Centre de services scolaire des Hautes-Laurentides
Québec

SG-2023-26

☐ Règlement
☐ Politique (cadre, code)
☒ Procédure (directive, guide, référentiel)

LIGNES DIRECTRICES SUR LA SÉCURITÉ DE L'INFORMATION

Approbation :	Direction générale
Responsable :	Direction du Service du secrétariat général, des communications et du transport
Date d'approbation :	15 mai 2023
Date d'entrée en vigueur :	15 mai 2023
Date prévue de révision :	Au besoin

Liste des écrits de gestion remplacés :

Consultations effectuées :
Comité consultatif de gestion – 13 octobre 2022 (art. 193.3 de la LIP).

Ce document a été rédigé en respectant les règles de la nouvelle orthographe de l'Office de la langue française.

TABLE DES MATIÈRES

1. PRÉAMBULE

Les *Lignes directrices sur la sécurité de l'information* (ci-après appelées *Lignes directrices*) découlent de la *Politique de sécurité de l'information* et du *Cadre de gestion de la sécurité de l'information*. Elles s'insèrent aussi dans le prolongement du *Code d'éthique* du Centre de services scolaire des Hautes-Laurentides (CSSHL). Elles s'appliquent à tous les utilisateurs ayant accès à l'information du centre de services scolaire.

La notion d'utilisateur comprend tout le personnel et toute personne physique ou morale qui, à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public, utilisent les actifs informationnels du CSSHL.

Rappelons que l'information peut être d'ordre pédagogique ou d'ordre administratif et celle-ci peut se retrouver sous forme numérique ou non numérique (papier).

2. CADRE LÉGAL

- *Politique de sécurité de l'information* (SG-2018-20).
- *Cadre de gestion de la sécurité de l'information* (SG-2018-21).
- *Code d'éthique* (RH-2023-22).

3. DIRECTIVES SPÉCIFIQUES

3.1 INFORMATION NÉCESSAIRE

L'utilisateur doit se limiter à utiliser les informations nécessaires à l'exercice de ses fonctions en se limitant aux fins auxquelles elles sont destinées.

3.2 RESPECT DES DROITS DE PROPRIÉTÉ INTELLECTUELLE

L'utilisateur doit se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister.

3.3 INTÉGRITÉ DES DONNÉES

Le CSSHL doit s'assurer de préserver l'intégrité des données afin que les informations ne puissent subir aucune altération ni destruction sans autorisation ou de façon erronée.

4. RESPONSABILITÉS ET OBLIGATIONS DE L'UTILISATEUR

L'utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le CSSHL. Pour ce faire, il doit faire preuve de rigueur, de prudence et mettre en application les éléments suivants :

4.1 FORMATION-SENSIBILISATION À LA SÉCURITÉ INFORMATIQUE (CAPSULES)

La sensibilisation est un élément clé de la sécurité informationnelle. En ce sens, l'utilisateur doit suivre les capsules de formation-sensibilisation offertes par le CSSHL. L'accès est géré par le Service des ressources informatiques.

4.2 PRINCIPE DE BUREAU PROPRE

Le vol de données et d'informations confidentielles peut se faire non seulement par un moyen informatique, mais également directement sur le lieu de travail. Quelques mesures de protection conformes au principe de bureau propre :

- Verrouillez votre session de travail dès que vous quittez votre poste de travail (touche Windows + L);
- Verrouillez les classeurs et tout autre espace de rangement qui contiennent de l'information précieuse;
- Ne laissez pas de documents confidentiels dans le bac de sortie de l'imprimante;
- Ne laissez pas d'informations confidentielles ni de supports de données mobiles sur votre bureau lorsque vous le quittez, et ce, même de façon temporaire;
- Effacez l'information sensible inscrite sur un tableau blanc dans votre bureau ou dans une salle de travail;
- N'utilisez jamais une clé USB dont la provenance vous est inconnue;
- Détruisez de façon sécuritaire les documents contenant des renseignements personnels dont vous n'avez plus besoin (déchiquetage ou ramassage par une firme spécialisée).

4.3 COURRIEL

Les courriels font partie des outils privilégiés par les fraudeurs afin de réaliser des attaques informatiques. Les bonnes pratiques concernant les courriels :

- **Pièces jointes :** N'ouvrez pas les pièces jointes provenant d'expéditeurs inconnus ou dont le titre et le format paraissent incohérents;
- **Liens :** Parfois un lien peut apparaitre adéquat, mais cache un lien frauduleux. Si des liens figurent dans un courriel, passez votre souris au-dessus avant de cliquer;
- **Chaine de lettre :** N'ouvrez pas et ne relayez pas de messages de types chaines de lettre;
- **Informations personnelles ou confidentielles :** Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles.
- **Cryptage :** Les informations envoyées par courriel ne doivent pas être de nature confidentielle à moins d'utiliser l'option de cryptage offert par Office 365.

4.4 MOT DE PASSE (RÉSEAU OU APPLICATIONS)

Les systèmes et les applications qui hébergent des données sensibles et confidentielles sont protégés par un code d'identification personnel (ex. : courriel) et un mot de passe. Le niveau de protection des données est dès lors proportionnel au degré de complexité et au caractère secret du mot de passe. Les bonnes pratiques concernant les mots de passe :

- **Complexe :** Utilisez un mot de passe suffisamment complexe (composé de lettres, de chiffres et de caractères spéciaux);
- **Confidentiel :** Ne divulguez jamais votre mot de passe et n'écrivez votre mot de passe nulle part;
- **Unique :** Utilisez un mot de passe distinct pour le travail et vos sites personnels;
- **Double sécurité :** Si possible, activez l'authentification doubles facteurs.

