Politique de sécurité de l'information et des technologies de l'information

1.1 Aperçu

Dans notre monde d'aujourd'hui, interconnecté et marqué par l'omniprésence de la haute technologie, la sécurité est au cœur des préoccupations du Partenariat afin de protéger ses ressources informationnelles et de technologies de l'information (TI) contre les menaces provenant de sources internes et externes. En conformité avec cet objectif, la présente politique fournit au Partenariat des orientations en matière de gestion des mesures à prendre en vue de sécuriser ses ressources informationnelles et TI. La Politique de sécurité de l'information et des technologies de l'information constitue en outre la clé de voûte sur laquelle s'appuie la vision plus globale du Partenariat en matière de gestion du risque décrite dans sa Politique sur la gestion du risque d'entreprise. On trouvera dans d'autres composantes du Cadre de sécurité et de protection des renseignements personnels du Partenariat les détails sur le processus de mise en œuvre de la présente Politique de sécurité de l'information et des technologies de l'information. Le Partenariat pourrait, à sa seule discrétion, imposer des directives supplémentaires en la matière.

1.2 But

La présente politique a pour but de définir des règles en matière de configuration et de gestion de la sécurité de façon à ce qu'elle protège les ressources informationnelles et TI du Partenariat. Ces règles sont fondées sur les normes internationales suivantes :

i. ISO/CEI 27001 « Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Exigences »
ii. ISO/CEI 27002 « Technologies de l'information – Techniques de sécurité – Code de bonne pratique pour le management de la sécurité de l'information »
iii. ISO/CEI 27005 « Technologies de l'information – Techniques de sécurité – Gestion des risques liés à la sécurité de l'information »

La présente politique permet au Partenariat de minimiser ses risques et de faire preuve de diligence vis-à-vis de ses partenaires, des intervenants et du grand public. 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 du Partenariat accédant à ses ressources informationnelles par l'entremise de ses ressources TI.

1.4 Énoncé de politique

1.4.1 Gouvernance

i. Il incombera à l'agent en chef de la sécurité et de la protection des renseignements personnels du Partenariat de publier cette politique et d'en contrôler l'application.

ii. Il incombera à l'agent en chef de la sécurité et de la protection des renseignements personnels du Partenariat de veiller à l'examen périodique de cette politique et à sa mise à jour, le cas échéant.

1.4.2 Responsabilités de l'organisation

i. Il incombera à la direction du Partenariat de définir des orientations et d'appuyer cette politique.

ii. Il incombera à la direction du Partenariat de confirmer, au moins tous les deux ans, que l'organisation respecte cette politique.

1.4.3 Gestion des actifs

i. Il conviendra d'établir un inventaire de tous les actifs importants de l'organisation (matériels ou immatériels) associés à l'information et aux technologies de l'information et de le tenir à jour.

ii. Il conviendra de désigner un propriétaire pour chacun des actifs associés au traitement et au stockage de l'information.

iii. Il conviendra de déterminer, de documenter et de mettre en œuvre des règles définissant les utilisations et les éliminations acceptables des actifs du Partenariat.

1.4.4 Classification des renseignements

i. Il incombera au Partenariat de définir des classes de renseignements en fonction de leur degré de sensibilité.

ii. Les évaluations de la sécurité et de la protection des renseignements personnels, effectuées par le Partenariat ou en son nom, devront s'appuyer sur le tableau de classification du Partenariat.

iii. Les renseignements devront être recensés, « étiquetés » lorsqu'il y a lieu et manipulés en conformité avec le tableau de classification du Partenariat.

1.4.5 Sécurité en matière de ressources humaines

i. Les membres du personnel, les consultants et les sous-traitants du Partenariat devront subir une enquête de sécurité avant d'entamer une relation professionnelle avec l'organisation. Le niveau de contrôle de cette enquête devra être adapté au degré de confiance requis pour mener à bien les tâches associées à ladite relation. À titre d'exemple, les personnes devant accéder à des renseignements **confidentiels** ou **à diffusion restreinte** dans le cadre de leurs fonctions devront subir une vérification des antécédents conduite par le Centre d'information de la police canadienne (CIPC).

ii. Les membres du personnel, les consultants et les sous-traitants devant accéder à des renseignements **confidentiels** ou **à diffusion restreinte** dans le cadre de leurs fonctions devront signer l'entente de confidentialité du Partenariat.

