pour prévenir et détecter les activités non autorisées sur son réseau (notamment les virus et les logiciels malveillants) et y faire face, en utilisant des technologies modernes telles que les pare-feu, la prévention et la détection des intrusions, le filtrage du contenu Web et des courriels et les antimaliciels.

Il peut faire appel à des spécialistes externes pour améliorer la sécurité du réseau.

Toute personne qui croit avoir reçu un virus ou un courriel malveillant doit le signaler au service informatique.

Contrôle de l'accès aux lieux sécurisés, notamment :

- la salle des serveurs : tous les serveurs et équipements réseau de l'organisme se trouvent dans une salle de serveurs sécurisée dont l'accès est limité;
- les dossiers pour Iron Mountain;
- les classeurs verrouillés en permanence (dossiers RH, classeur 4).

Mesures de sécurité liées à l'accès des tiers

Les tiers n'ont accès aux réseaux du CCES qu'après avoir reçu l'autorisation formelle du gestionnaire principal de la technologie et après avoir signé une entente de sécurité et de confidentialité.

Tous les tiers qui traitent des renseignements personnels au nom du CCES (y compris par le biais d'un système informatique hébergé) doivent signer une entente de confidentialité précisant les modalités du traitement des données avant de pouvoir accéder aux renseignements.

Le CCES a mis en place et tient à jour des politiques et procédures visant à assurer la protection de toute l'information envoyée à des systèmes externes, ainsi que des contrôles de sécurité qui régissent les activités de ces tiers.

Les tiers sont soumis aux mêmes normes de confidentialité que le personnel du CCES.

Sauvegarde des données

Le CCES a des processus de sauvegarde en place qui garantissent un archivage approprié et permettent de récupérer des données en cas d'urgence. Les données du CCES sont conservées dans un répertoire réseau pour s'assurer d'une sauvegarde adéquate.

Les sauvegardes sont stockées sur place et dans un emplacement hors site secret et sont soumises aux mêmes normes de sécurité que les données en direct. Des procédures sont en place pour récupérer les sauvegardes au besoin et pour permettre au CCES de poursuivre ses activités en situation d'urgence.

Si les données en direct sont corrompues, l'ensemble des logiciels, du matériel informatique et des moyens de communication touchés seront vérifiés avant de procéder à l'utilisation des données de sauvegarde, afin de s'assurer que ces dernières ne sont pas également corrompues ou compromises.

Logiciels

Le personnel ne doit installer sur l'équipement du CCES que des logiciels approuvés par l'équipe informatique. En limitant l'accès administrateur, on assure le respect de cette directive.

Si le CCES détermine qu'un certain logiciel ou matériel informatique est nécessaire, il doit en faire l'achat, puis le faire installer et suivre par l'équipe informatique.

Les progiciels doivent être conformes aux normes de sécurité du CCES et ne pas les compromettre.

Utilisation de supports amovibles (comme des clés USB)

Le personnel du CCES ne doit utiliser que des supports amovibles autorisés. Pour obtenir l'autorisation d'utiliser un support amovible, il faut bâtir un dossier qui présente le cas particulier le nécessitant, puis le faire approuver par l'équipe informatique.

Procédures liées au délai d'inactivité

Les ordinateurs inactifs sont automatiquement mis en veille après un certain laps de temps. Passé le délai d'inactivité, les renseignements à l'écran ne seront plus visibles. Dans les lieux à haut risque, les applications et sessions ouvertes doivent également se déconnecter. Sont considérés comme des lieux à haut risque les endroits publics ou externes qui échappent au contrôle de la sécurité du CCES. Le délai d'inactivité doit refléter le niveau de risque associé au lieu où se trouve l'appareil.

Dès qu'une personne s'éloigne de son poste de travail, elle doit verrouiller son écran. Pour les applications à haut risque, il convient d'envisager une restriction du temps de connexion. Limiter le temps de connexion aux outils informatiques réduit le risque d'accès non autorisé.

