Centre
de services scolaire
de Kamouraska–
Rivière-du-Loup
Québec

POLITIQUE
CODE : RI-POL-0702
EEV : 2025-04-08

POLITIQUE DE LA SÉCURITÉ DE L'INFORMATION

TABLE DES MATIÈRES

1 PRÉAMBULE

La Politique de la sécurité de l'information vise à protéger les informations numériques et physiques du Centre de services scolaire de Kamouraska–Rivière-du-Loup (CSSKRDL). Cela inclut les données personnelles des élèves, du personnel et des partenaires externes, ainsi que les informations stratégiques nécessaires à l'administration.

L'objectif est de garantir que les informations restent accessibles et sécurisées tout au long de leur utilisation ou de leur cycle de vie.

La mise en place de cette politique s'inscrit dans le cadre des lois et directives gouvernementales sur la gestion et la sécurité de l'information (mars 2020 – décembre 2021), qui imposent aux organismes publics de créer et maintenir des politiques de cybersécurité.

2 OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du CSSKRDL à s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information, quels que soient son support ou ses moyens de communication. Plus précisément, le CSSKRDL doit veiller à :

- assurer la disponibilité de l'information de manière qu'elle soit accessible en temps voulu et de la façon requise aux personnes autorisées par le CSSKRDL;
- assurer l'intégrité de l'information afin qu'elle ne soit ni altérée ni détruite d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- assurer la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seuls ayants droit, particulièrement s'il s'agit de renseignements personnels ou sensibles;
- assurer une utilisation sécuritaire et appropriée des actifs informationnels du CSSKRDL au sens large du terme.

Par conséquent, le CSSKRDL met en place cette politique dans le but d'orienter et de déterminer sa vision de la sécurité de l'information.

Cette politique renforcera les systèmes de contrôles internes en offrant une assurance raisonnable de conformité à l'égard des lois et directives gouvernementales, ainsi qu'aux autres besoins du CSSKRDL en matière d'atténuation des risques associés à la protection de l'information.

3 CADRE LÉGAL

Le Centre de services scolaire de Kamouraska–Rivière-du-Loup (CSSKRDL), en tant qu'organisme public, est soumis à un ensemble de lois, de directives et de règlements émis par le gouvernement du Québec. La Politique de la sécurité de l'information du CSSKRDL s'inscrit dans ce cadre légal et prend appui spécifiquement sur ceux en matière de protection de l'information et de cybersécurité. Les lois et règlements auxquels nous sommes soumis seront détaillés en annexe pour consultation. (Voir Annexe A TBD)

4 CHAMP D'APPLICATION

Cette politique s'applique à toutes les personnes qui utilisent ou accèdent aux informations et actifs informationnels du Centre de services scolaire de Kamouraska–Rivière-du-Loup. Cela inclut :

- le personnel, quel que soit leur statut;
- les élèves, étudiants, partenaires, consultants, invités et fournisseurs;
- toute autre personne autorisée par le CSSKRDL.

Ces utilisateurs doivent respecter les lois et règlements en vigueur.

Les informations concernées par cette politique incluent toutes les données détenues par le CSSKRDL, qu'elles soient stockées par le CSSKRDL ou par un tiers. Cela englobe à la fois les supports numériques et papier, ainsi que tous les systèmes informatiques permettant d'accéder aux informations du CSSKRDL.

5 PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions du CSSKRDL en matière de sécurité de l'information sont les suivants :

- Bien connaître l'information à protéger, la classer, et désigner les responsables de sa sécurité;
- Adopter une approche de gestion des risques pour garantir la sécurité tout au long du cycle de vie de l'information;
- Trouver un équilibre entre l'accès aux outils de travail et la protection des données;
- Réévaluer régulièrement les risques et appliquer des mesures préventives pour éviter tout usage abusif;
- Identifier et réduire les risques qui menacent les informations ou systèmes du CSSKRDL;
- Partager les bonnes pratiques en sécurité de l'information avec les autres organismes de l'éducation et du secteur public;
- S'assurer que chaque utilisateur est responsable de la sécurité de l'information;
- Limiter l'accès à l'information nécessaire à chaque employé pour accomplir ses tâches;
- Adapter les mesures de protection à la valeur de l'information et aux risques associés;
- Mettre en place et actualiser un plan de reprise informatique en cas d'incident ou de sinistre.

6 DISPOSITIONS GÉNÉRALES ET PARTICULIÈRES D'APPLICATION

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être remises en question de manière périodique dans le but de tenir compte non seulement des changements juridiques, organisationnels, technologiques, physiques et environnementaux, mais aussi de l'évolution des menaces et des risques.

