POLITIQUE DE SÉCURITÉ

Tables des matières

1. Objet, champ d'application et utilisateurs

Objectifs du document. Le présent document (ci-après la « **Politique** ») a pour objet de définir des règles claires pour l'utilisation de la documentation papier, du système d'information et d'autres actifs informationnels (ci-après les « **Actifs informationnels** ») dans l'École secondaire de Bromptonville (l'« **Établissement** »). Ce document expose les responsabilités du Chef de la sécurité de l'information organisationnelle en matière de sécurité informationnelle. La Politique expose également les règles applicables aux employés et représentants de l'Établissement dans leur gestion et dans leur usage de tout Actif informationnel appartenant à l'Établissement et de tout Actif informationnel sur lesquels des informations confidentielles de l'Établissement sont conservées.

Prohibition d'usage de la documentation. Seuls des employés, représentants et sous-traitants autorisés de l'Établissement peuvent accéder à ce document.

2. Documents de référence

- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, c. A-2.1 telle qu'amendée par la L*oi modernisant des dispositions législatives en matière de protection des renseignements personnels*, SQ 2021, c 25 (la « **Loi 25** ») (soit la « **Loi sur le secteur public** »);
- *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement,* G-1.03 (la « **Loi sur la gouvernance** »);
- *Règlement sur les modalités et conditions d'application des articles 12.2 à 12.4 de la Loi sur la gouvernance et la gestion des ressources informationnelles des Établissements publics et des entreprises du gouvernement*, G-1.03, r. 1 ;
- Directive gouvernementale sur la sécurité de l'information ;
- Directive gouvernementale sur la sécurité de l'information ;
- Cadre gouvernemental de gestion de la sécurité de l'information ;
- Guide de catégorisation de l'information, Pratique recommandée en sécurité de l'information, PR-057 du Gouvernement du Québec ;
- Norme ISO/IEC 27001 (si applicable) ;
- Cadre normatif existant au sein de l'Établissement en matière de sécurité et technologies de l'information ;
- Politique de gestion et de notification en cas d'incidents de confidentialité.

3. Définitions

Actifs informationnels : dans le contexte de la présente politique *Actifs informationnels* englobe tous systèmes d'information et autres informations et équipements, y compris les documents papier, les téléphones mobiles, les ordinateurs portables, les supports de stockage de données, les bases de données, etc.

Antivirus : le système d'Antivirus utilisé par l'Établissement soit : *Windows Sécurité* & *Malwarebytes*

Évènements de sécurité : dans le contexte de la présente Politique, le terme « Évènement de sécurité » réfère à sa définition prévue à l'art 2 (7) de la *Directive gouvernementale sur la sécurité de l'information* soit « toute forme d'atteinte, présente ou appréhendée, telle une cyberattaque ou une menace à la confidentialité, à l'intégrité et à la disponibilité d'une information ou d'une ressource informationnelle sous la responsabilité d'un Établissement public ou d'une personne agissant pour ce dernier ».

Incident de confidentialité : désigne tout accès non autorisé par la loi à un Renseignement personnel, à son utilisation ou à sa communication, de même que sa perte ou toute autre forme d'atteinte à sa protection ou à son caractère confidentiel.

Responsable de la protection des renseignements personnels : désigne la personne qui veille à assurer le respect et la mise en œuvre des Lois sur la protection de la vie privée au sein de la Société.

Chef de la sécurité de l'information organisationnelle : membre du personnel désigné par le dirigeant de l'Établissement en charge de l'implémentation et du respect de la présente Politique soit le Responsable Informatique conjointement avec le Directeur général de l'école.

Système d'échange : dans le contexte de la présente Politique, le terme « Système d'échange » comprend toute méthode permettant de communiquer des informations ou de la documentation sous format papier ou numérique. Le terme regroupe le courrier électronique, le téléchargement de fichiers, le transfert et partage de données via des plateformes numériques, les téléphones, les télécopieurs, les messages texte SMS, les téléphones intelligents, les forums et les réseaux sociaux.

Système d'information : comprend tous les serveurs et systèmes clients, l'infrastructure réseau, les logiciels système et applicatifs, les données et autres sous-systèmes et composants informatiques qui appartiennent ou sont utilisés par l'Établissement ou qui sont sous la responsabilité de l'Établissement. L'utilisation d'un système d'information comprend également l'utilisation de tous les services internes ou externes, tels que l'accès à Internet, le courrier électronique, etc.