Documentation des systèmes

Tous les systèmes doivent être adéquatement documentés et mis à jour.

Les exigences contenues dans les addendas du CCES sur le traitement des données doivent être mises à jour par le gestionnaire principal de la technologie.

Contrôle de version

Numéro de la version	Date	Approuvée par
1	1er janvier 2025	Jeremy Luke

POLITIQUE DE CONFIDENTIALITÉ

4.6 Politique de confidentialité – contexte

Le Centre canadien pour l'éthique dans le sport (le « **CCES »**) s'engage à ce que toute personne puisse effectuer un signalement de maltraitance en toute confiance et en connaissance des obligations de confidentialité qui régissent le Programme canadien de sport sécuritaire (le « **PCSS** »).

Le PCSS est une procédure confidentielle impliquant tout ou partie des personnes suivantes : la *personne à l'origine du signalement*, la *personne touchée*, la *partie intimée* et les témoins. Les signalements transmis au CCES sont traités de manière confidentielle, mais il existe des limites à cette confidentialité, telles que décrites dans le PCSS et le CCUMS. La présente Politique de confidentialité (la « **Politique** ») se veut un complément du PCSS et du CCUMS; elle ne les remplace pas. En cas de conflit entre les documents, c'est le PCSS qui prévaut.

4.7 Champ d'application

La Politique s'applique à l'ensemble des personnes et organismes impliqués dans un processus du PCSS, notamment à la *personne à l'origine du signalement*, à la *partie intimée*, à la *personne touchée*, aux témoins, à l'*organisme de sport*, à la personne chargée de l'enquête indépendante, ainsi qu'aux contractants et au personnel du CCES qui participent à l'administration du *signalement*.

La personne à l'origine du signalement et/ou la personne touchée, la partie intimée et toute autre personne participant à un processus du PCSS doivent garder confidentielles les informations reçues d'une autre partie, d'un organisme de sport ou d'une ou un témoin, sauf si le CCES, le PCSS ou la loi l'exigent. Cette obligation de confidentialité vise à préserver l'intégrité de chaque processus de résolution ou d'enquête du PCSS entrepris en réponse à un signalement.

Les obligations de confidentialité énoncées dans la présente Politique et dans le PCSS s'appliquent pendant toute la durée de l'enquête et du processus de résolution du PCSS. Toutefois, après la conclusion d'un processus de signalement, rien n'empêche la personne à l'origine du signalement, la personne touchée, la partie intimée ou une ou un témoin de parler de sa propre expérience par rapport à l'incident signalé, au processus du PCSS ou au résultat des procédures. Il est entendu qu'aucune disposition du présent règlement ne protège une personne qui communique des renseignements contre un recours en diffamation ou en vertu d'autres lois applicables.

Remarque : Les renseignements publiés sur le registre public sont publics et ne sont pas confidentiels.

4.8 Définitions

Les termes en italique dans les présentes ont le sens qui leur est donné dans les Règlements du PCSS. Pour s'assurer que toutes les modifications au Règlements du PCSS s'appliquent également à la présente Politique, les définitions ne sont pas reproduites ici. Elles sont accessibles au lien suivant : Règlements du PCSS.

4.9 Obligations

Les *signalements* transmis au CCES sont confidentiels.

Les limites de cette confidentialité sont que le CCES prend tous les moyens raisonnables pour protéger les renseignements personnels des personnes concernées par le traitement de *signalements*, tout en tenant compte de la nécessité de recueillir des informations pour évaluer les *signalements* ou mener des enquêtes et de la nécessité d'appliquer le PCSS d'une manière équitable sur le plan procédural.

Le CCES doit limiter les renseignements qu'il communique.

