Politique sur la sécurité de l'information

Unité administrative : Service des technologies, de l'organisation scolaire et du transport

13, rue Saint-Antoine
Sainte-Agathe-des-Monts (Québec) J8C 2C3
Téléphone : 819 326-0333
Télécopieur : 819 326-2121
www.cslaurentides.qc.ca

TABLE DES MATIÈRES

1. CONTEXTE 2
2. DÉFINITIONS 2
3. CADRE LÉGAL ET ADMINISTRATIF 4
4. LES OBJECTIFS DE LA POLITIQUE 5
5. CHAMP D'APPLICATION 5
6. PRINCIPES DIRECTEURS 5
   6.1. PROTECTION DE L'INFORMATION 5
   6.2. PROTECTION DES RENSEIGNEMENTS CONFIDENTIELS 6
   6.3. SENSIBILISATION ET FORMATION 6
   6.4. DROIT DE REGARD 7
7. GESTION DES RISQUES 7
   7.1. CATÉGORISATION DE L'ACTIF INFORMATIONNEL 8
      7.1.1. ACTIF INFORMATIONNEL CONFIDENTIEL 8
   7.2. ÉTAPES DE LA GESTION DES RISQUES 8
      7.2.1. RISQUE DE PORTÉE GOUVERNEMENTALE 9
   7.3. ENTENTE AVEC UNE TIERCE PARTIE 9
   7.4. SÉPARATION DES OBLIGATIONS DE CHACUN DES INTERVENANTS 9
8. GESTION DES INCIDENTS 9
   8.1. INCIDENT DE PORTÉE GOUVERNEMENTALE 10
   8.2. INCIDENT DE SÉCURITÉ – ACTIF INFORMATIONNEL DE NATURE INFORMATIQUE 10
   8.3. INCIDENT DE SÉCURITÉ – ACTIF INFORMATIONNEL AUTRE 11
9. OBLIGATIONS DES INTERVENANTS CLÉS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION 11
10. OBLIGATIONS DES UTILISATEURS 12

APPROUVÉE :
CC-2019-12-11, 829e rés.

DATE D'ENTRÉE EN VIGUEUR :
Le 11 décembre 2019

1. CONTEXTE

Le Centre de services scolaire des Laurentides est un organisme public soumis à l'application de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (chapitre G-1.03).

Ce faisant, le Centre de services scolaire des Laurentides doit notamment, en application de l'alinéa 2 de l'article 7 de la *Directive sur la sécurité de l'information gouvernementale*, adopter, appliquer, mettre en œuvre et maintenir à jour une politique de sécurité de l'information. C'est le conseil d'administration, à titre de dirigeant du Centre de services scolaire des Laurentides, qui doit adopter une telle politique.

La Directive sur la sécurité de l'information gouvernementale oblige également le Centre de services scolaire des Laurentides, pour satisfaire à son obligation de sécurité de l'information, à avoir recours à des processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion des incidents et la gestion de l'accès à l'information. Dans ce contexte, il est prévu que le Centre de services scolaire des Laurentides désigne un Responsable de la sécurité de l'information et un deux (2) Coordonnateurs sectoriels de la gestion des incidents, dont un (1) agissant à titre de substitut.

Par l'adoption de la présente Politique sur la sécurité de l'information, le Centre de services scolaire des Laurentides démontre ainsi son engagement à protéger l'ensemble de l'information auprès de son personnel, ses usagers, sa clientèle, ses partenaires et toute autre personne qui utilise ses services ou avec qui elle fait affaire.

La Politique sur la sécurité de l'information oriente et détermine la vision du Centre de services scolaire des Laurentides en matière de sécurité de l'information. Elle est complétée par le cadre de gestion de la sécurité de l'information du Centre de services scolaire, laquelle présente plus en détails les mécanismes et autres mesures mises en place relativement à la sécurité informationnelle.

2. DÉFINITIONS

a) **Actif informationnel** : Une information, quel que soit son canal de communication ou son support, un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

Sans restreindre la généralité de ce qui précède, sont considérés comme un actif informationnel :

- Les informations appartenant au CSSL et exploitées par le CSSL;
- Les informations appartenant au CSSL et exploitées ou détenues par un tiers : partenaire, fournisseur de produits/services ou tout autre intervenant;
- Les informations appartenant à un tiers : partenaire, fournisseur de produits/services ou tout autre intervenant, et exploitées par lui au profit du CSSL;
- Les informations n'appartenant pas au CSSL, mais qui sont détenues ou exploitées par le CSSL;

- Les ordinateurs de bureau ou portables, les imprimantes, les appareils mobiles (tablettes, téléphones intelligents), les logiciels et applications d'affaires, les CD-ROM, les DVD, les clés USB, les copies de sauvegarde, et tout autre système, support ou technologie de l'information utilisée par les employés du CSSL dans l'exercice de ses fonctions;
- Les centres de traitement informatique, les salles de télécommunications et de serveurs ainsi que les points de raccordement avec les télécommunicateurs et les archives du CSSL.