iii. Les membres du personnel, les consultants et les sous-traitants devront recevoir une formation de sensibilisation appropriée à la sécurité de l'information et des technologies de l'information et être tenus informés des évolutions de la présente politique.

iv. Les responsabilités en matière de sécurité devront être documentées dans le cadre des différentes relations établies entre le Partenariat, d'une part, et les membres du personnel, les consultants et les sous-traitants, d'autre part, notamment dans le cas de la cessation du contrat qui les lie.

v. À l'issue de leur relation avec le Partenariat ou, s'il y a lieu, à l'occasion d'un changement d'emploi ou de l'instauration d'un autre type de relation, les membres du personnel, les consultants et les sous-traitants devront rendre au Partenariat les actifs qui peuvent être en leur possession.

vi. Les droits d'accès des membres du personnel, des consultants et des sous-traitants à l'information et aux technologies de l'information devront être supprimés immédiatement à l'issue de l'emploi ou de tout autre type de relation avec le Partenariat; en outre, lesdits droits devront être revus lors d'un changement d'emploi ou lors de l'instauration d'un autre type de relation.

1.4.6 Sécurité physique et sécurité de l'environnement

i. Les installations de traitement de l'information du Partenariat (par exemple les centres de données et les armoires abritant les installations des réseaux locaux) devront être protégées par un périmètre de sécurité physique.
ii. Les exigences en matière de sécurité physique devront être conçues et documentées pour toutes les zones situées à l'intérieur d'une installation de traitement de l'information ainsi que pour les environs d'une telle zone, et y être appliquées.
iii. Les zones de travail du Partenariat devront être protégées par des contrôles d'entrée appropriés afin de garantir que seul le personnel autorisé peut y accéder. À titre d'exemple, les visiteurs et le personnel de service ne pourront pénétrer dans les zones de travail du Partenariat à moins d'être escortés par un membre du personnel.

1.4.7 Sécurité des équipements

i. Les équipements devront être protégés, en proportion de leurs exigences en matière de disponibilité, vis-à-vis des pannes de courant et autres perturbations causées par des défaillances des services publics.
ii. Les câbles d'alimentation et de télécommunication devront être protégés vis-à-vis des interceptions et des dommages.
iii. Les équipements devront être correctement entretenus afin de protéger, en tout temps, leur disponibilité et leur intégrité.
iv. Les équipements situés à l'extérieur des locaux du Partenariat devront être protégés à l'aide de contrôles de sécurité documentés. Un tel contrôle pourrait, par exemple, consister à interdire de laisser des dossiers ou des ordinateurs portables dans des véhicules non verrouillés ou posés sur des sièges où ils pourraient être visibles des passants.
v. Les renseignements, les dossiers et les logiciels devront être protégés contre toute divulgation non autorisée, pendant et après la réaffectation ou la destruction des ordinateurs ou des supports informatiques sur lesquels ils se trouvaient.
vi. Les équipements, les renseignements ou les logiciels appartenant au Partenariat ou qui sont sous son contrôle ne devront pas être sortis des locaux qui lui appartiennent ou qu'il loue, sans son autorisation préalable.
vii. Les ordinateurs portatifs présents dans les locaux devront être sécurisés en tout temps. Lorsqu'ils ne sont pas utilisés, ils devront, par exemple, être verrouillés à un meuble fixe, ou rangés dans un bureau verrouillé ou, à défaut, dans une armoire munie d'un verrou.

1.4.8 Norme relative à la sécurité de l'infrastructure TI

i. L'infrastructure TI (par exemple les serveurs et le réseau d'entreprise) constitue la clé de voûte sur laquelle le Partenariat s'appuie pour fournir les services relevant de son mandat. La mise en œuvre efficace de mesures de sécurité portant sur toutes les composantes de l'infrastructure TI permet de réduire le risque de consultation, d'utilisation et d'exploitation non autorisées de l'information et des TI du Partenariat. Il incombera donc au Partenariat de documenter et de mettre en œuvre des pratiques exemplaires en vue de sécuriser son infrastructure TI.

