



Service : Service des technologies de l'information	Code : POL-11TI-001
Date d'approbation : 2025-12-09	Numéro de résolution : 2025-12-09-CA-11
Responsable de l'application : Chef de la sécurité de l'information organisationnelle	
Entrée en vigueur : 2026-07-01	

Section 1 – Disposition générale

1. PRÉAMBULE

Le Centre de services scolaire des Hautes-Rivières (CSSDHR) reconnaît que l'information et les technologies qui la soutiennent sont essentielles à ses opérations courantes et à l'accomplissement de sa mission. Étant donné la valeur pédagogique, administrative, légale et financière de ses ressources informationnelles, ces dernières doivent faire l'objet d'une évaluation continue, d'une utilisation et d'une protection appropriée et adéquate tout au long de leur cycle de vie, selon les meilleures pratiques en matière de sécurité informationnelle et avec une approche de gestion des risques, quel qu'en soit le support ou l'emplacement.

L'application de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LRQ, chapitre G-1.03), de la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (RLRQ, 2021, chapitre 25) et de la *Directive gouvernementale sur la sécurité de l'information* (2021) du Secrétariat du Conseil du trésor du Québec applicable aux organismes publics impose des obligations importantes aux établissements scolaires ainsi qu'à leurs partenaires en matière de sécurité de l'information.

Pour se conformer à ses obligations réglementaires et légales ainsi que pour atteindre des standards élevés en matière de sécurité de l'information, le CSSDHR doit adopter une politique générale de sécurité de l'information, la garder à jour et veiller à son application. Cette politique vise à encadrer la gestion des risques, le contrôle des accès aux ressources informationnelles, la gestion des incidents, la continuité des activités ainsi que tout processus lié à la sécurité de l'information.

2. CADRE LÉGISLATIF, RÉGLEMENTAIRE OU NORMATIF

Le présent document s'appuie sur des fondements légaux et normatifs, notamment les lois, directives, normes, standards et pratiques gouvernementales.

Fondements légaux :

- Directive gouvernementale sur la sécurité de l'information ;
- Cadre gouvernemental de gestion de la sécurité de l'information ;
- Aide-mémoire : Politique gouvernementale en cybersécurité ;
- Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1) ;
- Loi modernisant des dispositions législatives en matière de protection des renseignements personnels (RLRQ, 2021, chapitre 25) ;
- Règlement sur les incidents de confidentialité ;
- Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LRQ, chapitre G-1.03) ;

- 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 ;
- Règles relatives à la gestion des projets en ressources informationnelles ;
- Règles relatives à la planification et à la gestion des ressources informationnelles ;
- Loi sur les archives (LRQ, chapitre A-21.1) ;
- Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics ;
- Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r 2).

Fondements normatifs :

- Cadre de gestion des risques et des incidents à portée gouvernementale en matière de sécurité de l'information ;
- Cadre gouvernemental de gestion de la sécurité de l'information ;
- Normes internationales, notamment ISO 27000 et NIST 800-60.

3. CHAMP D'APPLICATION

3.1 Personnes visées

Cette politique s'applique, sans exception, à toutes les personnes physiques ou morales – qu'elles aient un statut régulier, temporaire ou contractuel – appelées à utiliser les ressources informationnelles du CSSDHR, notamment :

- le personnel à l'emploi du CSSDHR ;
- les consultants œuvrant pour le CSSDHR ;
- les membres des instances et des comités du CSSDHR ;
- les élèves, parents, tuteurs légaux et bénévoles du CSSDHR ;
- les stagiaires du CSSDHR ;
- les partenaires, fournisseurs et tiers du CSSDHR.

3.2 Actifs visés

Cette politique couvre également l'ensemble des informations et des ressources informationnelles, et ce, quel que soit leur support de conservation, notamment :

- celles appartenant au CSSDHR ;
- celles détenues par un tiers, mais appartenant au CSSDHR ;
- celles utilisées et détenues par un tiers pour le compte ou au bénéfice du CSSDHR.

3.3 Activités visées

Cette politique concerne l'ensemble des activités liées au cycle de vie de l'information, à savoir : la collecte, l'enregistrement, le traitement, la modification, la diffusion, la conservation et la destruction des ressources informationnelles du CSSDHR, et ce, en tout lieu, en tout temps et sur tout type de support.