Unité administrative spécialisée en sécurité de l'information : aussi appelé Centre opérationnel de cyberdéfense. Cette unité est composée d'une équipe en cyberdéfense chargée de mettre à l'épreuve les mesures de cybersécurité applicables, y compris les mécanismes de cyberdéfense, et de voir au traitement des événements de sécurité liés à la cybersécurité.

Utilisateur : toute personne utilisant ou pouvant utiliser un Actif informationnel que cette dernière soit un employé, un représentant ou un sous-traitant de l'Établissement.

4. Responsabilités du Chef de la sécurité de l'information organisationnelle

Implémentation de mesures de sécurité. Le Chef de la sécurité de l'information organisationnelle doit s'assurer de l'implémentation et du respect des mesures de sécurité suivantes :

1. Implémenter des mesures techniques, physiques et organisationnelles permettant un contrôle des accès (tel qu'un système de séparation des tâches, une identification de zones sécurisées fermées sous clefs inaccessibles par la majorité des employés et du public;

2. S’assurer de la suppression des accès aux Actifs informatifs d’un employé, représentant ou sous-traitant de l’Établissement immédiatement après la résiliation ou la résolution de son contrat de travail ou de services ;

3. S’assurer que les contrats d’emploi et les contrats de service imposés aux employés, représentants et sous-traitants de l’Établissement prévoient des responsabilités en matière de sécurité de l’information et des Actifs informationnels conforment à la présente Politique qui demeurent valides postérieurement à la résiliation de leurs contrats ;

4. Assurer la protection des clés cryptographiques, le cas échéant, en localisant ces dernières dans des Actifs informatifs sécurisés qui ne peuvent être accédés que par les personnes devant y accéder afin d’accomplir leurs fonctions au sein de l’Établissement ;

5. Assurer la mise en œuvre de mesures de journalisation des accès aux Actifs informatifs et éliminer toute capacité des Utilisateurs de modifier les journaux d’accès ;

6. Vérifier périodiquement les droits d’accès privilégiés ;

7. Rédiger et mettre à jour l’Inventaire des actifs et les Registres identifiés à la section de la présente Politique ;

8. Prévoir et assister à la mise en œuvre des processus disciplinaires à l’égard des employés et de représentants causant des Évènements de sécurité ;

9. Autoriser les installations de logiciels ou d’extensions à tout Actif informationnel de nature numérique ;

10. Assurer la mise en œuvre de mesure de sécurité technique limitant l’accès à l’Internet par les Actifs informationnels de l’Établissement. Il ne devrait être possible de se connecter à l’Internet à travers les Actifs informationnels de l’Établissement que via le réseau local avec une infrastructure et une protection par pare-feu appropriées. Cette mesure ne s’applique pas lors de connexion à distance hors-site. ;

11. Enquêter tout Évènement de sécurité. Répondre à tout Évènement de sécurité en conformité avec le Plan de réponse aux évènements de confidentialité ;

12. Prendre toutes les mesures visant à en corriger les impacts ou à réduire le risque pouvant survenir d’un Évènement de sécurité et inscrire ce dernier dans le Registre des évènements de sécurité ;

13. Élaborer et mettre en œuvre, pour les membres du personnel de l’Établissement, un programme formel et continu de formation et de sensibilisation en matière de sécurité de l’information ;

14. S’assurer de l’installation de l’Antivirus ;

15. S’assurer que les mises à jour automatiques de l’Antivirus doivent être, et rester, en tout temps, activées ;

16. Mettre en place un système d'authentification multiple pour les Utilisateurs des Actifs informationnels de nature numériques, quand la situation le permet et sans nuire aux opérations normales de l'institution ;

17. S'assurer que les informations entreposées dans des Actifs informationnels numériques soient sauvegardées quotidiennement ; et

Registre des canaux de communication autorisés. Lorsqu'il rédige ou modifie le Registre des canaux de communication autorisés, le Chef de la sécurité de l'information organisationnelle y inscrit les restrictions possibles à l'égard des utilisateurs pour qui des restrictions s'appliquent quant à l'utilisation de ces canaux de communication ainsi que des types d'activités qui sont interdites.

5. Règles de sécurité de base

5.1. Utilisation acceptable

Usage limité aux tâches liées à l'Établissement. Les ressources informationnelles ne peuvent être utilisées que pour les besoins de l'Établissement dans le but d'exécuter des tâches liées à l'Établissement.

5.2. Responsabilité des Actifs informationnels

Inventaire des actifs. Chaque Actif informationnel physiquement présent dans les locaux respectifs a un propriétaire désigné dans l'Inventaire des actifs. Le propriétaire de l'actif est responsable de la confidentialité, de l'intégrité et de la disponibilité des renseignements contenus dans l'actif en question.