Est aussi un actif informationnel, tout document dont la définition correspond à celle de l'article 3 de la Loi concernant le cadre juridique des technologies de l'information (chapitre C-1.1). Cette loi définit le document comme étant : « Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrit sous l'une de ses formes ou en un autre système de symboles. »

Cette loi assimile aussi au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite;

b) **Confidentialité** : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées;

c) **CSSL** : Le Centre de services scolaire des Laurentides;

d) **CSGI** : Coordonnateur sectoriel de la gestion des incidents désigné par le CSSL;

e) **Cycle de vie de l'information** : L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'organisme public;

f) **Disponibilité** : Propriété d'une information disponible en temps voulu et de la manière requise pour une personne autorisée;

g) **Intégrité** : Propriété d'une information de ne subir aucune altération ou destruction de façon erronée ou sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité. L'Intégrité fait référence à l'exactitude et à la complétude;

h) **Personne autorisée** : Personne autorisée par le CSSL pouvant avoir accès aux actifs informationnels;

i) **RSI** : Responsable de la sécurité informationnelle désigné par le CSSL;

j) **Utilisateur** : Toute personne du CSSL, de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne qui, par engagement contractuel ou autrement, utilise un actif informationnel du CSSL ou y a accès.

Les personnes suivantes sont notamment des utilisateurs :

- Les personnes autorisées;
- Les cadres et administrateurs des unités composant le CSSL;
- Les employés du CSSL;
- Les représentants liés par contrat ou autrement avec le CSSL;
- Les sous-traitants, fournisseurs de services et consultants liés par contrat ou autrement avec le CSSL ainsi que leurs employés;
- Les bénévoles œuvrant au sein du CSSL.

3. CADRE LÉGAL ET ADMINISTRATIF

La politique de sécurité s'inscrit principalement dans un contexte régi par :

- La *Loi canadienne sur les droits de la personne* (chapitre H-6);
- La *Charte des droits et libertés de la personne* (chapitre C-12);
- Le *Code civil du Québec* (chapitre 64);
- Le *Code criminel* (chapitre C-46);
- La *Loi sur l'instruction publique* (chapitre I-13.3);
- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (chapitre G-1.03);
- La *Loi sur le droit d'auteur* (chapitre C-42);
- La *Loi sur l'administration publique* (chapitre A-6.01);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1);
- La *Loi sur les archives* (chapitre A-21.1);
- La *Loi concernant le cadre juridique des technologies de l'information* (chapitre C-1.1);
- Le *Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques* (chapitre A-21.1, r.1);
- Le *Règlement sur la diffusion et sur la protection des renseignements personnels* (chapitre A-2.1, r.02);
- Le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels* (chapitre A-2.1, R.2);
- La *Directive sur les services de certification offerts par le gouvernement du Québec pendant la phase intérimaire*;

- La *Directive sur la sécurité de l'information gouvernementale*;
- La *Politique relative à l'utilisation des services informatiques* du CSSL;
- La *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics*.

4. LES OBJECTIFS DE LA POLITIQUE

La présente politique a pour objectif d'affirmer l'engagement du CSSL à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou son moyen de communication.

Le CSSL s'engage ainsi à soutenir la prise en charge des exigences de sécurité de l'information et à mettre de l'avant les moyens nécessaires à leur réalisation.

Sans restreindre la généralité de ce qui précède, le CSSL s'engage plus précisément à s'assurer, tout au long du cycle de vie de l'information, de la disponibilité, l'intégrité et la confidentialité de l'information. Le CSSL veillera aussi à assurer l'authentification de l'information.

5. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs, c'est-à-dire à toute personne autorisée, administrateur, membre du conseil d'administration et membre du personnel du CSSL, peu importe son statut, ainsi qu'à toute personne physique ou morale qui, à titre d'employé, élève ou d'étudiant, parent d'un élève ou étudiant, consultant, partenaire, sous-traitant, fournisseur, ou bénévole a accès, utilise ou manipule les actifs informationnels du CSSL ainsi qu'à toute autre personne dûment autorisée à y avoir accès.

L'information visée est celle que le CSSL détient dans l'exercice de ses fonctions et activités, que sa conservation soit assurée par elle-même ou par un tiers et peu importe son canal de communication (téléphone analogique ou numérique, télégraphie, télécopie, voix, etc.), son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.) ou sa valeur.