Les renseignements ne seront communiqués qu'aux personnes qui, selon le CCES, doivent les connaître pour pouvoir mettre en œuvre le PCSS, par exemple, le personnel et les contractants du CCES qui participent à l'administration du *signalement*, les conseillères et conseillers juridiques, la *personne à l'origine du signalement*, la *personne touchée* la *partie intimée*, les témoins et les *organismes de sport* concernés.

Le CCES peut être tenu ou avoir le choix de partager tout ou partie des renseignements suivants conformément au PCSS ou à d'autres obligations légales :

i) les noms de la *personne à l'origine du signalement*, de la *personne touchée*, de la *partie intéressée* et/ou des témoins, en fonction des choix en matière d'anonymat et des demandes formulées dans le respect de l'équité procédurale (comme décrit ci-dessus);

ii) les allégations formulées à l'encontre de la *partie intimée*;

iii) les renseignements et les documents obtenus dans le cours d'une enquête;

iv) les conclusions de fait impliquant la *partie intimée*;

v) les conclusions de violation contre la *partie intimée*;

vi) les sanctions imposées à la *partie intimée*.

Quiconque reçoit des renseignements dans le cadre du processus du PCSS doit en préserver la confidentialité, à moins d'indication contraire du CCES, du PCSS ou de la loi.

Aucune des dispositions relatives à la confidentialité n'empêche les *personnes à l'origine d'un signalement*, les *personnes touchées*, les *parties intimées* et les témoins de parler en toute confidentialité à des prestataires de soins de santé, à des prestataires de conseils juridiques, à des personnes pouvant leur offrir un soutien émotionnel ou aux forces de l'ordre.

Le CCES peut être tenu de transmettre des renseignements reçus dans le cadre d'un *signalement* aux autorités locales ou aux services de protection de l'enfance en vertu de l'obligation de signalement prévue par la loi.

Tous les documents créés dans le cadre d'un processus du PCSS, ainsi que leur contenu, sont confidentiels, notamment le *rapport d'enquête*, les *avis de préoccupation*, les observations écrites, les documents liés à la *résolution corrective* et les lettres de décisions émises par le CCES.

Ces documents, de même que leur contenu, ne doivent pas être communiqués en dehors du processus du PCSS, du tribunal de protection ou du tribunal d'appel, sauf si la loi l'exige ou si le CCES ou un tribunal du Centre de règlement des différends sportifs du Canada (CRDSC) l'autorise.

Toute violation de la confidentialité pourrait compromettre l'intégrité du processus.

Il est interdit aux personnes concernées par le processus du PCSS, notamment à la *personne à l'origine du signalement*, à la *partie intimée*, à la ou aux *personnes touchées* et aux témoins, de discuter entre elles du cas ou de divulguer à d'autres des renseignements sur le cas (notamment sur les médias sociaux ou publiquement), et ce, durant tout le processus. Cela pourrait non seulement compromettre la crédibilité et la fiabilité des renseignements communiqués, mais aussi entraver le déroulement et les conclusions de l'enquête.

4.10 Sanctions

Toute infraction à la présente Politique peut donner lieu à une enquête dans le cadre du PCSS et entraîner des sanctions prévues dans le PCSS.

Il incombe au CCES de faire respecter les obligations de confidentialité de la Politique. Lorsque c'est sur une ou un membre du personnel du CCES que pèsent les allégations, une tierce partie doit être chargée d'administrer le processus contre cette personne, conformément à la Politique.

4.11 Sensibilisation et formation en lien avec la Politique

L'ensemble des personnes et des organismes soumis à la Politique recevront un exemplaire du document ou des indications pour la consulter, et ce, dans les meilleurs délais.

Ces personnes et organismes concernés par le PCSS et soumis à la Politique doivent se familiariser avec son contenu et la passer régulièrement en revue.

Le CCES doit organiser périodiquement des séances de formation sur ses politiques de confidentialité afin de s'assurer que toutes les parties concernées par la Politique comprennent leurs obligations et l'importance du maintien de la confidentialité.