4. OBJECTIFS

La présente politique constitue le cadre général de gestion de la sécurité des ressources informationnelles. Dans le respect des droits et obligations du CSSDHR, elle vise à garantir l'atteinte des objectifs en matière de sécurité de l'information, et plus particulièrement à :

1. assurer la protection des ressources informationnelles tout au long de leur cycle de vie, quel que soit leur support ou leur emplacement ;
2. assurer l'intégrité de l'information en la protégeant contre toute destruction, modification ou altération, de quelque nature que ce soit, sans autorisation préalable du responsable de la ressource informationnelle ;
3. assurer la disponibilité de l'information afin qu'elle soit accessible au moment opportun et utilisable sur demande par les personnes et les outils technologiques autorisés ;
4. préserver la confidentialité de l'information en veillant à ce qu'elle ne soit ni accessible ni divulguée à des personnes ou entités non autorisées ;
5. assurer la traçabilité des changements d'état de l'information tout au long de son cycle de vie ;
6. regrouper les lignes directrices qui orientent les intervenants en matière de sécurité de l'information, et définir leurs rôles et responsabilités ;
7. identifier et classer les ressources informationnelles du CSSDHR selon leur degré de criticité, et assurer une vigie constante de leur évaluation ainsi que de leur protection adéquate ;
8. assurer la conformité aux lois ou à tout autre cadre réglementaire applicable ;
9. mettre en place un plan de continuité des services essentiels ainsi qu'un plan de relève informatique afin d'assurer la résilience des opérations en cas d'incident ou d'interruption ;
10. assurer le respect de la vie privée des individus, notamment en protégeant la confidentialité des renseignements personnels.

5. DÉFINITIONS

5.1 Autorisation

Attribution, par une autorité compétente, de droits d'accès aux ressources informationnelles à une personne, un dispositif ou une entité. Cette autorisation constitue un privilège leur permettant d'accéder à ces ressources conformément aux règles établies.

5.2 Chef de la sécurité de l'information organisationnelle (CSIO)

Membre du personnel d'encadrement du CSSDHR responsable de la prise en charge globale de la sécurité de l'information au sein de l'organisation. Conformément au *Cadre gouvernemental de gestion de la sécurité de l'information* – adopté en vertu de l'article 21 de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* – cette personne soutient la direction générale dans l'exercice de ses obligations en matière de sécurité de l'information.

5.3 Code d'accès

Mécanisme d'identification et d'authentification reposant sur un code personnel et un mot de passe, ou sur un dispositif équivalent, comme une carte magnétique ou une carte à puce, permettant d'identifier de manière unique toute personne qui utilise des ressources informationnelles du CSSDHR.



5.4 Comité sur l'accès à l'information, la protection des renseignements personnels et la sécurité de l'information (CAIPRPSI)

Comité du CSSDHR regroupant notamment le responsable de la protection des renseignements personnels (RPRP), le chef de la sécurité de l'information organisationnelle (CSIO), le coordonnateur organisationnel des mesures de sécurité de l'information (COMSI), la direction du Service des technologies de l'information (STI), la personne responsable de l'accès à l'information ainsi que la personne responsable de la gestion documentaire.

Ce comité répond aux obligations relatives à la mise en place d'un comité sur l'accès à l'information et la protection des renseignements personnels, conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Il satisfait également aux exigences liées à l'existence d'un comité sur la sécurité de l'information, comme prévu dans le *Cadre gouvernemental de gestion de la sécurité de l'information*.

5.5 Coordonnateur organisationnel des mesures de sécurité de l'information (COMSI)

Membre du personnel d'encadrement ou professionnel du CSSDHR chargé de la mise en œuvre des mesures de sécurité informatique visant à protéger les actifs informationnels internes, y compris les renseignements personnels détenus par l'organisation. Cette personne assure également la coordination des mesures de sécurité gérées à l'externe par le ministère de la Cybersécurité et du Numérique.

5.6 Confidentialité

Propriété que possède une donnée ou une information dont l'accès et l'utilisation sont strictement réservés à des personnes ou entités autorisées.

5.7 Cycle de vie de l'information

Ensemble des étapes que parcourt une information, depuis sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, conformément au calendrier de conservation du CSSDHR.

