CANADIAN PARTNERSHIP AGAINST CANCER

PARTENARIAT CANADIEN CONTRE LE CANCER

POLITIQUE D'UTILISATION ACCEPTABLE

À partir de mai 2020

OBJECTIF DE LA POLITIQUE

La **Politique d'utilisation acceptable** fournit un cadre pour l'utilisation responsable et acceptée des ressources de la technologie de l'information du Partenariat (infrastructure hébergée, locale et en nuage, services réseau, ordinateurs, appareils mobiles, applications, réseaux, logiciels, communications, bases de données, etc.).

Notre technologie et nos solutions en nuage appuient les activités du Partenariat, et comprennent des solutions de cybersécurité qui soutiennent nos programmes et nos obligations réglementaires et juridiques, et ceux se rapportant à la cybersécurité.

En tant qu'utilisateur des systèmes d'information du Partenariat, vous cherchez à soutenir cet objectif; toute autre utilisation de nos technologies de l'information est secondaire et non liée aux activités professionnelles.

Tous les utilisateurs ont une attente raisonnable de protection des renseignements personnels et d'un accès juste aux ressources de technologies de l'information. Toutefois, les activités de surveillance et d'enregistrement des éléments de cybersécurité du Partenariat, réalisées à l'aide des ressources opérationnelles, pourraient relever les activités et le trafic à l'échelle de ses réseaux, de ses fournisseurs de services en nuage et de ses appareils. Pour plus d'information sur les attentes des utilisateurs à l'égard de la protection des renseignements personnels et sur la manière dont le Partenariat utilise et protège les données et les renseignements personnels, se reporter à la **Politique de confidentialité destinée au personnel**.

Les activités interdites qui compromettent l'intégrité, la consommation juste, la protection des renseignements personnels et la sécurité des autres ne seront pas tolérées. Les manquements à cette politique sont traités comme indiqué par l'équipe de gestion des talents pour les employés, et par l'équipe des services aux partenaires et aux fournisseurs pour les travaux contractuels.

PUBLIC

Tous les employés, sous-traitants et tiers autorisés à accéder à l'information ou aux systèmes technologiques du Partenariat.

PRINCIPES

1. Les ressources informationnelles et de TI du Partenariat sont des biens de valeur qui demandent une gestion responsable et de la diligence pour prévenir les abus, les vols et les incidents de cybersécurité.

2. Limiter l'accès aux ressources informationnelles et de TI du Partenariat et restreindre leur utilisation peut atténuer les risques d'incidents de cybersécurité et empêcher qu'on se serve de ces ressources à des fins inappropriées. Les contrôles des technologies de l'information peuvent limiter votre accès à cette fin.

3. Les appareils informatiques mobiles (qui se connectent aux systèmes et aux services du Partenariat, comme les cellulaires, les tablettes, les ordinateurs portables et d'autres appareils connectés), les supports amovibles (comme les clés USB) et les appareils appartenant aux employés utilisés pour des activités opérationnelles du Partenariat doivent être utilisés conformément à la politique d'utilisation acceptable. Cela peut inclure les technologies de gestion des appareils mobiles.

4. Les solutions en nuage et les solutions technologiques de fournisseurs tiers sont assujetties à l'approbation du directeur des technologies de l'information avant d'être mises en œuvre, et doivent être conformes à la politique d'utilisation acceptable.

RÔLE DU COMITÉ DE DIRECTION

Recevoir, examiner et adopter cette politique, ainsi que toute modification recommandée à celle-ci.

1. DÉFINITIONS

1.01 Utilisateurs autorisés – Individus qui ont reçu l'autorisation de se connecter aux systèmes et aux services du Partenariat, y compris les individus qui se connectent à distance et les utilisateurs tiers approuvés par l'autorité compétente du Partenariat.

1.02 LCAP – Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications (L.C. 2010, ch. 23)

1.03 Systèmes et services du Partenariat – L'ensemble des réseaux, de l'infrastructure technique, des applications et de la technologie des utilisateurs finaux qui sont détenus ou exploités par le Partenariat, ou qui sont connectés à son réseau.

1.04 Nuage – Services de technologie de l'information offerts lorsque l'infrastructure informatique ne se trouve pas dans les installations du Partenariat.