La Politique de la sécurité de l'information du CSSKRDL s'articule autour de trois axes fondamentaux de gestion en matière de sécurité de l'information. Ces axes sont :

- la gestion des identités et des accès;
- la gestion des risques;
- la gestion des incidents.

6.1 GESTION DES IDENTITÉS ET DES ACCÈS

La gestion des accès doit être encadrée et contrôlée pour que seules les personnes autorisées et uniquement dans les limites de leur fonction aient accès aux informations sensibles du CSSKRDL. Ces mesures basées sur le principe du moindre privilège protègent l'intégrité, la confidentialité et les renseignements personnels de l'organisation.

L'efficacité des mesures de sécurité repose sur une attribution claire des responsabilités et sur l'obligation de chaque membre du personnel de rendre compte selon sa fonction. Tout incident de sécurité doit être signalé et il faut informer les parties prenantes pertinentes, le tout suivi d'une analyse post-incident pour en identifier les causes profondes. Un plan de reprise est mis en place et testé régulièrement afin d'assurer une gestion rapide et efficace des incidents, conformément aux obligations légales et aux meilleures pratiques. Des contrôles internes réguliers sont effectués pour vérifier que les procédures de notification sont conformes aux exigences légales, et une documentation détaillée est conservée pour chaque incident afin de démontrer la transparence et la conformité en cas d'audit.

6.2 GESTION DES RISQUES

Dans le cadre de son engagement en matière de sécurité de l'information, le CSSKRDL procède à une évaluation des risques pour identifier, analyser et traiter les menaces susceptibles de compromettre la confidentialité, l'intégrité et la disponibilité des informations. Cette évaluation permet de déterminer les menaces, d'évaluer leur impact potentiel, et de définir des stratégies de traitement telles que la réduction, le transfert, l'acceptation ou l'élimination des risques identifiés.

La gestion des risques est assurée par le comité de sécurité, il a pour action :

- d'effectuer les analyses de risques nécessaires à la saine gestion de la sécurité de l'information;
- de mettre en place des mesures de contrôle afin de protéger toute ressource informationnelle contre les accès non autorisés. Ces mesures doivent tenir compte de la nécessité de préserver la confidentialité et l'intégrité de l'information;
- d'établir les normes applicables au CSSKRDL afin d'assurer la sécurité de l'information.

6.3 GESTION DES INCIDENTS

Bien que des mesures d'atténuation des risques soient déployées, il faut que le CSSKRDL soit en mesure de faire face à un incident ayant des impacts sur ses services de mission.

Le CSSKRDL déploie ainsi des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, le CSSKRDL met en place de façon proactive les mesures suivantes :

- Rechercher, corriger et réduire les vulnérabilités de l'organisation face aux menaces en matière de sécurité de l'information en appliquant les bonnes pratiques en cette matière;
- Gérer adéquatement les incidents en suivant un processus structuré comprenant les phases suivantes :
  - détection de l'incident;
  - analyse pour évaluer l'impact et la gravité;
  - confinement afin de limiter la propagation;
  - éradication des causes profondes de l'incident;
  - récupération pour restaurer les services et opérations.

  Si nécessaire, le Comité de la sécurité de l'information (CSI – réf. 10.3) est mobilisé pour coordonner la réponse, sous l'approbation du CSIO (réf. 10.4).

- Mettre en place des mesures correctives lors d'un incident afin de rétablir les services affectés et éviter les impacts sur les utilisatrices et utilisateurs.

Les incidents de sécurité de l'information d'importance gouvernementale doivent être rapportés au Centre opérationnel en cyberdéfense (COCD) du ministère de l'Éducation, en conformité avec les directives de la DGSI et la politique gouvernementale en matière de cybersécurité.

Exercer ses pouvoirs et ses prérogatives à l'égard de tout incident relié à une utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

7 RÔLES ET RESPONSABILITÉS

La sécurité de l'information repose sur une répartition claire des rôles et des responsabilités au sein du CSSKRDL. Cette politique confie la gestion de la sécurité de l'information du CSSKRDL à des groupes (instances, comités) et des personnes précises en fonction de leurs rôles.

7.1 Conseil d'administration

Le conseil d'administration adopte la politique de sécurité de l'information et ses futures mises à jour.

7.2 Direction générale

La Direction générale est responsable de la sécurité de l'information et veille à l'application de la politique. Elle :

- s'assure du respect des lois et règlements en vigueur;
- supervise le chef de la sécurité de l'information (CSIO);
- désigne les personnes responsables (CSIO et COMSI);

- autorise des mesures pour faciliter la mise en œuvre de la politique;
- permet au CSIO d'enquêter en cas de non-respect de la politique.