5.3. Activités interdites

Activités prohibées pour les actifs. Il est interdit d'utiliser les Actifs informationnels d'une manière qui absorberait inutilement la capacité ou affaiblit les performances du système d'information ou d'une manière qui constituerait une menace pour sa sécurité. Il est également interdit :

1. De télécharger sur les Actifs informationnels des fichiers image ou vidéo pour réaliser des activités, des tâches ou des fonctions qui ne sont pas liées à la prestation de votre travail, envoyer des chaînes de lettres électroniques, télécharger et installer des jeux, etc. ;

2. D'installer un logiciel sur un ordinateur local sans autorisation explicite du Chef de la sécurité de l'information organisationnelle ;

3. D'utiliser des applications Java, des contrôles Active X et d'autres codes mobiles, sauf lorsque cela est autorisé par le Chef de la sécurité de l'information organisationnelle ;

4. D'utiliser des outils cryptographiques sur un Actif Informationnel, à moins d'y être autorisé par le Chef de la sécurité de l'information organisationnelle ou une politique de l'Établissement ;

5. De télécharger le code d'un programme à partir d'un support externe ;

6. D'installer sur les Actifs informationnels ou d'y connecter des modems, des cartes mémoire ou d'autres dispositifs de stockage et de lecture de données (par exemple, des clés USB) sans l'autorisation explicite du Chef de la sécurité de l'information organisationnelle ; et

7. De déplacer les Actifs informationnels contenant des informations sensibles de zones sécurisées qui leur ont été assignées, le cas échéant ;

5.4. Retrait des Actifs informationnels hors site

Prohibition générale de transporter les Actifs informationnels hors site. Un Actif informationnel, quel soit sa forme et autre qu'un ordinateur portable, ne peut être emporté hors site sans que cela ne soit explicitement permis par une politique de l'Établissement ou par une autorisation écrite préalable du Chef de la sécurité de l'information organisationnelle. Dans le cas d'un ordinateur portable prêté par l'Établissement, le paragraphe suivant doit être appliqué dans son intégralité.

Obligations applicables à un Actif informationnel situé hors site. Un Utilisateur en possession ou en contrôle d'un Actif informationnel situé hors site se doit de respecter toutes obligations imposées par la présente Politique dans la mesure où celles-ci sont applicables. Un Utilisateur doit également s'assurer de maintenir sa possession et son contrôle de l'Actif informationnel en tout temps.

5.5. Restitution des Actifs informationnels à la résiliation du contrat

Obligation de restituer les Actifs informatifs à la fin de la relation contractuelle. L'Utilisateur doit retourner sans délai tout Actif informationnel de l'Établissement sous sa possession ou son contrôle au Chef de la sécurité de l'information organisationnelle ou à toute personne désignée par ce dernier, suite à la résiliation ou la résolution de son contrat de travail ou de tout autre contrat sur la base duquel des Actifs informationnels de l'Établissement sont utilisés ou accédés.

Obligation de ne pas accéder, utiliser, détruire ou endommager des Actifs informationnels. L'Utilisateur ne doit pas accéder, utiliser, détruire ou endommager des Actifs informationnels de l'Établissement suivant la résiliation ou la résolution de son contrat.

5.6. Protection antivirus

Protection par antivirus. L'Antivirus doit être installé sur chaque ordinateur.

Mises à jour automatiques. Les mises à jour automatiques de l'Antivirus doivent être et rester, en tout temps, activées.

5.7. Autorisations d'utilisation du système d'information

Limitation des accès. Une personne ne peut accéder qu'aux Actifs informationnels que si cet accès est nécessaire à l'exercice de ses fonctions au sein de l'Établissement et que si cet accès a été explicitement autorisé par le propriétaire de ces actifs.

Limitation de l'usage. Toute personne accédant à un Actif informationnel ne peut utiliser le Système d'information qu'à des fins pour lesquelles elle a été autorisée et pour lesquelles ses accès ont été accordés.

Respecter les contrôles de sécurité. Les Utilisateurs ne doivent pas initier ou participer à des activités susceptibles d'être utilisées pour contourner les contrôles de sécurité des Systèmes d'information ou des Actifs informationnels.

Obligation de notification en cas de contournement des contrôles de sécurité. Tout Utilisateur qui découvre un moyen de contourner les contrôles de sécurité des systèmes d'information doit le notifier sans délai au Chef de la sécurité de l'information organisationnelle.