6. PRINCIPES DIRECTEURS

6.1. PROTECTION DE L'INFORMATION

Le CSSL adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information.

Le CSSL s'engage ainsi à ce que ses actions en matière de sécurité de l'information soient guidées par les principes directeurs suivants :

a) S'engager à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées, tant à l'échelle nationale qu'internationale;

b) Reconnaître l'importance de la politique de sécurité de l'information;

c) Reconnaître que les actifs informationnels qu'il détient sont essentiels à ses activités courantes et, de ce fait, qu'ils doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate. Le niveau de protection dont les actifs informationnels doivent faire l'objet est établi en fonction de leur importance, de leur confidentialité et des risques d'accident, d'erreur et de malveillance auxquels ils sont exposés;

d) Exiger un comportement éthique de la part de tous les utilisateurs. La sécurité des actifs informationnelles est en effet soutenue par une démarche d'éthique visant à assurer la régulation des conduites et la responsabilisation individuelle;

e) Adhérer, appliquer et assurer le respect des lois, politiques, cadres de gestion, directives, règlements et autres auxquels est assujettie le CSSL en matière de sécurité de l'information;

f) En regard du niveau de protection des actifs informationnelles, s'assurer que chaque employé ait accès au minimum d'information nécessaire à l'exercice de ses fonctions;

g) S'assurer de bien connaitre l'information à protéger, d'en identifier les détenteurs ou les utilisateurs ainsi que d'identifier les caractéristiques de sécurité de cette information;

h) Reconnaître que l'environnement technologique des actifs informationnels, peu importe leur support, est en changement constant et interconnecté avec le monde.

6.2. PROTECTION DES RENSEIGNEMENTS CONFIDENTIELS

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée.

Sont notamment considérés confidentiels, au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (chapitre A-2.1), les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences, notamment sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, les tiers relativement à leurs renseignements industriels, financiers, commerciaux, scientifiques ou techniques, l'administration de la justice et de la sécurité publique, les décisions administratives ou politiques et la vérification.

6.3. SENSIBILISATION ET FORMATION

Le CSSL s'engage, sur une base régulière, à former les utilisateurs à la sécurité des actifs informationnels, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, le CSSL s'assure que tous les utilisateurs adoptent un comportement éthique et respectueux des lois, politiques, règlements, directives et autres règles de conduite encadrant l'utilisation des actifs informationnels et que les rôles et obligations de chacun des intervenants soit connu et compris.

Ainsi, les membres du personnel du Centre de services scolaire et, le cas échéant, tout utilisateur doivent être formés et sensibilisés :

- À la sécurité de l'information et des systèmes d'information du CSSL;
- Aux directives et guides du CSSL en matière de sécurité de l'information;
- Au cadre de gestion en matière de sécurité de l'information du CSSL;
- À la gestion des risques;
- À la gestion des incidents;
- Aux menaces existantes;
- Aux conséquences d'une atteinte à la sécurité;
- À leurs responsabilités en la matière;
- Au cycle de vie des actifs informationnels.

À ces fins, et pour instaurer une culture de sécurité, des activités de sensibilisation, de prévention et de formation continue sont offertes périodiquement par le CSSL afin que tous les utilisateurs comprennent et collaborent à la prévention de tout incident en matière de sécurité de l'information. De plus, des documents explicatifs sont disponibles sur le site Internet du CSSL.

6.4. DROIT DE REGARD

Le CSSL exerce, en conformité avec la législation et la règlementation en vigueur, un droit de regard et d'intervention sur tout usage de ses actifs informationnels ou sur toute activité susceptible de les affecter, dans le respect du cadre légal et administratif applicable au respect de la vie privée et à la protection des renseignements confidentiels.

Le CSSL se réserve de tels droits afin d'assurer la sécurité de ses actifs informationnels.

7. GESTION DES RISQUES

Un processus de gestion des risques doit exister au sein du CSSL afin de soutenir l'ensemble des utilisateurs et autres personnes de même que pour soutenir les actions à prendre dans la gestion de l'incident.

7.1. CATÉGORISATION DE L'ACTIF INFORMATIONNEL

Afin de permettre la gestion des risques et l'application des mesures de sécurité appropriées, une catégorisation de l'ensemble des actifs informationnels est préalablement réalisée. Une telle catégorisation permet notamment au RSI de déterminer les premiers actifs devant faire l'objet d'une gestion des risques. Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger. Le CSSL est ainsi en mesure de justifier les mesures de sécurité devant être appliquées afin de fournir le niveau de sécurité adéquat.