1.05 Cybersécurité – Ensemble de techniques utilisées pour protéger l'intégrité des réseaux, des programmes et des données contre des attaques, des dommages ou des accès non autorisés.

1.06 Solution technologique d'un fournisseur tiers – Tout service de technologie de l'information qui n'est pas fourni par le Partenariat.

1.07 Appareil – Tout article, y compris les objets personnels, ceux appartenant au Partenariat et ceux appartenant à l'État, qui peut se connecter aux systèmes et aux services du Partenariat, y compris les cellulaires, les tablettes et les ordinateurs portables.

1.08 Communications électroniques – Communications, y compris la messagerie instantanée, la messagerie vocale, l'historique de navigation Web, les journaux de vérification, les vidéos,

les courriels, ainsi que les autres documents créés, envoyés ou reçus à partir des systèmes et des services du Partenariat.

1.09 Incident de cybersécurité – Comprend les tentatives (infructueuses ou réussies) d'accès non autorisé à un système ou à ses données; l'interruption ou le refus de service non voulu; l'utilisation non autorisée d'un système pour le traitement ou le stockage des données, et les changements aux caractéristiques du matériel, des micrologiciels ou des logiciels sans que le Partenariat le sache, le demande ou donne son consentement.

1.10 Données du réseau – Toutes les données créées, reçues ou envoyées à partir des systèmes et des services du Partenariat.

1.11 Renseignements personnels – Renseignements à propos d'une personne identifiable, ou renseignements qui permettent d'identifier une personne, qu'ils soient enregistrés ou non.

1.12 TI – Technologie de l'information.

1.13 Fournisseur de services tiers – Tout tiers qui offre un service qui pourrait influer sur les systèmes et les services du Partenariat.

1.14 Contenu non autorisé – Matériel qui intimide, menace, humilie une personne ou un groupe, ou qui est discriminatoire à son égard; contenu pornographique; allusions ou représentations diffamatoires.

1.15 Activités non autorisées – Envoyer ou afficher des messages ou des images discriminatoires, harassants ou menaçants; commettre toute forme de fraude ou de vol; divulguer le mot de passe de quelqu'un sans autorisation; télécharger, copier ou pirater un logiciel, un film, de la musique ou des fichiers électroniques qui sont protégés par le droit d'auteur sans autorisation; partager des documents confidentiels, des secrets commerciaux ou des renseignements exclusifs à l'extérieur de l'organisation sans autorisation; accéder à des sites Web non autorisés; envoyer ou afficher des renseignements qui sont diffamatoires envers le Partenariat, ses produits ou services, ses collègues ou ses clients, ou consulter intentionnellement de tels renseignements; introduire un logiciel malveillant dans les systèmes et services du Partenariat; compromettre la cybersécurité des systèmes et des services du Partenariat; envoyer ou afficher des chaînes de lettres, des sollicitations ou des publicités qui ne sont pas liées à des activités ou à des fins opérationnelles sans autorisation.

POLITIQUE D'UTILISATION ACCEPTABLE

2. RESPONSABILITÉS

2.01 Comité de direction du Partenariat

(a) Recevoir, examiner et adopter cette politique, ainsi que toute modification recommandée à celle-ci.

(b) Examiner et adopter des procédures qui sont élaborées pour la mise en œuvre de cette politique.

(c) Assurer un suivi de l'application, de l'interprétation et de l'administration de cette politique.

2.02 Directeur des technologies de l'information

(a) S'assurer que les autres directeurs et gestionnaires gèrent l'utilisation autorisée des systèmes et des services du Partenariat dans leurs services respectifs.

(b) S'assurer que tous les employés et les tiers ont eu l'occasion de lire cette politique et d'obtenir des précisions à son égard.

(c) Mettre en œuvre, examiner et surveiller les normes connexes de cybersécurité, comme celles portant sur les mots de passe, l'accès à distance et les appareils mobiles.

(d) Assurer et surveiller la conformité à cette politique.

(e) S'assurer que cette politique est revue périodiquement et mise à jour au besoin.

2.03 Directeurs et gestionnaires

(a) Déterminer quels employés et tiers travaillant dans leur division doivent être des utilisateurs autorisés.