Ne pas partager ses droits d'accès. Tout utilisateur d'un Actif informationnel ne doit pas, directement ou indirectement, permettre à une autre personne d'utiliser ses propres droits d'accès, tel que son nom d'utilisateur ou son mot de passe.

Ne pas accaparer des droits d'accès. Tout Utilisateur d'un Actif informationnel ne doit pas tenter d'accéder à des Actifs informationnels auquel il n'est pas autorisé à accéder. Par exemple, un utilisateur ne peut pas utiliser le nom d'utilisateur ou le mot de passe d'une autre personne.

Responsabilité. Le propriétaire du compte utilisateur est responsable, en tout temps pendant la durée de son contrat, de l'utilisation qui est faite de son compte et de toutes les transactions effectuées via ce compte utilisateur.

5.8. Contrôler l'accès aux Actifs informationnels sous son contrôle ou sa possession

Assurer l'inaccessibilité aux personnes non autorisées lorsque l'on quitte son lieu de travail. Tout Utilisateur doit s'assurer que les Actifs informationnels qu'il contrôle ou possède restent en tout temps inaccessibles pour toute personne qui ne serait pas autorisée à y accéder. Notamment, l'Utilisateur doit, lorsqu'il quitte son lieu de travail :

- Retirer de son bureau (ou de tout autre endroit pouvant les contenir tel qu'une imprimante, un télécopieur ou un photocopieur) tout Actif informationnel (e.x. documents papiers, clés USB…) afin de les ranger dans un endroit sécurisé tel qu'à l'intérieur d'un casier ou d'un bureau cadenassé.

- Supprimer toutes informations de ses écrans ;

- Éteindre ou mettre en veille les Actifs informationnels numériques qu'il contrôle ou possède ; et

- Verrouiller ses accès aux Actifs informationnels qu'il contrôle ou possède.

Diligence en cas d'usage d'installations ou d'équipements partagés. Si l'Utilisateur doit imprimer un document en utilisant une imprimante ou une photocopieuse, il doit s'assurer de retirer le plus rapidement possible toute documentation papier de l'imprimante ou de la photocopieuse. Il en va de même lorsqu'il reçoit ou communique un document par télécopieur ou par courrier.

5.9. Responsabilité en matière de mot de passe

Obligation d'utiliser des mots de passe. Tout Utilisateur disposant de droits d'accès à un Actif informatif doit s'assurer que ses accès sont protégés par des mots de passes répondant aux conditions suivantes :

1. Les mots de passe ne doivent pas être divulgués à d'autres personnes, à l'exception de la direction et les administrateurs du système d'information ;

2. Les mots de passe ne doivent pas être transcrits sur des Actifs informationnels physiques, sauf par une méthode numérique sécurisée et approuvée par le Chef de la sécurité de l'information organisationnelle ;

3. Les mots de passe générés par l'utilisateur ne doivent pas être distribués par quelque moyen que ce soit (par distribution orale, écrite ou électronique, etc.) ;

4. Les mots de passe doivent être modifiés sans délai en présence d'indications que les mots de passe ou le système ont pu être compromis – dans ce cas, un Évènement de sécurité doit être signalé au Chef de la sécurité de l'information organisationnelle ;

5. Les mots de passe forts doivent être sélectionnés, de la manière suivante :

    - En utilisant au moins huit caractères,
    - En utilisant au moins un caractère numérique,
    - En utilisant au moins un caractère alphabétique majuscule,
    - En utilisant au moins un caractère alphabétique minuscule,
    - En utilisant au moins un caractère spécial,
    - Les mots de passe ne doivent pas être basés sur des données personnelles (par exemple, date de naissance, adresse, nom du membre de la famille, etc.),
    - Les trois derniers mots de passe créés par l'utilisateur ne doivent pas être réutilisés.

6. Un mot de passe doit être modifié lors de la première connexion à un Actif informationnel ou à un compte utilisateur ;

7. Les mots de passe ne doivent pas être stockés dans un système de connexion automatisé (par exemple, votre navigateur). Il est permis de stocker un mot de passe dans un gestionnaire de mot de passe avec l'approbation du Chef de la sécurité de l'information organisationnelle ;

8. Les mots de passe utilisés à des fins privées ne doivent pas être utilisés à des fins professionnelles.

Astuce pour mémoriser le mot de passe

Il peut être difficile de mémoriser un mot de passe répondant aux critères susmentionnés. Afin de faciliter sa mémorisation du mot de passe, nous vous proposons de mémoriser une phrase, choisie aléatoirement, et de composer le mot de passe à partir de la première lettre de chacun des mots composant la phrase. Ainsi :

« J'ai de la difficulté à mémoriser un mot de passe de seize caractères. »

Peut devenir le mot de passe suivant :

« Jadldàmumdpd16c. »

5.10. Utilisation d'Internet

Limitation de l'accès à l'Internet. Internet n'est accessible **que** via le réseau local de l'Établissement avec une infrastructure et une protection pare-feu appropriées.