5.8 Disponibilité

Propriété qu'ont les données, l'information et les systèmes d'information et de communication d'être accessibles et utilisables, en temps opportun et de manière adéquate, par les personnes et les outils technologiques autorisés.

5.9 Droit d'auteur

Droit exclusif que détient une personne de publier, produire, reproduire, représenter ou exécuter publiquement son œuvre, de la traduire ou de l'adapter sous une autre forme, ou d'autoriser une autre personne à le faire.

5.10 Écrit de gestion

Ensemble des politiques, règlements, directives, procédures et bonnes pratiques encadrant les activités du CSSDHR.

5.11 Évaluation des facteurs relatifs à la vie privée (EFVP)

Démarche préventive visant à analyser les éléments d'un projet susceptibles d'avoir des impacts, positifs ou négatifs, sur le respect de la vie privée des personnes concernées. Elle permet d'identifier les mesures appropriées pour mieux protéger les renseignements personnels et assurer une conformité accrue aux principes de protection de la vie privée.



5.12 Gestion des menaces, des vulnérabilités et des incidents (GMVI)

Processus intégré visant à identifier, évaluer, traiter et résoudre les menaces, les vulnérabilités et les incidents liés à la sécurité de l'information, afin de préserver l'intégrité, la confidentialité et la disponibilité des ressources informationnelles.

5.13 Intégrité

Propriété d'une information ou d'une technologie de l'information garantissant qu'elle ne peut être modifiée, altérée ou détruite sans autorisation.

5.14 Organisme public

Entité relevant du secteur public, incluant notamment le gouvernement, le Conseil exécutif, le Conseil du trésor, les ministères, les organismes gouvernementaux, les organismes municipaux, les organismes scolaires publics ainsi que les établissements de santé et de services sociaux.

5.15 STI

Service des technologies de l'information du CSSDHR, responsable de la gestion, du développement, de la sécurité et du soutien des infrastructures et des systèmes informatiques de l'organisation.

5.16 Renseignement personnel

Information concernant une personne physique permettant de l'identifier, directement ou indirectement. Le terme inclut les renseignements personnels anonymisés, dépersonnalisés et confidentiels. Ces renseignements peuvent être regroupés en différentes catégories, notamment :

- renseignements d'identification : nom, numéro de fiche, code permanent, adresse, numéro de permis de conduire, date de naissance, numéro d'assurance sociale, numéro d'assurance maladie, numéro de passeport, etc. ;
- renseignements financiers : numéro de carte de crédit ou de débit, informations bancaires (hypothèque, numéro de compte, placements, NIP), contrat de travail, salaire, etc. ;
- renseignements scolaires ou académiques : résultats, niveaux de difficulté, plan d'intervention, difficultés de comportement, etc. ;
- renseignements médicaux ou génétiques : diagnostic médical, historique médical, arrêt de travail, etc. ;
- renseignements démographiques : orientation sexuelle, identité de genre, religion, origine ethnique, niveau de scolarité, état matrimonial, etc.

5.17 Réseau du CSSDHR

Infrastructure informatique hybride – sur site et infonuagique – qui relie l'ensemble des établissements et permet l'accès aux services numériques hébergés à la fois dans les centres de données du CSSDHR et dans le nuage. Ce réseau assure la connectivité, la sécurité et la disponibilité des ressources : Internet, communications (dont la visioconférence), applications pédagogiques et administratives, stockage et sauvegardes. Conçu pour la résilience et la sécurité, il soutient efficacement les activités pédagogiques et administratives, quel que soit le médium de communication utilisé (notamment le réseau sans fil, le réseau filaire ou la fibre optique).

5.18 Responsable des ressources informationnelles

Direction d'une unité administrative au sein du CSSDHR dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des ressources informationnelles sous sa responsabilité. Elle peut déléguer certaines responsabilités à un membre de son équipe, selon les besoins et les compétences requises.

5.19 Responsable de la protection des renseignements personnels (RPRP)

Membre du personnel d'encadrement du CSSDHR désigné pour veiller à l'application et au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. Elle met en œuvre les règles de gouvernance relatives aux renseignements personnels.

5.20 Ressource informationnelle

Information acquise ou conservée par le CSSDHR, quel que soit son canal de communication (ex. : téléphone, courriel, clavardage) ou son support (ex. : papier, ruban magnétique, support électronique). Cela englobe les systèmes et supports d'information, les technologies de l'information, les installations ou tout ensemble de ces éléments. Une ressource informationnelle peut, par exemple, être un disque dur, une clé USB, un dossier papier dans un classeur ou une boîte de documents gardée aux Archives.