(b) Déterminer à quels systèmes, services et appareils du Partenariat chacun des employés et des tiers travaillant dans leur division aura un accès autorisé.

(c) S'assurer que tous les employés et les tiers qui travaillent dans leur division et qui sont des utilisateurs autorisés ont eu l'occasion de lire cette politique et d'obtenir des précisions à son égard.

(d) En cas d'infraction à cette politique, prendre les mesures disciplinaires pertinentes en collaboration avec l'équipe de gestion des talents.

(e) Mettre en œuvre, réviser et surveiller les normes applicables figurant dans le Manuel de cybersécurité, et veiller à ce qu'elles soient respectées.

2.04 Gestion des talents

(a) Traiter les cas de non-conformité ou les violations à la Politique et à l'utilisation acceptable des ressources des technologies de l'information du Partenariat.

(b) Transmettre les violations à cette Politique ou à l'utilisation acceptable des ressources des technologies de l'information du Partenariat au directeur des technologies de l'information, au besoin.

(c) Aider à offrir des solutions d'apprentissage en ligne aux employés du Partenariat.

2.05 Employés des technologies de l'information

(a) Fournir des outils et des solutions de formation de sensibilisation à la sécurité de l'information.

(b) Utiliser les systèmes technologiques, les journaux d'activité, les analyseurs de performance, les outils de récupération et d'archivage des données, les outils de surveillance et de filtrage, et la confirmation visuelle comme des outils de détection et de prévention des incidents de cybersécurité.

(c) Évaluer et approuver les logiciels ou le matériel à utiliser sur les systèmes et dans le cadre des services du Partenariat, ou qui seront connectés à ceux-ci.

(d) Fournir les renseignements d'utilisation et de vérification des systèmes et des services du Partenariat, selon les demandes et les besoins de l'équipe de gestion des talents.

(e) Mettre en œuvre, réviser et surveiller les normes applicables en matière de sécurité de l'information figurant dans le Manuel de cybersécurité, et veiller à ce qu'elles soient respectées.

2.06 Tous les employés, sous-traitants et utilisateurs autorisés

(a) Respecter les exigences de cette Politique d'utilisation acceptable et les normes de sécurité de l'information pertinentes décrites dans le Manuel de cybersécurité.

(b) Utiliser les systèmes et les services du Partenariat d'une manière responsable, éthique et respectueuse de la loi.

(c) Reconnaître que le Partenariat peut surveiller ses systèmes, ses services et ses appareils.

(d) Comprendre que les communications électroniques découlant d'un emploi ou d'un contrat avec le Partenariat sont considérées comme étant sa propriété.

(e) Utiliser les ressources et la formation en matière de cybersécurité du Partenariat et prendre des décisions éclairées et soucieuses de la sécurité.

(f) Signaler les violations présumées de la cybersécurité ou les incidents potentiels de cybersécurité à leur superviseur immédiat et au gestionnaire des services de TI.

(g) Protéger l'information du Partenariat, comme les justificatifs d'identité des comptes, les mots de passe, l'information électronique et les autres ressources informationnelles par rapport à l'utilisation des systèmes et des services du Partenariat.

(h) Consulter les employés des technologies de l'information pour obtenir des conseils sur la cybersécurité, en toutes circonstances.

(i) Comprendre que les employés peuvent faire un usage personnel limité de la technologie de l'information du Partenariat, conformément à cette politique et à ses normes, mais que toutes les données du Partenariat peuvent faire l'objet d'une surveillance et que l'usage personnel ne doit pas nuire au fonctionnement des systèmes et des services du Partenariat.