Les actifs informationnels du CSSL sont inventoriés, catégorisés et appartiennent au CSSL.

7.1.1. ACTIF INFORMATIONNEL CONFIDENTIEL

Le degré de sensibilité de l'actif informationnel influence les mesures de sécurité de l'information que le CSSL doit mettre en place. Généralement, plus un actif détient un niveau de catégorisation élevé, plus l'actif doit être sécurisé à l'aide de contrôles et de mesures. Les actifs informationnels de nature confidentielle ou ayant une valeur gouvernementale élevée font l'objet d'une attention particulière par le CSSL.

7.2. ÉTAPES DE LA GESTION DES RISQUES

La gestion des risques s'effectue selon les étapes suivantes :

a) L'établissement du contexte, ce qui comprend l'organisation à mettre en place, le champ d'application et la portée du processus ainsi que les facteurs d'évaluation des risques doivent être précisés pour tout type d'actif informationnel;

b) L'analyse des risques, laquelle comprend :

- L'identification des risques: elle permet de produire une liste de risques potentiels à évaluer pour chaque actif informationnel étudié, tout en se demandant comment, où et quand ces risques peuvent survenir. Elle comprend l'identification des actifs informationnelles, des menaces, des mesures de sécurité existantes, des vulnérabilités et des impacts;
- L'évaluation des risques : elle consiste à attribuer une valeur à chaque scénario de risque, laquelle peut être quantitative ou qualitative (exemples : pertes financières, dommages matériels, atteintes à la réputation, pertes de productivité et autres);
- Le classement des risques.

c) Le traitement des risques;

d) La mise en place des mesures de sécurité. Les mesures de sécurité à appliquer par le CSSL doivent évoluer et être déterminées selon une évaluation régulière des risques liés à la sécurité de l'information. Le niveau de sécurité ou de protection est établit, notamment, en fonction :

- De la nature de l'information et de son importance;
- Des probabilités d'accident, d'erreur ou de malveillance auxquelles elle est exposée;
- Des conséquences de la matérialisation de ces risques;
- Du niveau de risque acceptable par le CSSL.

e) La communication des risques : elle consiste à échanger l'information sur les risques, notamment à propos de leur existence, leur probabilité d'apparition, leur gravité, etc.;

f) La revue des risques : elle est nécessaire sur une base régulière, notamment afin d'inclure les nouveaux risques, s'il y a lieu;

g) L'amélioration de la gestion des risques.

7.2.1. RISQUE DE PORTÉE GOUVERNEMENTALE

Conformément au paragraphe d), alinéa 1 de l'article 7 de la *Directive sur la sécurité de l'information gouvernementale*, tout risque de sécurité de l'information à portée gouvernementale est déclarée au Dirigeant principal de l'information du Ministère de l'Éducation et de l'Enseignement supérieur, conformément à la procédure décrite dans le Guide de mise en œuvre du cadre de gestion des risques à portée gouvernementale.

7.3. ENTENTE AVEC UNE TIERCE PARTIE

Toute entente ou contrat entre le CSSL et un fournisseur, partenaire, sous-traitant ou toute autre personne doit être écrit et inclure les obligations applicables en matière de sécurité de l'information, dont les mesures de protection appliquées par chacune des parties. Lorsque l'entente ou le contrat vise les actifs informationnels, il doit être conforme à la présente politique.

7.4. SÉPARATION DES OBLIGATIONS DE CHACUN DES INTERVENANTS

Certaines tâches ou obligations, de par leur nature, doivent être exécutées par différentes personnes, afin d'atteindre correctement l'ensemble des objectifs de sécurité du CSSL. Une telle séparation doit être un élément clé lors de l'élaboration ou de la révision de processus en lien, directement ou indirectement, avec la gestion de la sécurité de l'information.

8. GESTION DES INCIDENTS

Un processus de gestion des incidents de sécurité doit exister au sein du CSSL afin de soutenir l'ensemble des utilisateurs et autres personnes, de même que pour soutenir les actions à prendre dans la gestion de l'incident.

À cet égard, le CSSL met en place les mesures nécessaires à l'obtention des buts suivants, en respect du processus de gestion des incidents existant:

- Prévenir les incidents (prévention);
- Limiter l'occurrence et les effets des incidents en matière de sécurité de l'information sur le CSSL (surveillance et détection);
- Réagir aux incidents et les gérer adéquatement pour en minimiser les conséquences sur les activités et les opérations du CSSL, ce qui comprend notamment l'analyse et l'évaluation des conséquences, le confinement des dommages et l'éradication (réaction). Le CSSL déploie d'ailleurs des mesures de sécurité de l'information de manière à assurer la continuité de ses services;
- Transmettre l'information au palier hiérarchique supérieur;
- Rétablir la situation.