5.21 Risques liés à la sécurité de l'information

Tout événement survenant au cours du cycle de vie de l'information et comportant un degré d'incertitude susceptible de compromettre sa confidentialité, son intégrité ou sa disponibilité, et d'entraîner un préjudice pour l'organisation ou les personnes concernées.

5.22 Technologies de l'information

Ensemble des techniques, principalement issues des domaines de l'informatique, de l'audiovisuel, du multimédia, d'Internet et des télécommunications (réseau filaire, sans fil et téléphonie), permettant à toute personne utilisatrice de communiquer, d'accéder aux sources d'information, de stocker, de manipuler, de produire et de transmettre de l'information.

5.23 Situation urgente

Tout événement ou toute condition ou circonstance imprévisible nécessitant une intervention immédiate afin de prévenir un impact significatif ou irréversible sur la santé, la vie, la sécurité, la propriété ou l'environnement.

5.24 Unité administrative

Toute entité placée sous la responsabilité d'une direction au sein du CSSDHR. Il peut s'agir d'une école, d'un centre ou d'un service.

5.25 Personne utilisatrice

Toute personne qui utilise des informations, des applications ou des outils numériques appartenant au CSSDHR.



Section 2 – Énoncés de la politique

6. RÔLES ET RESPONSABILITÉS

6.1 CAIPRPSI

Le CAIPRPSI conseille les personnes titulaires des mandats de CSIO et de RPRP dans l'exercice de leurs fonctions.

6.2 COMSI

La personne qui exerce le rôle de COMSI collabore avec la personne titulaire de la charge de CSIO du CSSDHR à l'élaboration de stratégies en matière de sécurité de l'information. Elle contribue notamment à :

- maintenir le registre des événements et des incidents liés à la sécurité de l'information ;
- effectuer et participer aux analyses de risques en sécurité de l'information ;
- gérer le processus de déclaration des incidents et de résolution des problèmes liés à la sécurité de l'information.

6.3 CSIO

La personne nommée CSIO a la responsabilité de la prise en charge globale de la sécurité de l'information au sein du CSSDHR, et ce, conformément au Cadre gouvernemental de gestion de la sécurité de l'information. Elle apporte à la direction générale le soutien nécessaire lui permettant d'assumer ses obligations en matière de sécurité de l'information.

Elle doit approuver conjointement avec la personne nommée RPRP toute EFVP liée à un projet d'acquisition, de développement ou de refonte de système d'information ou encore de prestation électronique de services impliquant des renseignements personnels.

Elle doit approuver seule tout projet d'acquisition, de développement ou de refonte de système d'information ou encore de prestation électronique de services n'impliquant pas de renseignements personnels.

6.4 Direction générale

La direction générale détermine les orientations stratégiques en matière de sécurité de l'information. Elle désigne les personnes occupant les rôles de chef de la sécurité de l'information organisationnelle (CSIO), de coordonnateur organisationnel des mesures de sécurité de l'information (COMSI) et de responsable de la protection des renseignements personnels (RPRP).

6.5 Direction du Service des technologies de l'information

La direction du Service des technologies de l'information assume la responsabilité de l'application de la présente politique. Elle veille à la prise en charge des exigences de sécurité de l'information, tant dans l'exploitation des systèmes d'information que dans la réalisation de projets de développement ou d'acquisition de ces systèmes.

En collaboration avec la personne nommée CSIO, elle participe à l'identification et à l'intégration des mesures de sécurité permettant de protéger adéquatement les ressources informationnelles du CSSDHR. Ces mesures sont établies en fonction du niveau de sensibilité de l'information, tout en tenant compte des exigences réglementaires, d'affaires, légales ou contractuelles.



6.6 Direction du Service des ressources humaines

La direction du Service des ressources humaines doit, en matière de sécurité de l'information :

- vérifier les antécédents judiciaires des personnes candidates à l'embauche et des membres du personnel du CSSDHR impliqués dans la sécurité de l'information ;
- informer tout membre ou tout nouveau membre du personnel du CSSDHR et obtenir son engagement explicite au respect du Code de conduite – *Utilisation des ressources informationnelles*.