1.4.9 Nom d'utilisateur, mot de passe et contrôles administratifs

i. Les noms d'utilisateur, les mots de passe et les autres contrôles administratifs du même type constituent un fondement essentiel de la sécurité informatique. Ils représentent la première ligne de protection des comptes utilisateur. Des noms d'utilisateur et des mots de passe mal conçus peuvent affaiblir la sécurité des technologies de l'information du Partenariat. C'est pourquoi il incombera au Partenariat de documenter et de mettre en œuvre des pratiques exemplaires en matière de robustesse et de complexité des mots de passe, de chiffrement acceptable et d'autres contrôles administratifs du même type.

1.4.10 Appareils mobiles

i. Étant donné que les employés du Partenariat peuvent se connecter au réseau d'entreprise à l'aide d'un appareil mobile, les renseignements privés et confidentiels devront être protégés vis-à-vis de toute divulgation, délibérée ou involontaire, pouvant entraîner une perte d'information, des dommages à des applications critiques et une atteinte à la réputation du Partenariat. C'est pourquoi il incombera au Partenariat de documenter et de mettre en œuvre des pratiques exemplaires en matière d'utilisation d'appareils mobiles personnels et d'entreprise pour accéder au réseau et aux systèmes de l'entreprise.

1.4.11 Destruction des supports de stockage

i. Le Partenariat crée, recueille, stocke et traite des renseignements personnels et des renseignements commerciaux confidentiels qui constituent sa propriété intellectuelle. L'élimination, sans avoir détruit préalablement les données de nature délicate qu'ils contiennent, d'ordinateurs de bureau, d'ordinateurs portables et de supports électroniques devenus inutiles pourrait, sans nécessité, mettre le Partenariat en situation de violation de

la vie privée ou l'amener à subir un contentieux. C'est pourquoi il incombera au Partenariat de documenter et de mettre en œuvre des contrôles efficaces de destruction des supports informatiques de façon à empêcher toute récupération des données qu'ils contiennent.

1.4.12 Accès à l'information et aux technologies de l'information du Partenariat

I. L'accès à l'information et aux technologies de l'information du Partenariat devra exploiter des contrôles proportionnels à leur importance et à leur sensibilité ainsi qu'un processus de connexion sécurisé.
   a) Chaque accès à l'information ou aux technologies de l'information du Partenariat devra suivre un processus d'autorisation clairement défini et faisant l'objet d'un suivi; l'autorisation d'accès devant être officiellement accordée par le ou les propriétaires du système, du processus opérationnel ou de l'information concernés.
   b) L'attribution de privilèges système ou d'autorisations d'accès devra être restreinte et contrôlée selon les principes du « droit d'accès minimal » et de la « séparation des responsabilités ».
   c) Les utilisateurs devront uniquement avoir accès aux systèmes d'information et aux technologies pour lesquels ils ont explicitement reçu une autorisation d'utilisation.
   d) Pendant la durée de l'autorisation, il conviendra de mettre en place des restrictions particulières en matière de connexion et d'horaires afin d'offrir une sécurité accrue pour les applications particulièrement sensibles.

II. L'accès de tiers à l'information ou aux technologies de l'information du Partenariat devra exploiter des contrôles d'autorisation proportionnels à l'importance et à la sensibilité de cette information ou de ces technologies de l'information.
   a) Les organisations tierces devront convenir par écrit ou par contrat de veiller à ce que tout utilisateur, qu'il fasse partie de leur personnel ou qu'il agisse en tant qu'agent, s'engage à se conformer aux politiques applicables du Partenariat en matière de sécurité et de protection des renseignements personnels avant de recevoir une autorisation d'accès.

III. Tous les accès à l'information ou aux technologies de l'information du Partenariat devront exploiter des techniques et des mécanismes d'authentification appropriés proportionnels à leur importance et à leur sensibilité. Les options d'authentification pourront inclure :
   a) Un nom d'utilisateur et un mot de passe.

b) Une authentification améliorée à un facteur exigeant deux informations relatives à l'utilisateur pour valider l'authentification.
c) Une authentification à deux facteurs exigeant deux facteurs indépendants relatifs à l'utilisateur (par exemple, un élément détenu par une personne autorisée et un élément connu d'une personne autorisée) pour valider l'authentification.
d) L'authentification devra, au minimum, inclure un nom d'utilisateur et un mot de passe valides, créés par le Partenariat et remis à une personne afin qu'elle puisse accéder à l'information et aux technologies de l'information dont elle a besoin.
e) L'accès à l'information ou aux technologies de l'information du Partenariat pourra intégrer un processus d'authentification améliorée, prévoyant notamment le recours à des jetons de sécurité.
f) Une authentification robuste ou améliorée devra être employée pour contrôler l'accès aux renseignements **confidentiels**.
g) Une authentification à deux facteurs devra être employée pour contrôler l'accès à des renseignements **à diffusion restreinte**.
h) Tous les accès à distance à l'information du Partenariat à partir d'un appareil qui ne lui appartient pas devront exploiter un processus d'authentification à deux facteurs.

