Politique de classification des renseignements

1.1 Aperçu

Le Cadre de sécurité et de protection des renseignements personnels du Partenariat intègre une politique de classification des renseignements. Lors de l'élaboration de stratégies de stockage, de sécurisation et de gestion des renseignements, de leur création à leur destruction, il est essentiel de comprendre l'importance de différencier et de séparer les renseignements qui sont de nature délicate et ceux qui ne le sont pas. Ce faisant, il devient possible de mettre en œuvre des contrôles de sécurité et de protection des renseignements appropriés et proportionnels à leur degré de sensibilité.

La classification des renseignements est un *processus* regroupant les ressources informationnelles dans différentes catégories en fonction de leurs caractéristiques en matière de sensibilité. Ce processus de classification s'appuie sur lesdites caractéristiques pour regrouper les renseignements au sein de classes définies auxquelles l'on associe différentes répercussions en cas de compromission ou de modification.

Ce document définit des classes visant à garantir la protection des renseignements en conformité avec leur degré de sensibilité. Le Partenariat pourrait, à sa seule discrétion, imposer des classifications supplémentaires.

1.2 But

Ce document a pour but de fournir des orientations sur la classification et la manipulation des renseignements et de présenter les différentes classes de renseignements du Cadre de sécurité et de protection des renseignements personnels du Partenariat. Afin de faciliter la compréhension et le respect de cette politique, l'ensemble du personnel du Partenariat recevra une formation de sensibilisation à la sécurité et à la protection des renseignements personnels.

1.3 Portée

Cette politique s'applique à l'ensemble du personnel, des consultants et des sous-traitants manipulant des renseignements administrés par le Partenariat ou qui sont sous son contrôle ainsi qu'à ceux mettant en œuvre des contrôles en matière de sécurité et de protection des renseignements sur les ressources de technologies de l'information (TI) du Partenariat.

1.4 Énoncé de politique

i. Afin de protéger les renseignements en fonction de leur degré de sensibilité, il conviendra tout d'abord de recenser les ressources informationnelles afin de procéder à leur évaluation sur les plans de la confidentialité, de l'intégrité et de la disponibilité. Pour ce faire, le Partenariat s'appuie, en tant que référence pour une telle évaluation de ces ressources, sur la norme de classification des renseignements du guide de classification aux fins de la sécurité de l'information et de la protection de la vie privée du gouvernement de l'Ontario. Cette norme a été largement adoptée dans le secteur des soins de santé en Ontario et fournit une orientation appropriée en matière d'évaluation globale des ressources informationnelles.

ii. Les renseignements dans un état « final » ou qui sont publiés, administrés ou produits et détenus par le Partenariat devront être classés dans l'une des quatre catégories suivantes :

- **Renseignements publics –** renseignements que le public ainsi que le personnel, les consultants et les sous-traitants travaillant pour le Partenariat peuvent consulter.
- **Renseignements internes –** renseignements que le personnel et les personnes autorisées ne faisant pas partie du personnel (consultants et sous-traitants) peuvent consulter en vue de répondre à un « besoin de savoir » pour des motifs professionnels.
- **Renseignements confidentiels –** renseignements de nature délicate présents au sein du Partenariat destinés à n'être utilisés que par certains groupes de membres du personnel; une violation de la confidentialité de ces renseignements pouvant s'avérer très embarrassante pour le Partenariat et miner la confiance que lui accorde le public.
- **Renseignements à diffusion restreinte –** renseignements de nature extrêmement délicate destinés à n'être utilisés que par certaines personnes ou par les titulaires de certains postes; une violation de la sécurité de ces renseignements pouvant mettre en danger la santé, la sécurité, la vie privée ou la réputation d'une personne, de membres du public ou d'abonnés ainsi que celles du Partenariat, de membres de son personnel, de ses consultants, de ses sous-traitants ou de sa clientèle organisationnelle.

Veuillez vous reporter au tableau aux pages suivantes pour consulter les détails associés à chaque classe de renseignements.

iii. Il incombera à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat manipulant des renseignements administrés par le Partenariat ou qui sont sous son contrôle de comprendre et d'appliquer cette politique.

iv. Il incombera à l'ensemble du personnel, des consultants et des sous-traitants du Partenariat mettant en œuvre des contrôles sur ses systèmes TI en matière de sécurité et de protection des renseignements personnels de veiller à ce que lesdits contrôles soient appropriés et proportionnels au degré de sensibilité des renseignements gérés.

v. Tous les renseignements classifiés comme internes, confidentiels ou à diffusion restreinte devront faire l'objet de contrôles suffisants en matière de sécurité et de protection des renseignements personnels afin que l'accès à ces renseignements soit réservé aux seuls utilisateurs autorisés.

Classification des renseignements	Description	Exemples de ressources informationnelles	Répercussions du risque	Exigences en matière de sécurité d'accès
Publics	Renseignements accessibles au grand public, aux partenaires et au personnel	• Contenu du site Web du Partenariat • Rapports publiés • Matériels promotionnels • Offres d'emploi • Présentations externes	• Aucune répercussion • Inconvénient minimal en cas de non-disponibilité	Aucune
Internes	Renseignements accessibles au personnel et aux personnes autorisées ne faisant pas partie du personnel (consultants et sous-traitants) ayant un « besoin de savoir » pour accomplir leurs tâches opérationnelles	• Documents de planification • Rapports d'avancement de projets • Ordre du jour et procès-verbal de réunions • Documents contenant des coordonnées professionnelles • Documents de planification stratégique • Documents opérationnels • Politiques et procédures • Conseils d'orientation stratégique	• Perturbation des activités en cas de non-disponibilité • Faible degré de risque en cas de corruption ou de modification	Nécessité d'une authentification améliorée à un facteur pour l'accès des utilisateurs au réseau du Partenariat et d'un système de gestion des dossiers