3. ACTIVITÉS INTERDITES

3.01 Les utilisateurs sont responsables de respecter la vie privée des autres et de protéger leur identité opérationnelle ainsi que l'accès à l'information. Les utilisateurs sont également responsables de bien utiliser les ressources technologiques et d'éviter les activités qui auraient des effets négatifs sur les autres. Utiliser les systèmes et les services du Partenariat aux fins suivantes est considéré comme un manquement à cette politique :

(a) Accéder intentionnellement à tout contenu non autorisé ou effectuer des activités non autorisées
(b) Effectuer des activités commerciales non liées à son emploi ou à son contrat au sein du Partenariat pour des gains personnels
(c) Consulter, utiliser ou divulguer sans autorisation des renseignements personnels, des renseignements confidentiels et des données exclusives du Partenariat, ou d'une autre personne ou entité avec laquelle le Partenariat fait affaire
(d) Accéder, ou tenter d'accéder, au compte d'un autre utilisateur ou à un compte d'un service en nuage sans autorisation
(e) Révéler des mots de passe ou permettre d'une autre façon à des tiers d'utiliser des comptes personnels pour accéder à un ordinateur ou au réseau (intentionnellement ou par négligence)
(f) Installer du contenu non autorisé ou sans licence
(g) Utiliser les systèmes et les services du Partenariat pour enfreindre toute loi internationale, fédérale, provinciale ou locale, y compris les lois sur la propriété intellectuelle et la LCAP
(h) Utiliser les technologies de l'information du Partenariat pour créer, stocker ou diffuser des documents qui harcèlent, intimident ou menacent des individus ou des groupes
(i) Connecter tout appareil qui n'est pas détenu par le Partenariat aux systèmes et aux services du Partenariat sans autorisation
(j) Compromettre la cybersécurité des systèmes et des services du Partenariat
(k) Utiliser les biens de TI du Partenariat d'une manière qui altère la performance des systèmes et des services du Partenariat
(l) Tenter de retirer ou de modifier un réseau ou des mesures de protection d'un appareil installés sur les systèmes et les services du Partenariat

(m) Envoyer des messages anonymes en contradiction avec les valeurs fondamentales de transparence et de responsabilisation du Partenariat

APPLICATION ET MISE EN ŒUVRE

Chaque gestionnaire est responsable de mettre en œuvre, d'examiner et de surveiller les politiques d'usage acceptable et de confidentialité des employés et de veiller à ce qu'elles soient respectées.

La non-conformité à cette politique fera l'objet d'une enquête et des mesures peuvent être recommandées, conformément aux directives de l'équipe de gestion des talents du Partenariat et du directeur des technologies de l'information.

Exceptions : Il y a très peu de situations, voire aucune, dans lesquelles une exception à cette politique sera accordée. Toutes les exceptions doivent être approuvées par le directeur des technologies de l'information.

Cette politique remplacera toutes les politiques d'utilisation acceptable antérieures du Partenariat. Cette politique peut être modifiée ou révisée à tout moment. Les utilisateurs sont responsables de consulter cette politique régulièrement, afin de voir si des révisions y ont été apportées, et, le cas échéant, de les respecter.

Annexe A – Consentement à la Politique d'utilisation acceptable pour les employés et les sous-traitants

Je reconnais avoir lu la Politique d'utilisation acceptable du Partenariat canadien contre le cancer et je comprends mes obligations à titre d'employé de me conformer aux normes décrites dans cette Politique. Je comprends que cet accès n'est autorisé qu'à des fins opérationnelles, et qu'il est assujetti à toute exception à la présente politique. Je comprends que le Partenariat ne peut pas restreindre l'accès à tout contenu controversé et inapproprié, et qu'il ne sera pas tenu responsable des contenus acquis sur le réseau.

Enfin, je comprends que toute infraction à cette politique peut avoir des conséquences allant du retrait des privilèges d'accès à la suspension ou à la cessation d'emploi, et que le Partenariat se réserve le droit de signaler toute activité illicite aux forces de l'ordre et de coopérer à toute enquête sur une telle activité.

Le Partenariat ne considère pas qu'une conduite qui viole la présente politique soit dans le cadre de l'emploi d'un employé ou d'un sous-traitant, ni qu'elle soit la conséquence directe de l'exercice des fonctions de l'employé ou du sous-traitant. Par conséquent, dans la mesure permise par la loi, le Partenariat se réserve le droit de ne pas défendre les employés ou les partenaires qui ont enfreint la présente politique, ou de ne pas payer les dommages-intérêts infligés aux employés ou aux partenaires qui découlent d'une infraction à la présente politique.

Signé le _____ jour de _____ 20__

Nom de l'employé ou du sous-traitant : _____

Signature de l'employé ou du sous-traitant : _____