Prohibition de l'accès à l'Internet. L'accès direct à Internet par modems, Internet mobile, clé USB d'internet, réseau sans fil n'appartenant pas à l'Établissement, par usage de VPN, ou autres appareils est interdit.

Limiter les accès à des pages Internet. Le Chef de la sécurité de l'information organisationnelle peut bloquer l'accès à certaines pages Internet pour des Utilisateurs individuels, des groupes d'utilisateurs ou tous les employés de l'Établissement. Si l'accès à certaines pages Web est bloqué, l'utilisateur peut soumettre une demande écrite au Chef de la sécurité de l'information organisationnelle pour obtenir l'autorisation d'accéder à ces pages.

Ne pas contourner les restrictions imposées. L'Utilisateur ne doit pas essayer de contourner les restrictions.

Éviter les sites web non sécurisés. L'utilisateur doit considérer les informations reçues par le biais de sites Web non vérifiés ou non protégés par un certificat de chiffrement comme non fiables. Ces informations ne peuvent être utilisées à des fins commerciales qu'après vérification de leur authenticité et de leur exactitude.

Responsabilité de son usage de l'Internet. L'Utilisateur est responsable de toutes les conséquences possibles découlant d'une utilisation non autorisée ou inappropriée des services ou contenus Internet.

5.11. Usage des Systèmes d'échange

N'utiliser que les Systèmes d'échange approuvés. L'Utilisateur ne peut pas utiliser des Méthodes d'échange qui ne sont pas inscrites dans le Registre des canaux de communication autorisés.

Non-responsabilité. Si un Utilisateur publie un message sur un système d'échange en son nom personnel, il doit déclarer sans ambiguïté que son message ne représente pas le point de vue de l'Établissement.

Vigilance à l'égard des tentatives d'hameçonnage. Tout Utilisateur doit rester en tout temps vigilant aux tentatives d'hameçonnage. Le destinataire d'un courriel ou d'un message texte doit se méfier de tout message de destinataire inconnu les invitant à cliquer sur un lien ou à télécharger un fichier en pièce jointe.

Notifications en cas d'hameçonnage. Tout Utilisateur recevant un pourriel ou un message tentant de l'hameçonner doit en informer sans délai le Chef de la sécurité de l'information organisationnelle. Il est important que l'Utilisateur lui indique s'il a cliqué sur un lien ou téléchargé un fichier en provenance de ce message ou courriel.

Suivre les instructions du Responsable. Un Utilisateur doit suivre toutes instructions du Chef de la sécurité de l'information organisationnelle à l'égard du pourriel ou du message tentant de l'hameçonner.

Reconnaitre les tentatives d'hameçonnage.

Une personne devrait se méfier des messages ou des courriels comportant un ou plusieurs des éléments suivants :

- le message ou courriel tentent de susciter un sentiment d'urgence ;

- le message ou courriel comportent un hyperlien ;

- plusieurs fautes d'orthographe ou de syntaxe sont présentes dans le message ou le courriel ; ou

- le message ou le courriel provient d'une adresse inconnue.

5.12. Droit d'auteur

Respecter la propriété de l'Établissement. Les Utilisateurs ne doivent pas faire de copies non autorisées de logiciels ou de documents appartenant à l'Établissement, sauf dans les cas autorisés par la loi, par le propriétaire ou le Chef de la sécurité de l'information organisationnelle.

Respecter la propriété de tiers. Les Utilisateurs ne doivent pas copier de logiciels ou d'autres documents originaux provenant d'autres sources et sont responsables de toutes les conséquences qui pourraient survenir en cas d'infraction survenant en vertu de la *Loi sur le droit d'auteur,* LRC 1985, c C-42.

Seul le Directeur général de l'École secondaire de Bromptonville peut accorder à d'autres employés l'accès à l'un des documents susmentionnés.

6. Validité et gestion des documents

Le propriétaire de ce document est le Chef de la sécurité de l'information organisationnelle, qui doit vérifier et, si nécessaire, mettre à jour le document au moins une fois par an.

7. Entrée en vigueur

Ce document entre en vigueur à la date de son adoption par le Comité.