IV. L'accès de tiers à l'information ou aux technologies de l'information du Partenariat devra exploiter des contrôles d'authentification proportionnels à leur importance et à leur sensibilité.
a) Il incombera au Partenariat d'envisager d'intégrer un processus d'authentification améliorée ou à deux facteurs, prévoyant notamment le recours à des jetons de sécurité, dans le cadre de l'accès de tiers à son information ou à ses technologies de l'information.
b) Il incombera au Partenariat de documenter et de mettre en œuvre des politiques et des pratiques exemplaires en matière de consultation de renseignements personnels par des tiers et de diffusion de ces renseignements à des tiers.

1.4.13 Protection des technologies et de l'information du Partenariat

i. L'ensemble du personnel devra posséder un laissez-passer ou une autorisation de sécurité valide pour accéder aux locaux du Partenariat, sous la forme, par exemple, de cartes d'accès valides à certaines zones, à certains étages ou ascenseurs.

ii. Il incombera aux utilisateurs de veiller à ce que les équipements non utilisés soient adéquatement protégés.

iii. Il incombera aux utilisateurs de veiller à la sécurité des renseignements de nature délicate, qu'ils soient sous forme électronique ou imprimée, et de les protéger vis-à-vis de toute consultation non autorisée, de toute perte ou de tout dommage. Il incombera aux utilisateurs de veiller à ce que leurs mots de passe, leurs jetons sécurisés, leurs certificats numériques et tous les autres identifiants qu'ils utilisent pour obtenir un accès, direct ou indirect, aux produits, aux services ou à l'infrastructure technologique du Partenariat soient protégés. Au besoin, le Partenariat pourra fournir aux utilisateurs des caches de préservation de la confidentialité pour leurs écrans.

iv. Tous les supports informatiques amovibles devront être gérés dans le cadre de contrôles correspondant au niveau de sensibilité le plus élevé des données qu'ils contiennent. Tous les supports informatiques amovibles devront être analysés avant d'être connectés au réseau d'entreprise.

v. Afin que les renseignements concernés restent protégés lors de leur transfert par tous les types de services de communications électroniques, il conviendra de documenter et de mettre en œuvre des politiques, des procédures et des contrôles en matière d'échange de renseignements avec des tiers.

vi. Les ententes d'échange de renseignements et de logiciels entre le Partenariat et d'autres organisations ou tierces parties devront être documentées et devront contenir des exigences en matière de sécurité et de protection des renseignements personnels ainsi que des rôles et des responsabilités clairement définis en la matière.

vii. Les renseignements hébergés sur des services Web ou des systèmes d'information transactionnels devront être protégés contre les activités frauduleuses, la répudiation, la divulgation non autorisée et la modification.

viii. Les systèmes d'information utilisant des services Web ou des transactions en ligne devront être dotés de contrôles de sécurité en rapport avec la valeur et la classification des renseignements concernés.

1.4.14 Sécurité des réseaux et des équipements réseau

i. L'accès physique et logique aux ports de diagnostic devra être contrôlé de manière sécurisée.

ii. Afin de permettre la mise en place d'un modèle d'accès par zone, des groupes de services d'information, d'utilisateurs et de systèmes d'information devront être séparés sur les réseaux.

iii. L'utilisation des utilitaires système permettant de gérer et de contrôler les systèmes et le réseau du Partenariat devra être limitée aux utilisateurs autorisés et faire l'objet d'un contrôle strict.

iv. Afin d'atteindre un niveau de sécurité sur le réseau du Partenariat conforme aux niveaux de tolérance au risque définis et de le maintenir, des contrôles appropriés de la sécurité du réseau devront être mis en œuvre.

v. Les sessions inactives devront être verrouillées après une période d'inactivité déterminée.

vi. Afin de protéger les technologies de l'information contre les codes malveillants, il conviendra d'utiliser des contrôles de prévention et de détection.

vii. Les supports informatiques devant être transportés physiquement devront faire l'objet d'une protection appropriée soit sous la forme de verrous physiques sécurisés, soit sous la forme d'un chiffrement.

