Politique d'utilisation acceptable

1.1 Aperçu

Le Cadre de sécurité et de protection des renseignements personnels du Partenariat intègre une politique d'utilisation acceptable. Le Partenariat a adopté une philosophie d'autoréglementation et permet aux utilisateurs d'accéder à ses ressources informationnelles et à ses technologies de l'information (TI), sous réserve qu'ils assument la responsabilité personnelle de leurs actions lors de la consultation et de l'utilisation desdites ressources. Il appartient aux utilisateurs de déterminer si leurs actions constituent une violation de la présente politique, le Partenariat ne fournissant aucun avertissement lorsqu'une telle violation survient.

Cette politique fournit aux organisations utilisatrices des orientations de gestion précisant ce que sont les utilisations acceptables (ou inacceptables) des ressources TI du Partenariat, sans toutefois préciser les modalités de sa mise en œuvre. D'autres composantes du Cadre de sécurité et de protection des renseignements personnels du Partenariat détaillent les modalités de mise en œuvre de la présente politique. Le Partenariat pourrait, à sa seule discrétion, imposer des directives supplémentaires en la matière.

1.2 But

Ce document a pour but de définir les utilisations acceptables et inacceptables des ressources TI du Partenariat, lui permettant ainsi, en tant qu'organisation, de répondre de sa responsabilité dans ses actions. 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, des sous-traitants et des partenaires qui utilisent les ressources TI du Partenariat.

1.4 Énoncé de politique

1.4.1 Responsabilisation

i. Il incombera à chaque directeur et à chaque vice-président de prendre des mesures en cas de consultation ou d'utilisation inappropriées des ressources du Partenariat par un utilisateur travaillant pour le secteur d'activité dont il est responsable.

ii. Il incombera aux utilisateurs des ressources TI du Partenariat de protéger toutes les ressources physiques et logiques qui leur ont été confiées.

1.4.2 Utilisations acceptables

i. Les utilisateurs sont autorisés à utiliser les ressources TI du Partenariat dans le cadre d'activités opérationnelles spécifiquement liées à leurs tâches à l'appui des stratégies et des objectifs du Partenariat.

ii. Une utilisation limitée des ressources TI du Partenariat à des fins personnelles est acceptable, tant qu'elle ne viole pas le Cadre de sécurité et de protection des renseignements personnels et qu'elle n'interfère pas avec la réalisation des tâches de l'utilisateur. Il incombera aux utilisateurs d'exercer un jugement sûr afin de déterminer si une utilisation des ressources TI du Partenariat à des fins personnelles est raisonnable ou non.

1.4.3 Utilisations inacceptables

i. Il est inacceptable d'utiliser les ressources TI du Partenariat à des fins illégales, notamment, sans que cela soit limitatif :

- En contrevenant à la protection légale offerte par le droit d'auteur et les licences visant les programmes, les technologies et les renseignements informatiques.
- En contrevenant aux dispositions du Code criminel du Canada en matière de sécurité et de protection des renseignements personnels.
- En contrevenant aux dispositions d'autres textes réglementaires auxquels le Partenariat est soumis ou pourrait être soumis en matière de sécurité et de protection des renseignements personnels.
- En contrevenant à la protection légale fournie par le droit relatif au harcèlement sexuel et au climat hostile sur le lieu de travail.

ii. Il est inacceptable d'utiliser les ressources TI du Partenariat pour tenter de contrevenir au Cadre de sécurité et de protection des renseignements personnels du Partenariat ou de le remettre en cause, notamment, sans que cela soit limitatif :

- En contournant ou en sabotant volontairement les contrôles de sécurité physiques, électroniques ou procéduraux du Partenariat.
- En tentant de modifier ou de détruire des ressources TI du Partenariat (par exemple des ressources informationnelles, électroniques ou réseau).
- En propageant délibérément du code malveillant (par exemple des virus, des vers, des chevaux de Troie ou d'autres logiciels malveillants).
- En accédant volontairement à des renseignements qui ne sont pas requis pour la réalisation des tâches d'un utilisateur.
- En permettant à des personnes non autorisées de consulter ou d'utiliser les ressources TI du Partenariat.
- En utilisant à des fins personnelles des réseaux poste-à-poste non approuvés.
- En installant des logiciels piratés ou d'autres produits logiciels pour lesquels le Partenariat ne dispose pas de licences.
- En plagiant les travaux d'un autre utilisateur du Partenariat susceptibles de constituer une propriété intellectuelle.
- En s'engageant dans des activités pouvant être considérées comme perturbatrices pour les communications réseau, telles que le reniflage de réseau, l'inondation du serveur par requêtes « ping », l'usurpation de paquets, le déni de service et l'acheminement falsifié de données.
- En consultant, en utilisant ou en divulguant, sans le consentement explicite d'une personne, ses renseignements personnels, sauf si la loi l'exige.
- En consultant, en utilisant ou en divulguant, sans l'autorisation du Partenariat, des renseignements confidentiels ou à diffusion restreinte.
- En contournant les processus de sécurité ou d'authentification des utilisateurs relatifs aux ressources TI du Partenariat.

iii. Il est inacceptable d'utiliser les ressources TI du Partenariat d'une manière quelconque contrevenant à la politique du Partenariat en matière de respect en milieu de travail. Les utilisateurs devront notamment s'abstenir de produire ou de transmettre des contenus commerciaux ou publicitaires non sollicités, par exemple sous la forme de pourriels, de courriels en chaîne ou de tout autre contenu inapproprié ou ayant pour effet de harceler.

De plus, les utilisateurs devront s'abstenir de générer ou de transmettre des menaces de violence.

iv. Il est inacceptable d'utiliser les ressources TI du Partenariat afin de réaliser des gains personnels, par exemple par le biais d'activités commerciales.

v. Il est inacceptable d'envoyer des messages anonymes en contradiction avec les valeurs fondamentales de transparence et de responsabilisation du Partenariat.

vi. Il est inacceptable de consulter ou de visualiser volontairement des contenus inappropriés sur Internet, tels que des sites Web incitant à la haine, proposant des contenus pornographiques ou offrant la possibilité de s'adonner à des jeux et à des paris électroniques. Reconnaissant qu'un accès accidentel à de tels sites est possible, le Partenariat s'est doté des moyens de différencier un tel accès d'une consultation volontaire.

vii. Les réseaux sociaux (blogues, wikis, messagerie instantanée, Skype, Facebook, Twitter, etc.) devront être utilisés de manière professionnelle, transparente et responsable, et leur utilisation à des fins personnelles ne devra pas interférer avec les tâches habituelles d'un utilisateur. Ils devront, en outre, ne pas être utilisés d'une manière préjudiciable aux intérêts fondamentaux du Partenariat.

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.

iv.

1.6 Définitions

Terme	Définition
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 une 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 des TI du Partenariat
Utilisateur	Toute personne qui consulte et utilise les ressources informationnelles et les TI du Partenariat

1.7 Documents connexes

- Politique de protection des renseignements personnels
- Politique de sécurité de l'information et des technologies de l'information
- Politique de gestion de l'information
- Politique de gestion des dossiers
- Politique de respect en milieu de travail
- Politique de classification des renseignements
- Norme relative aux mots de passe

- Norme relative au chiffrement acceptable
- Norme relative au courrier électronique
- Norme relative à la gestion des vérifications et de la vulnérabilité
- Procédure de consultation et de diffusion des renseignements personnels

Fin du document