7.3 Comité de la sécurité de l'information (CSI)

Ce comité, sous la direction du CSIO, planifie les stratégies en cas d'incidents de sécurité. Il se réunit pour gérer les crises et activer le Plan de reprise informatique (PRI) si nécessaire.

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

Le CSIO, désigné par la direction générale, applique la politique et gère les risques liés à la sécurité de l'information. Il :

- tient à jour les registres des infractions à la politique;
- participe à l'élaboration et à la mise en œuvre des mesures de sécurité.

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

Le COMSI, nommé par la direction générale, soutient le CSIO dans la gestion des incidents de sécurité et des risques. Il est le point de contact avec le Centre gouvernemental de cyberdéfense.

7.6 Service des ressources informatiques (SRI)

Le service des ressources informatiques (SRI) gère la sécurité dans les systèmes d'information. Il :

- applique et met à jour les mesures de sécurité;
- participe à l'élaboration de la politique de la sécurité de l'information;
- surveille les nouvelles menaces et adopte des pratiques en cybersécurité.

7.7 Directions d'établissements et de services

Les directions assurent l'application de la politique dans leur unité. Elles :

- diffusent la politique auprès du personnel;
- s'assurent du respect des mesures de sécurité;
- signalent tout incident de sécurité.

7.8 Responsable d'actifs informationnels

Les responsables des actifs s'assurent de la sécurité des informations qu'ils gèrent. Ils :

- sensibilisent les utilisateurs à leurs obligations;
- signalent tout problème lié à la sécurité des informations au CSIO ou à la direction.

7.9 Responsable de la gestion documentaire (Secrétariat général)

Le Secrétariat général s'assure que les systèmes informatiques respectent les normes de sécurité. Il :

- classe et catégorise les informations en fonction de leur sensibilité;
- préserve le patrimoine informationnel et respecte les lois en vigueur.

7.10 Responsable de l'accès à l'information et à la protection des renseignements personnels

Cette personne veille au respect des lois sur l'accès à l'information et la protection des données personnelles. Elle applique la *Loi sur la protection des renseignements personnels*.

7.11 Utilisateurs

Tous les utilisateurs des actifs informationnels du CSSKRDL sont responsables de leur sécurité. Ils doivent :

- respecter la politique et les procédures en matière de sécurité;
- utiliser les informations uniquement dans le cadre de leurs tâches;
- signaler tout incident de sécurité.
-

Les fournisseurs externes et ses employés doivent aussi respecter cette politique.

8 FORMATION ET SENSIBILISATION

Pour s'assurer que les utilisateurs connaissent la sécurité de l'information, le CSSKRDL effectue :

- des formations abordant les meilleures pratiques en matière de sécurité de l'information, les politiques, directives, procédures et les menaces pertinentes pour l'organisation. Ces formations sont obligatoires et destinées à tous les employés;
- des campagnes de simulations d'attaques (comme des tests d'hameçonnage) sont effectuées pour évaluer et renforcer la vigilance des employés.

9 CONFORMITÉ ET AUDIT

- **CONFORMITÉ RÉGLEMENTAIRE :** Le CSSKRDL reconnait l'importance de se conformer aux exigences légales et normatives en matière de sécurité de l'information afin de protéger la confidentialité, l'intégrité et la disponibilité de ces informations. Le CSSKRDL se conforme à toutes les lois et réglementations gouvernementales applicables.

- **AUDIT ET SUIVI :** Dans le cadre de son engagement à maintenir un haut niveau de sécurité de l'information, des audits internes sont réalisés. Ces audits permettent de :
  - **vérifier la conformité des processus;**

- **détecter les points d'amélioration.**

Le CSSKRDL met un plan d'action pour corriger les non-conformités détectées et mettre en place les améliorations nécessaires. Les actions correctives sont ensuite suivies et réévaluées lors des audits suivants afin d'assurer leur efficacité et de maintenir la conformité avec les exigences gouvernementales en matière de sécurité de l'information.

10 SANCTIONS

- Tout membre de la communauté scolaire qui contrevient au cadre légal, à la présente Politique de la sécurité de l'information, s'expose à des sanctions selon la nature, la gravité et les conséquences de la contravention, en vertu de la loi ou des règles disciplinaires applicables.
- De même, toute contravention à la politique, qu'elle soit perpétrée par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au CSSKRDL ou en vertu des dispositions de la législation provinciale ou fédérale applicable en la matière.