Le CSSL doit, lors de l'application du processus de gestion des incidents, assurer un suivi afin de constituer toute documentation se rapportant aux événements relatifs à l'incident ainsi que la mise à jour des directives et des procédures.

Dans la gestion des incidents, le CSSL peut exercer ses pouvoirs et ses prérogatives en égard de toute utilisation inappropriée de l'information ou de tout actif informationnel dont il est responsable.

8.1. INCIDENT DE PORTÉE GOUVERNEMENTALE

Conformément au paragraphe d), alinéa 1 de l'article 7 de la *Directive sur la sécurité de l'information gouvernementale*, tout incident de sécurité de l'information à portée gouvernementale est déclarée au Dirigeant principal de l'information du Ministère de l'Éducation et de l'Enseignement supérieur, conformément à la procédure décrite dans le Guide de mise en œuvre du cadre de gestion des risques à portée gouvernementale.

8.2. INCIDENT DE SÉCURITÉ – ACTIF INFORMATIONNEL DE NATURE INFORMATIQUE

Tout utilisateur doit, sans délai, alerter le Service des technologies de l'information et de la communication (le « STIC »), lors de l'observation, connaissance ou détection de tout événement, action, geste ou incident représentant ou pouvant représenter une atteinte à l'une des dispositions de la présente politique ou à toute autre règle de sécurité de l'information du CSSL, et ce, que cette atteinte soit concrète et authentique, ou simplement hypothétique.

8.3. INCIDENT DE SÉCURITÉ – ACTIF INFORMATIONNEL AUTRE

Tout utilisateur et toute autre personne doit, sans délai, alerter le RSI, lors de l'observation, connaissance ou détection de tout événement, action, geste ou incident représentant ou pouvant représenter une atteinte à l'une des dispositions de la présente politique ou à toute autre règle de sécurité de l'information du CSSL, et ce, que cette atteinte soit concrète et authentique, ou simplement hypothétique.

9. OBLIGATIONS DES INTERVENANTS CLÉS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION

La présente politique fixe les obligations en matière de sécurité de l'information attribuées, notamment, au conseil d'administration, au détenteur de l'information, à la direction générale, à la direction du service des technologies de l'information, au secrétariat général, au RSI, au détenteur de l'information et aux utilisateurs :

a) Le conseil d'administration : Il est le dirigeant du CSSL au sens de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (chapitre G-1.03). Ce faisant, il :

- Adopte la présente politique;
- Désigne directement, ou par délégation de pouvoir à la direction générale du CSSL, le RSI, le CSGI et son substitut.

b) Le détenteur de l'information : il s'agit des directions des unités administratives. À ce titre, elles sont chargées de la mise en œuvre des dispositions de la présente politique auprès du personnel relevant de leur autorité;

c) La direction générale du CSSL : Elle agit à titre de premier répondant de la sécurité au CSSL et, à ce titre, elle veille au respect du cadre gouvernemental de sécurité de l'information et s'acquitte de ses obligations, telles qu'elles sont édictées dans la Directive sur la sécurité de l'information gouvernementale;

d) La direction du service des technologies de l'information : Elle assiste le conseil d'administration et la direction générale dans la détermination des orientations stratégiques et des priorités d'intervention en matière de sécurité informatique des données informationnelles;

e) Le secrétariat général : Il est responsable de l'accès aux documents et de la protection des renseignements personnels;

f) Le RSI : Il a notamment pour rôle d'assister la direction générale et de la conseiller dans la détermination des orientations stratégiques et priorités d'intervention du CSSL en matière de sécurité de l'information;

g) Les utilisateurs : Ils sont visés par la présente politique et doivent ainsi s'y conformer, ainsi qu'aux directives, guides ou règles qui leur sont applicables, en signant la déclaration d'engagement jointe en annexe.

Les rôles et responsabilités attribués à d'autres intervenants ainsi que les structures internes de coordination et de concertation en matière de sécurité de l'information sont définis dans le cadre de la gestion de la sécurité de l'information, en complément à la présente politique.

10. OBLIGATIONS DES UTILISATEURS

Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le CSSL. À cette fin, il doit :

a) Prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer, en signant la déclaration jointe en annexe;

b) Utiliser, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés;

c) Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ou les désactiver;

d) Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;

e) Signaler immédiatement à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du CSSL;

f) Au moment de son départ du CSSL, remettre les différentes cartes d'identité ou d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphone mis à sa disposition dans le cadre de l'exercice de ses fonctions.