1.4.15 Opérations

i. Les procédures opérationnelles et la gestion des responsabilités relatives aux systèmes d'information et aux installations de traitement de l'information devront faire l'objet d'un processus d'autorisation, être documentées et maintenues.

ii. Afin de réduire les possibilités de modification ou d'utilisation non autorisée ou malveillante des systèmes d'information, il conviendra de séparer les tâches et les domaines de responsabilité.

iii. Les fonctionnalités et les attentes en matière de sécurité, les rôles et les responsabilités du fournisseur et du Partenariat, les niveaux de service et les exigences relatives à la gestion de tous les services réseau devront être documentés et intégrés à tout contrat portant sur ce type de services.

iv. L'utilisation des ressources TI devra être suivie et optimisée, et des projections des besoins futurs en matière de capacités devront être établies.

1.4.16 Suivi et surveillance

i. Les exigences relatives à la sécurité devront être recensées et prises en compte avant d'accorder un accès à l'information ou aux technologies de l'information à une partie externe. Le Partenariat devra régulièrement suivre et passer en revue les services, les rapports et les dossiers fournis par les parties externes, et mener des vérifications régulières.

ii. Des journaux de vérification devront consigner les activités des utilisateurs, les exceptions et les événements de sécurité de l'information. Les entrées de ces journaux, qui contribueront

à la surveillance des contrôles d'accès et faciliteront de futures enquêtes éventuelles, devront être régulièrement examinées dans le cadre de procédures opérationnelles normalisées.

iii. Les systèmes de journalisation des systèmes d'information et les données qu'ils contiennent devront être protégés contre toute tentative de falsification et d'accès non autorisé.

iv. Les principales activités des utilisateurs privilégiés devront faire l'objet d'examens périodiques détaillés.

v. En vue de permettre l'établissement de rapports précis, les horloges des ordinateurs devront être synchronisées par rapport à une source centralisée fiable.

1.4.17 Gestion du changement

i. Les processus de gestion du changement relatifs aux services de systèmes d'information fournis par des parties externes devront prendre en compte l'importance de chacun de ces systèmes ainsi que les processus concernés et intégrer une évaluation des risques.

ii. Les modifications apportées aux systèmes d'information et aux installations de traitement de l'information devront être contrôlées.

iii. Les modifications apportées aux systèmes d'information ou à des composants de traitement de l'information existants devront faire l'objet d'une évaluation préalable des risques de sécurité sur laquelle s'appuiera le processus d'approbation desdites modifications.

iv. Les environnements de développement et de simulation des systèmes d'information devront être séparés des environnements de production opérationnelle.

v. Toutes les modifications apportées aux technologies et aux systèmes devront être approuvées à la suite d'un examen effectué par un conseil consultatif sur les changements.

1.4.18 Évaluation des risques

i. La mise en place de nouveaux systèmes d'information et de nouvelles infrastructures nécessite une évaluation des risques en matière de sécurité sur laquelle s'appuiera la Norme de certification du Partenariat.

1.4.19 Formation et sensibilisation

i. Il incombera au Partenariat d'élaborer et de gérer un programme de sensibilisation et de formation en matière de sécurité de la GI et des TI destiné à l'ensemble du personnel.

1.4.20 Systèmes tiers

i. Il incombera au Partenariat d'autoriser la publication de renseignements sur des systèmes d'information accessibles au public, et de mettre en œuvre des processus visant à empêcher toute modification non autorisée de ces renseignements.

ii. Avant leur utilisation par les membres du personnel, il incombera au Partenariat d'approuver toutes les technologies tierces appartenant à des entités externes et tous les services d'infonuagique.

iii. Il incombera au Partenariat de contrôler le téléversement ou le transfert de ses renseignements vers des sites publics et d'empêcher l'utilisation de services non autorisés ou non approuvés tels que Dropbox, SkyDrive et Google Drive.