11 MISE À JOUR DE LA POLITIQUE

Le chef de la sécurité de l'information organisationnelle (CSIO) assure la diffusion, la mise en œuvre et la mise à jour de la présente politique sous l'autorité de la Direction générale.

Afin d'assurer son adéquation aux besoins de sécurité du CSSKRDL et s'ajuster aux nouvelles pratiques et technologies utilisées, la présente politique est révisée lors de tout changement majeur de l'environnement interne ou externe qui pourrait l'affecter.

12 ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration, soit le 2025-04-08.

13 GLOSSAIRE

Actif informationnel (AI) : Une information, une banque d'information, un système ou un support d'information, un document, une technologie de l'information, une installation ou un ensemble de ces éléments acquis ou constitué par le CSSKRDL habituellement accessible ou utilisable avec un dispositif des technologies de l'information (logiciels, progiciels, didacticiels, banques de données et d'informations textuelles, sonores, symboliques ou visuelles placées dans un équipement ou sur un média informatique, système de courrier électronique et système de messagerie vocale). Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

CGGSI : Cadre gouvernemental de gestion de la sécurité de l'information, version 2022.

Catégorisation : Processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant le degré de sensibilité de cette information et, conséquemment, le niveau de protection à lui accorder en matière de disponibilité, d'intégrité et de confidentialité.

COCD : Centre opérationnel de cyberdéfense du ministère de l'Éducation. Les centres opérationnels des différents ministères et organismes publics sont supervisés par le Centre gouvernemental de cyberdéfense (CGCD).

Confidentialité : Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées, les ayants droit.

COMSI : Coordonnateur organisationnel des mesures de sécurité de l'information. Cette personne assume principalement les mêmes responsabilités que le CSGI dans la version précédente du cadre gouvernemental de gestion en sécurité de l'information.

CSIO : Chef de la sécurité de l'information organisationnelle. Il remplace le Responsable de la sécurité de l'information (RSI) dans la version précédente de la DGSI.

Cycle de vie de l'information : Ensemble des étapes que franchit une information, 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 du CSSKRDL.

CSSKRDL : Centre de services scolaire de Kamouraska–Rivière-du-Loup.

DGSI : Directive gouvernementale sur la sécurité de l'information (mise à jour déc. 2021).

Responsable d'actif informationnel : Membre du personnel d'encadrement détenant la plus haute autorité au sein d'une unité pédagogique ou administrative et dont le rôle consiste notamment, du point de vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de cette unité.

Disponibilité : Propriété d'une information d'être accessible en temps voulu et de la manière requise par une personne autorisée.

Incident : Un événement qui porte atteinte ou qui est susceptible de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information, ou plus généralement à la sécurité des systèmes d'information, notamment une interruption des services ou une réduction de leur qualité.

Intégrité : Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

Plan de reprise : Plan de relève mis en œuvre lorsqu'il y a détérioration ou destruction d'actifs informationnels consécutive à un incident exigeant le transfert on non, de l'exploitation dans un autre lieu ou une autre salle des serveurs. Le plan de relève décrit les procédures visant à assurer, dans des conditions de continuité adaptées à l'urgence de la situation.

SRI : Service des ressources informatiques.

Utilisateur : Tout le personnel, toute personne physique ou morale qui, à titre d'employé, d'étudiant, de consultant, de partenaire, de fournisseur ou d'invité, utilise les actifs informationnels du CSSKRDL.

ANNEXE A

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (**Référence :** RLRQ, c. G -1.03)

Politique gouvernementale de cybersécurité
Date : Mars 2020

Directive gouvernementale sur la sécurité de l'information (DGSI)
Date : Décembre 2021
Référence : Article 12 de la Directive gouvernementale sur la sécurité de l'information

La Charte des droits et libertés de la personne (LRQ, chapitre C-12)

Le Code civil du Québec (LQ, 1991, chapitre 64)

La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics

La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI – LRQ, chapitre G-1.03)

Le Cadre gouvernemental de gestion de la sécurité de l'information (CGGSI)

La Directive gouvernementale sur la sécurité de l'information (DGSI, déc. 2021)

La *Loi concernant le cadre juridique des technologies de l'information* (LRQ, chapitre C-1.1)

La Politique gouvernementale de cybersécurité (SCT, 2020)

La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, chapitre A-2.1)

La *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (LRQ, chapitre 25)

La *Loi sur les archives* (LRQ, chapitre A-21.1)

Le Code criminel (LRC, 1985, chapitre C-46)

Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels

La *Loi sur l'instruction publique* (LRQ, chap. 1-13.3)

La *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42)

Politique d'utilisation des technologies de l'information et des communications (TI-POL-0701)