Confidentiels	Renseignements exclusivement accessibles aux personnes appartenant à un groupe particulier ou occupant une fonction ou un poste spécifiques	• Fichiers du personnel • Renseignements bancaires de personnes ne faisant pas partie du personnel du Partenariat • Contrats • Rapports financiers • Délibérations et documents complémentaires du comité de direction du conseil d'administration et des autres comités du conseil d'administration • Renseignements des partenaires désignés comme étant de nature délicate • Renseignements commerciaux de tiers transmis avec la mention « Confidentiel » • Renseignements sur les rémunérations • Conseils juridiques • Fichiers de signatures électroniques • Demandes de propositions et demandes de financement non attribuées • Enregistrements audio de réunions	• Atteinte à la réputation ou perte d'un avantage concurrentiel • Perte de confiance dans le Partenariat • Atteinte à la vie privée • Perte de renseignements personnels • Atteinte à la propriété intellectuelle • Occasion manquée • Perte financière • Degré élevé de risque en cas de corruption ou de modification • Compromission des délibérations du conseil d'administration • Violation de la vie privée	Contrôle d'accès au niveau du dossier uniquement pour les utilisateurs autorisés

			• Destruction de partenariats et de relations	

Classification des renseignements	Description	Exemples de ressources informationnelles	Répercussions du risque	Exigences en matière de sécurité d'accès
À diffusion restreinte	Renseignements exclusivement accessibles à certaines personnes en particulier ou aux titulaires de certains postes	• Casiers et enquêtes judiciaires • Dossiers de procédure • Bases de données comme le registre du cancer • Renseignements personnels sur la santé tels qu'ils sont décrits dans la *Loi sur la protection des renseignements personnels sur la santé de l'Ontario* (LPRPS)	• Blessure grave • Atteinte à la sécurité publique • Importantes pertes financières • Conséquences juridiques notables • Dommages importants	Authentification de l'utilisateur à deux facteurs requise

1.5 Contrôle de l'application de la politique

En cas de non-respect de cette politique, le Partenariat pourra, sans que cela soit limitatif, prendre les mesures suivantes :

I. Refuser l'accès à ses ressources informationnelles et TI.
II. Mettre en œuvre, pour les fournisseurs indépendants, les consultants ou les sous-traitants, les recours contractuels appropriés, par exemple les dispositions relatives aux manquements au contrat ou à sa résiliation.
III. Mettre en œuvre, pour le personnel, des mesures disciplinaires pouvant inclure, sans que cela soit limitatif, un avertissement écrit, une suspension avec ou sans traitement ou un licenciement immédiat motivé sans aucun préavis ni autre obligation.

1.6 Définitions

Terme	Définition
Renseignements contrôlés	Renseignements administrés par le Partenariat (voir la définition ci-après) recueillis, acquis, mis à jour, supprimés, utilisés et divulgués à la discrétion du Partenariat et dans les limites de la loi
Renseignements administrés	Renseignements conservés ou stockés par le Partenariat dans ses bureaux, ses installations, ses meubles de rangement ou ses ordinateurs
Ressources informationnelles et TI	Matériel informatique (y compris les ordinateurs portatifs et de bureau), logiciels, systèmes d'exploitation, supports de stockage, comptes réseau, courrier électronique, accès Internet, portails, passerelles, appareils réseau, appareils mobiles, serveurs, téléphones et systèmes téléphoniques, imprimantes multifonctions, ordinateurs personnels et domestiques connectés au réseau du Partenariat, directement ou par l'entremise d'une connexion VPN, ressources informationnelles (quel que soit le support ou le

	format), par exemple les renseignements commerciaux ou personnels, ainsi que tout autre élément que le Partenariat pourrait considérer comme une ressource informationnelle ou TI
Cadre de sécurité et de protection des renseignements personnels	Ensemble des politiques, des normes, des outils, des gabarits, des processus et des procédures qui régissent, individuellement et collectivement, la confidentialité, la protection et la sécurité des ressources informationnelles et TI du Partenariat
Authentification améliorée de l'utilisateur à un ou à deux facteurs	L'accès à certains renseignements ou à certaines technologies de l'information du Partenariat peut nécessiter une authentification améliorée de l'utilisateur à un facteur ou à deux facteurs, exigeant, respectivement, avant que l'accès ne soit autorisé, deux éléments connus de la personne autorisée à accéder à ces renseignements ou à ces technologies, et deux facteurs indépendants, par exemple un élément détenu par la personne autorisée et un élément qu'elle connaît. Ces facteurs d'authentification peuvent comprendre : • Un nom d'utilisateur et un mot de passe valides émis par le Partenariat et attribués à une personne afin qu'elle puisse accéder à certains de ses renseignements ou à certaines de ses technologies de l'information • Des moyens de contrôle de sécurité relatifs à l'accès physique aux installations du Partenariat, par exemple des cartes d'accès valides à certains étages, ascenseurs ou à certaines zones

	• Une entente entre le Partenariat et une organisation tierce dans le cadre de laquelle cette dernière s'engage à veiller à ce que tout utilisateur, qu'il soit membre de son personnel ou qu'il agisse à titre d'agent, respecte les politiques applicables du Partenariat en matière de sécurité et de protection des renseignements • Un jeton de sécurité émis par le Partenariat et attribué à une personne afin qu'elle puisse accéder à certains de ses renseignements ou à certaines de ses technologies de l'information

1.7 Documents connexes

- Politique de gestion de l'information
- Politique de gestion des dossiers
- Politique de sécurité de l'information et des technologies de l'information
- Politique de protection des renseignements personnels
- Politique d'utilisation acceptable

Fin du document