6.7 Responsable des ressources informationnelles

La personne responsable des ressources informationnelles doit :

- participer à la catégorisation de l'information sous sa responsabilité et à l'analyse des risques, contribuant ainsi activement aux EFVP ;
- veiller à la protection de l'information et des systèmes d'information, en conformité avec la présente politique ;
- rapporter tout événement ou toute menace concernant la sécurité de l'information à la personne nommée CSIO ;
- collaborer à la mise en œuvre des mesures correctives visant à améliorer la sécurité de l'information à la suite d'un incident ;
- s'assurer que les exigences relatives à la sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et voir à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la présente politique ainsi que l'ensemble des éléments du cadre de gestion.

6.8 RPRP

La personne nommée RPRP doit approuver conjointement avec la personne exerçant la charge de CSIO toute EFVP relative à tout projet d'acquisition, de développement ou de refonte de système d'information ou encore de prestation électronique de services impliquant des renseignements personnels.

6.9 Personnes utilisatrices

Les personnes utilisatrices de l'information du CSSDHR sont responsables de sa sécurité, et ce, tant lorsqu'elles y accèdent que lorsqu'elles la consultent ou la traitent. L'information visée est celle que le CSSDHR détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

À cette fin, les personnes utilisatrices doivent :

- se conformer à la présente politique et à tout écrit de gestion du CSSDHR en matière de sécurité de l'information et de ressources informationnelles ;
- s'assurer que l'utilisation d'un système d'information ou d'une prestation électronique de service est autorisée par le CSSDHR ;
- conserver de façon sécuritaire et confidentielle leurs codes d'accès ;
- assumer la responsabilité des actions effectuées à l'aide de leurs codes d'accès, qu'elles soient commises par elles-mêmes ou par un tiers, sauf en cas de vol d'un code, à condition que celui-ci ait été géré de façon prudente et responsable ;



- signaler à une personne responsable ou à leur gestionnaire immédiat toute situation susceptible de compromettre la sécurité des ressources informationnelles ;
- utiliser leurs droits d'accès, l'information et les systèmes d'information mis à leur disposition uniquement dans le cadre prévu et aux fins autorisées ;
- respecter les mesures de sécurité en place, sans les contourner, les modifier, ni les désactiver ;
- collaborer à toute intervention visant à identifier ou à mitiger une menace ou un incident en lien avec la sécurité de l'information.

Le CSSDHR se réserve le droit de restreindre l'accès à ses ressources à toute personne utilisatrice qui ne se conforme pas à la présente politique.

7. PRINCIPES GÉNÉRAUX

7.1 Applications utilisées pour la gestion des renseignements personnels

Le CSSDHR procède à une EFVP pour tout projet d'acquisition, de développement ou de refonte de système d'information ainsi que pour toute prestation électronique de services impliquant des renseignements personnels.

Tous les renseignements personnels touchant les élèves, les membres du personnel ou tout autre intervenant doivent être hébergés exclusivement sur les systèmes prescrits par les services éducatifs ou administratifs concernés. Le CSSDHR a l'obligation d'assurer la disponibilité, l'intégrité et la confidentialité des renseignements personnels qu'il détient.

Afin d'assurer une gestion rigoureuse du cycle de vie des ressources informationnelles, les interactions professionnelles entre les membres du personnel doivent se faire uniquement par l'entremise des outils approuvés et prescrits par le CSSDHR.

L'enregistrement de renseignements personnels dans une application non approuvée contrevient à la présente politique.

7.2 Demandes d'accès à l'information

Conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, le CSSDHR se réserve le droit, dans le cadre d'une enquête, d'accéder à toute information disponible afin de répondre à un besoin précis, et ce, selon la procédure établie de Gestion des demandes d'accès aux documents et aux renseignements personnels.

7.3 Droits d'auteur

La personne utilisatrice doit, en tout temps, respecter les droits d'auteur ainsi que les autres droits de propriété intellectuelle des tiers. La reproduction de logiciels, de banques de données ou de contenus informationnels (textuels, sonores, visuels ou symboliques) n'est autorisée qu'à des fins de copie de sécurité ou conformément aux modalités de la licence d'utilisation applicable.