4.5 NAVIGATION INTERNET

Les virus ne sont pas qu'une affaire de fichier dans un courriel. C'est aussi une page Web infectée et des mesures de sécurité inadéquate. Les bonnes pratiques concernant la navigation Internet :

- **Sites sécurisés :** Lors de l'échange de données confidentielles ou financières (ex. : achat en ligne), n'utilisez seulement que des sites en HTTPS dont vous aurez aussi validé le certificat et vérifié l'exactitude du lien;
- **Message de type POPUP :** Ne cliquez pas sur les messages de type POPUP. Ils sont souvent porteurs d'un message vous mentionnant que votre poste est infecté. Le lien vers lequel vous dirige ce message contient des logiciels malveillants;
- **Liens :** Parfois un lien peut apparaitre adéquat, mais cache un lien frauduleux. Passez votre souris au-dessus avant de cliquer.

4.6 ORDINATEUR (FIXE OU PORTABLE)

Les ordinateurs prêtés aux utilisateurs pour leur travail contiennent des informations professionnelles qui sont souvent confidentielles (humaines, éducatives, financières…). Les bonnes pratiques concernant l'utilisation des ordinateurs :

- **Mot de passe :** Votre appareil doit être protégé par un mot de passe et vous devez l'entrer à chaque démarrage;
- **Verrouillage :** Verrouillez votre session dès que vous quittez votre poste de travail (touches Windows + L);
- **Mise à jour du système d'exploitation et des logiciels :** Tenir à jour votre système d'exploitation et les applications sur votre appareil. Pour le système d'exploitation, l'option de mise à jour est activée par défaut par le Service des ressources informatiques;
- **Divers :** Ne pas modifier la configuration des mesures de sécurité ou les désactiver (antivirus, sauvegarde, etc.).

4.7 TÉLÉPHONE INTELLIGENT (PROFESSIONNEL OU PERSONNEL)

Les téléphones contiennent beaucoup d'informations personnelles et parfois professionnelles (informations bancaires, renseignements personnels, contacts, photos, courriels, etc.). Les bonnes pratiques sur leur utilisation :

- **Mécanisme de verrouillage :** Il est important de protéger votre appareil avec un mécanisme de verrouillage (NIP, mot de passe, biométrique…);
- **Mise à jour du système d'exploitation et des logiciels :** Tenir à jour votre système d'exploitation et les applications sur votre appareil;
- **Applications :** Assurez-vous que les logiciels installés proviennent des éditeurs officiels des logiciels ou de sites de confiance (Apple Store, Google Play);
- **Option de sécurité :** Configurez l'application de sécurité. En cas de perte ou de vol, vous pourrez ainsi localiser votre appareil et effacer les données si cela s'avère nécessaire.

4.8 MÉDIAS SOCIAUX

Les médias sociaux peuvent contenir beaucoup d'informations à votre sujet qui sont étalées au grand public si l'on ne porte pas une attention particulière à la sécurisation de ceux-ci.

- **Profil :** Limitez au maximum l'accès à votre profil (informations, photos) en configurant les paramètres de sécurité de la plateforme;

- **Informations personnelles :** Ne divulguez qu'un minimum d'informations personnelles;
- **Liens :** Portez attention aux liens avant de cliquer (même ceux de vos amis);
- **Sécurité :** Utilisez un mot de passe fort pour protéger l'accès à vos comptes et préconisez l'authentification doubles facteurs.

5. SIGNALEMENT

L'utilisateur doit signaler immédiatement au Service des ressources informatiques tout acte dont il a connaissance, susceptible de constituer une violation des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du CSSHL. Pour ce faire, l'utilisateur doit signaler l'incident par courriel à si@csshl.gouv.qc.ca et/ou aviser le technicien-opérateur informatique de son établissement. Il peut également composer le poste téléphonique 7178 lequel est assigné au responsable de la sécurité informatique.

6. RESPONSABILITÉS ET OBLIGATIONS DES INTERVENANTS

6.1 LA DIRECTION GÉNÉRALE

La Direction générale est responsable de voir à la mise en œuvre des *Lignes directrices sur la sécurité de l'information* et de voir à ce qu'elles soient observées par les services et établissements sous sa gouverne.

6.2 LES GESTIONNAIRES

Les gestionnaires, dans leur ensemble, sont responsables de l'application des *Lignes directrices sur la sécurité de l'information* ainsi que de l'encadrement des utilisateurs sous leur gouverne. Ils doivent intervenir au besoin et peuvent demander qu'une enquête soit effectuée concernant un utilisateur ou un groupe d'utilisateurs.

6.3 RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSI)

Le RSI accompagne les gestionnaires dans l'application des *Lignes directrices sur la sécurité de l'information*. De plus, il est responsable des enquêtes liées à la sécurité informationnelle (fuite de données, non-respect des règles de sécurité, etc.).

6.4 LE SERVICE DES RESSOURCES INFORMATIQUES

Au besoin, le Service des ressources informatiques accompagne le RSI sur des enquêtes liées à la sécurité informationnelle.