1.4.21 Stockage électronique des renseignements confidentiels et à diffusion restreinte

i. Tous les renseignements **confidentiels ou à diffusion restreinte** conservés sous forme électronique devront être stockés sur des serveurs du Partenariat, tels que ses lecteurs réseau partagés, ou sur des systèmes autonomes matériellement sécurisés. Une telle procédure garantira, d'une part, l'exploitation de ces types de renseignements sur les systèmes TI du Partenariat qui font l'objet d'une sauvegarde régulière et, d'autre part, l'activation de protections par mot de passe ainsi qu'un niveau de sécurité physique plus élevé par rapport à celui des ordinateurs de bureau et des ordinateurs portables.

ii. Les renseignements **confidentiels ou à diffusion restreinte** ne devront pas être stockés sur des ordinateurs portables ou des périphériques USB, sauf s'ils sont chiffrés en conformité avec la Norme relative au chiffrement acceptable du Partenariat et si lesdits périphériques sont conservés au sein d'une zone sécurisée.

iii. Les renseignements **confidentiels ou à diffusion restreinte** ne devront pas être stockés sur des appareils mobiles ou d'autres supports amovibles en conformité avec la Politique sur les appareils mobiles.

iv. Les renseignements **confidentiels ou à diffusion restreinte** ne devront être ni stockés, ni publiés, ni téléversés sur des services en ligne ou des outils de travail collaboratif sans l'approbation du directeur des technologies de l'information du Partenariat.

1.4.22 Réseaux sans fil

i. Sauf approbation expresse du directeur des technologies de l'information, les systèmes et les appareils TI du Partenariat ne devront pas être connectés à des réseaux sans fil dont il

n'est ni détenteur ni gestionnaire. Pour de plus amples renseignements, veuillez consulter la Norme relative à l'accès à distance.

1.4.23 Impressions sur papier (imprimante ou télécopie)

i. Les impressions peuvent contenir des renseignements **confidentiels ou à diffusion restreinte**. C'est pourquoi il conviendra de récupérer rapidement de telles impressions afin de ne pas les laisser sans surveillance dans une imprimante ou sur un bureau.
ii. Les imprimantes ou les télécopieurs situés dans des aires communes non surveillées ne devront pas être utilisés pour imprimer des documents contenant des renseignements **confidentiels ou à diffusion restreinte**, sauf si de telles impressions sont protégées par mot de passe.
iii. Les impressions contenant des renseignements **confidentiels ou à diffusion restreinte** devront être éliminées en toute sécurité en utilisant les boîtes à déchiquetage désignées.

1.4.24 Réseaux sociaux et outils connexes

i. Les utilisateurs des technologies de l'information du Partenariat ayant une activité sur les réseaux sociaux seront assujettis aux lignes directrices et aux conditions définies dans la Politique d'utilisation acceptable et dans la Politique relative aux médias sociaux du Partenariat.
ii. L'utilisation des médias sociaux ainsi que des outils de productivité ou de travail collaboratif qui ne sont ni détenus ni gérés par le Partenariat sera préalablement soumise à une approbation et à une autorisation officielles.

1.4.25 Accès à distance aux systèmes du Partenariat

i. L'accès aux systèmes TI du Partenariat depuis l'extérieur de ses locaux sera octroyé en conformité avec la Norme relative à l'accès à distance. On exigera du personnel accédant aux systèmes TI du Partenariat depuis l'extérieur de ses locaux qu'il soit familier avec cette norme et qu'il mette tout en œuvre pour que les accès qu'il effectue respectent l'ensemble de ses exigences.

1.4.26 Gestion des vérifications et de la vulnérabilité

i. Les utilisateurs des technologies de l'information du Partenariat à qui incombera la gestion des vérifications et de la vulnérabilité seront assujettis aux conditions énoncées dans la

Norme relative à la gestion des vérifications et de la vulnérabilité ainsi que dans la Norme relative à la gestion des correctifs.

1.4.27 Gestion des incidents de sécurité de l'information

i. Les incidents de sécurité de l'information devront être signalés par l'entremise des canaux appropriés aussi rapidement que possible en conformité avec la Procédure relative à la réponse aux incidents de sécurité de l'information.

ii. Il incombera aux personnes utilisant les technologies de l'information du Partenariat de prendre note de toutes les faiblesses observées ou présumées desdites technologies en matière de sécurité et de les signaler.

iii. On définira des responsabilités et des procédures en matière de gestion des incidents afin de veiller à la mise en œuvre d'une réponse rapide, méthodique et efficace en cas d'incident de sécurité de l'information.

iv. Il conviendra de recenser les types d'incidents de sécurité de l'information, de quantifier les volumes et les coûts associés, de produire des rapports y afférents et de mettre en place, le cas échéant, un processus de suivi.

v. Il conviendra de définir des règles de collecte des éléments de preuve dans le contexte des enquêtes sur les incidents de sécurité.

vi. Les enquêtes sur les incidents de sécurité de l'information devront veiller au recueil, à la conservation et à la présentation des éléments de preuve en conformité avec la norme du Partenariat en matière de réponse aux incidents et à ses règles régissant la collecte des éléments de preuve.