Il est interdit à toute personne d'effectuer ou de participer, directement ou indirectement, à la reproduction de logiciels, d'objets numérisés ou de leur documentation sans le consentement préalable du titulaire des droits d'auteur. De même, l'utilisation de reproductions illicites de logiciels ou de données numérisées sur les équipements informatiques ou les réseaux de télécommunication appartenant au CSSDHR, ou sur tout autre équipement utilisé dans ses locaux est strictement interdite.



7.4 Gestion de la continuité des services essentiels

Chaque unité administrative doit disposer d'un plan visant à assurer la continuité des services essentiels à la suite d'une interruption des systèmes informatiques. Ce plan doit inclure l'identification des risques, l'évaluation des impacts potentiels ainsi que la mise en œuvre de mesures permettant de limiter les interruptions et de garantir une reprise efficace et sécuritaire des opérations critiques.

7.5 Gestion des identités et des accès (GIA)

La gestion des identités et des accès est encadrée et contrôlée afin de garantir que l'accès à toute information détenue par le CSSDHR ainsi que sa divulgation et son utilisation soient strictement réservés aux personnes autorisées.

L'accès minimal et suffisant est accordé en fonction des niveaux requis pour l'exécution des tâches. Cette approche s'applique tant aux personnes utilisatrices qu'aux processus, et vise à réduire les risques liés aux erreurs, aux actions malveillantes ou aux logiciels malveillants, en limitant la surface d'attaque. Les individus et les systèmes doivent disposer uniquement des privilèges nécessaires à l'exercice de leurs responsabilités afin de prévenir tout accès non autorisé aux renseignements confidentiels.

L'accès aux informations est donc strictement limité à l'exercice des fonctions autorisées. Toute utilisation des accès à des fins personnelles ou non conformes est formellement interdite.

7.6 Gestion des incidents

La gestion des incidents repose sur la mise en place de procédures de signalement, d'analyse des événements liés à la sécurité de l'information ainsi que de mesures correctives appropriées. Ces interventions visent à limiter les impacts, à rétablir les services essentiels et à assurer la continuité des opérations. Dans le cadre de cette gestion, le CSSDHR peut exercer ses pouvoirs et prérogatives en cas d'utilisation inappropriée des ressources informationnelles.

7.7 Gestion des risques

La gestion des risques liés aux ressources informationnelles du CSSDHR repose sur une analyse rigoureuse des menaces pouvant compromettre l'intégrité, la disponibilité et la confidentialité des informations détenues par l'organisation. Cette analyse permet d'identifier les vulnérabilités, d'évaluer les impacts potentiels et de définir des mesures compensatoires adaptées à l'utilisation et à l'exploitation des systèmes d'information, en fonction des résultats attendus.

7.8 Gestion des vulnérabilités et des menaces

La gestion des vulnérabilités et des menaces repose sur la mise en œuvre de mesures préventives et correctives visant à assurer la sécurité de l'information. Elle s'inscrit dans le cadre du processus de gestion des menaces, des vulnérabilités et des incidents (GMVI), et contribue à la protection des actifs informationnels du CSSDHR contre les risques.

7.9 Interventions techniques sur les équipements réseaux du CSSDHR

Les interventions sur les équipements réseaux du CSSDHR, notamment les commutateurs, pare-feu, câblage, bornes sans fil et téléphonie, sont strictement réservées au personnel mandaté par le STI.

Toute intervention technique ou disposition d'équipement informatique doit faire l'objet d'une approbation préalable par la direction du STI.



En ce qui concerne le matériel désuet, le STI s'en défait conformément à la *Politique de disposition du matériel désuet ou en surplus (RIP 05)*.

7.10 Respect de la mission de l'organisation et préservation de sa réputation

Afin de préserver la réputation du CSSDHR et de maintenir la confiance du public, toute utilisation des ressources informationnelles à des fins non autorisées ou illégales est formellement interdite.

7.11 Situation urgente

Dans des circonstances exceptionnelles, l'urgence d'une situation peut justifier une dérogation à l'application de la présente politique. Dans un tel cas, une déclaration détaillée doit être transmise au CSIO immédiatement après les événements.

7.12 Utilisation à des fins personnelles proscrite

Les ressources informationnelles sont mises à la disposition des personnes utilisatrices exclusivement pour soutenir les activités d'enseignement, d'apprentissage, de gestion, d'administration et de services à la collectivité, en lien avec la mission du CSSDHR et celles de ses établissements.