1.4.28 Gestion de la continuité des opérations

i. Une évaluation des risques devra permettre de recenser les événements de sécurité de l'information et des TI susceptibles d'interrompre les processus opérationnels. Cette évaluation des risques pourra être conduite dans le cadre des activités relatives aux normes de certification et d'accréditation du Partenariat.

ii. Des plans devront être élaborés en vue de maintenir ou de rétablir les activités opérationnelles après une interruption ou une panne des services essentiels.

iii. Un plan de continuité des opérations devra prendre en compte les exigences en matière de sécurité de l'information et des TI.

iv. Les plans de continuité des opérations et de reprise après sinistre informatique devront être régulièrement mis à l'essai et mis à jour.

v. Les systèmes d'information et de TI devront faire l'objet de sauvegardes, et le processus de récupération devra être documenté et mis à l'essai régulièrement.

vi. La documentation relative à la conception et à la configuration des systèmes devra être protégée contre tout accès non autorisé.

1.4.29 Certification des systèmes

i. La certification des systèmes sert à vérifier si les exigences de sécurité établies pour un système ou un service particulier sont respectées et si les contrôles et les mesures de protection fonctionnent comme prévu. Elle vise à confirmer que la direction a autorisé le fonctionnement du système ou du service concerné et qu'elle a accepté, en se fondant sur les éléments probants de la certification, le risque résiduel lié au fonctionnement dudit système ou dudit service. Le rendement progressif de la certification dépend de la quantité et de la qualité des éléments probants de certification exigés par l'organisme délivrant la certification. Ces derniers peuvent inclure les résultats de toute évaluation pertinente des menaces et des risques, une évaluation des répercussions sur les activités, une évaluation des répercussions sur la protection des renseignements personnels, une évaluation de la vulnérabilité, une évaluation des essais et des produits de sécurité, des autoévaluations, des vérifications et des examens de sécurité ainsi que des évaluations juridiques ou stratégiques connexes apportant la preuve de la conformité aux lois et politiques pertinentes. En conséquence :

a) Le Partenariat devra maintenir une norme de certification des systèmes et certifier, dans ce cadre, tous les systèmes et services informatiques sensibles avant leur mise en service ou dans un délai raisonnable après leur mise en œuvre.

b) Le Partenariat devra, en cas de modifications importantes des systèmes ou des services ou lorsque cela s'avèrera nécessaire à la suite de changements survenus dans l'environnement de risque, en examiner périodiquement la certification.

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 à ses technologies de l'information.

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 confidentiels	Renseignements de nature délicate présents au sein du Partenariat et destinés à être utilisés exclusivement 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
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	Cadre comprenant des politiques, des normes, des processus, des procédures, des gabarits et des outils conçus pour être utilisés, individuellement et collectivement, à des fins de sécurité et de protection des ressources informationnelles et TI du Partenariat

Terme	Définition
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, des membres de son personnel, de ses consultants, de ses fournisseurs ou de sa clientèle organisationnelle
Utilisateur	Toute personne qui consulte et utilise les ressources du Partenariat

1.7 Documents connexes

- Politique de classification des renseignements
- Politique d'utilisation acceptable
- Politique de protection des renseignements personnels
- Politique sur les appareils mobiles
- Politique « Apportez votre équipement personnel de communication » (AVEC)
- Politique de gestion de l'information
- Politique et procédures de gestion des dossiers
- Norme relative à la destruction des supports informatiques
- Norme relative au chiffrement acceptable
- Norme relative à la gestion des vérifications et de la vulnérabilité
- Norme relative à l'accès à distance
- Norme relative aux mots de passe
- Norme relative au courrier électronique
- Norme relative à la gestion des correctifs
- Norme de certification des systèmes
- Norme relative à la sécurité de l'infrastructure TI
- Procédure relative aux incidents de sécurité de l'information
- Politique relative aux médias sociaux
- Politique de gestion des risques d'entreprise

Fin du document