L'espace personnel des téléphones cellulaires fournis par le CSSDHR est exempté de cette restriction.

En dehors des heures de travail, l'utilisation d'un navigateur Web peut être tolérée par la direction de l'unité administrative. Cette utilisation demeure soumise aux mêmes critères que ceux applicables à l'utilisation professionnelle, incluant les mécanismes de surveillance en place.

L'accès à des courriels personnels ou à des espaces de partage de fichiers personnels à partir des ordinateurs et tablettes du CSSDHR est interdit. Il est également interdit d'y conserver du contenu à des fins personnelles.

Les contenus hébergés dans l'écosystème du CSSDHR sont la propriété exclusive du CSSDHR. De la même manière, tout contenu produit à l'aide des ressources informationnelles du CSSDHR ou dans le cadre des fonctions des personnes utilisatrices appartient exclusivement au CSSDHR. Cette règle ne s'applique pas aux contenus publiés dans le cadre de travaux universitaires.

Aucun équipement personnel ne doit être utilisé ni connecté sur le réseau du CSSDHR. Toutefois, à la discrétion de la direction générale, un réseau invité peut être mis à la disposition des personnes utilisatrices pour permettre l'usage de leurs équipements personnels.

Aucune intervention technique ne peut être effectuée sur du matériel ne relevant pas de la propriété du CSSDHR.

En cas d'absence, la personne employée du CSSDHR peut être tenue de remettre l'ensemble des actifs informationnels en sa possession à la direction de son unité administrative, notamment afin d'en permettre le prêt à la personne désignée pour assurer son remplacement.

7.13 Utilisation d'équipement personnel à des fins professionnelles

Les personnes utilisatrices peuvent, à titre de privilège et non de droit, utiliser leur équipement personnel pour accéder aux ressources informationnelles du CSSDHR. Cette utilisation doit être conforme à la présente politique et peut être soumise à des restrictions. Ces restrictions peuvent être mises en place sans préavis, selon les besoins organisationnels ou les impératifs de sécurité.



7.14 Partage de contenu avec d'autres organismes publics

Le partage de contenu appartenant au CSSDHR avec un autre organisme public est permis uniquement avec l'autorisation explicite et écrite de la direction de l'unité administrative concernée. Ce contenu ne doit en aucun cas contenir de renseignements personnels.

7.15 Prévention

La sécurité de l'information repose notamment sur l'adoption de comportements sécuritaires et sur la responsabilisation individuelle.

À cet égard, les personnes utilisatrices du CSSDHR doivent être sensibilisées :

- à la sécurité de l'information et des systèmes d'information du CSSDHR ;
- aux conséquences potentielles d'une atteinte à la sécurité des ressources informationnelles ;
- à leur rôle et à leurs responsabilités en matière de sécurité de l'information.

Le CAIPRPSI est responsable d'informer, de sensibiliser et de former les personnes utilisatrices sur la sécurité des ressources informationnelles, les conséquences d'une atteinte à la sécurité de ces ressources ainsi que sur leur rôle et obligations en matière de sécurité de l'information. Les gestionnaires doivent s'assurer que les membres de leur équipe participent aux formations.

La personne utilisatrice a l'obligation de prendre part aux activités de sensibilisation et de formation. Le non-respect de cette obligation peut entraîner des mesures supplémentaires, comme le renforcement des exigences d'authentification ou la révocation des accès aux ressources informationnelles.

7.16 Surveillance

Le CSSDHR a l'obligation de mettre en place une surveillance appropriée des activités liées à l'utilisation des ressources informationnelles afin d'en assurer une utilisation conforme à la présente politique.

Les ressources informationnelles du CSSDHR doivent être accessibles en tout temps, à la demande des gestionnaires des unités administratives, conformément à la section 6.9 de la présente politique et aux obligations de confidentialité liées aux ordres professionnels.

Des mécanismes de filtrage sont également mis en place afin de limiter l'accès à du contenu inapproprié. D'autres outils de contrôle permettent d'analyser l'utilisation des ressources informationnelles du CSSDHR, la présence de logiciels malveillants dans les courriels ainsi que les tentatives de vol ou de fuite d'information. Malgré ces mesures, la vigilance individuelle demeure essentielle. Chaque personne utilisatrice doit adopter des comportements sécuritaires et responsables.

Le CSSDHR se réserve le droit de bloquer l'accès à certains outils organisationnels, si une utilisation est jugée susceptible de compromettre la sécurité, l'intégrité ou la protection des renseignements personnels.

7.17 Téléphone cellulaire

Le CSSDHR peut fournir un téléphone cellulaire aux membres du personnel dont les fonctions le justifient. Lors du départ d'une personne utilisatrice, celle-ci peut conserver son numéro de téléphone professionnel.

Toute personne utilisatrice souhaitant accéder aux ressources informationnelles du CSSDHR à partir de son appareil mobile personnel doit préalablement accepter les conditions d'utilisation en vigueur.



7.18 Télétravail

Le STI met à la disposition du personnel du CSSDHR des ressources informationnelles permettant la réalisation de ses tâches en télétravail. L'utilisation de ces ressources est autorisée uniquement sur le territoire du Québec, sauf en cas de dérogation.

7.19 Vie privée

L'utilisation des ressources informationnelles du CSSDHR est réservée à des fins strictement professionnelles. La direction d'une unité administrative peut demander la réalisation d'une enquête, lorsqu'elle dispose de motifs raisonnables et sérieux. Les situations suivantes peuvent justifier l'exercice des pouvoirs d'enquête et de surveillance : la protection de la santé et de la sécurité du personnel;

- la protection de la clientèle ;
- le respect des obligations en matière de relations du travail (notamment la prévention du harcèlement) ;
- la prévention d'actes criminels ;
- la prévention de fraudes ;
- le contrôle de la qualité du travail ;
- l'intégrité et la sécurité de l'infrastructure informatique ;
- la protection des renseignements personnels et confidentiels détenus par l'organisation.

8. ENTRÉE EN VIGUEUR ET MISE À JOUR

La présente politique entre en vigueur le 1^{er} juillet 2026.

Section 4 - Historique du document

Approbation par	Date de l'adoption	Date d'entrée en vigueur	Dépôt sur l'intranet	Commentaires
CA	2025-12-09	2026-07-01	2025-12-16	

Section 5 - Étapes de validation de la dernière version du document

	Nom	Date
Rédaction	Geneviève Baillargeon	Mai 2025
Collaboration		
Révision légale		
Révision linguistique	Natasha Galloy	12 septembre 2025
Mise en page	Jessica Thibert	10 septembre 2025

Section 6 - Personnes ou instances consultées

- | | |
|--|---|
| <input checked="" type="checkbox"/> Conseil d'administration | <input checked="" type="checkbox"/> Direction – Service des ressources humaines |
| <input checked="" type="checkbox"/> Syndicat du personnel de soutien des Hautes-Rivières | <input checked="" type="checkbox"/> Direction – Service des ressources financières |
| <input checked="" type="checkbox"/> Syndicat de l'enseignement du Haut-Richelieu | <input checked="" type="checkbox"/> Direction – Service des ressources matérielles |
| <input checked="" type="checkbox"/> Syndicat des professionnelles et professionnels de la Montérégie | <input checked="" type="checkbox"/> Direction – Service des ressources éducatives aux jeunes |
| <input checked="" type="checkbox"/> Association des directrices et des directeurs d'établissement d'enseignement de Champlain (ADEC) | <input checked="" type="checkbox"/> Direction – Services éducatifs en FGA |
| <input checked="" type="checkbox"/> Association québécoise des cadres scolaires (AQCS) | <input checked="" type="checkbox"/> Direction – Services éducatifs en FP |
| <input type="checkbox"/> Comité de répartition des ressources (CRR) | <input checked="" type="checkbox"/> Direction – Services complémentaires et adaptation scolaire |
| <input checked="" type="checkbox"/> Comité consultatif de gestion (CCG) | <input checked="" type="checkbox"/> Direction – Service de l'organisation scolaire et du transport scolaire |
| <input type="checkbox"/> Comité de parents | <input checked="" type="checkbox"/> Direction – Service des technologies de l'information |
| <input checked="" type="checkbox"/> Direction générale | <input type="checkbox"/> Partenaires |
| <input checked="" type="checkbox"/> Secrétariat général | <input checked="" type="checkbox"/> Autre : Comité de gouvernance et d'éthique |
| <input checked="" type="checkbox"/> Direction – Service des communications | |