Centre
de services scolaire
des Phares
Québec

A133-38-1

CADRE DE GESTION

TITRE :	Cadre de gestion de la sécurité de l'information
RESPONSABLE DE L'APPLICATION :	Service des ressources informationnelles
FONDEMENT :	Politique relative à la sécurité de l'information
ADOPTION :	2026-02-24
ENTRÉE EN VIGUEUR :	2026-02-25
RÉVISION :	N/A
DOCUMENT REMPLACÉ :	N/A

Table des matières

1. PRÉAMBULE

Le présent Cadre de gestion de la sécurité (Cadre de gestion) est adopté en vertu de l'article 12 de la *Directive gouvernementale sur la sécurité de l'information* (DGSI) découlant de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI) qui exigent des Centres de services scolaire de répondre à des obligations en matière de sécurité de l'information en leur qualité d'organismes publics. Ainsi, la DGSI oblige le Centre de services scolaire des Phares (CSS des Phares) à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'un Cadre de gestion de la sécurité de l'information.

2. OBJET

Le présent Cadre de gestion a pour objet de compléter les orientations de la Politique relative à la sécurité de l'information du CSS des Phares et de renforcer la gouvernance de la sécurité de l'information par la mise en place d'une structure organisationnelle et fonctionnelle en matière de sécurité de l'information.

Ce Cadre de gestion identifie les rôles et responsabilités des personnes et des comités impliqués permettant au CSS des Phares de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information.

3. DESTINATAIRES

Le présent Cadre de gestion s'adresse aux personnes utilisatrices des actifs informationnels du CSS des Phares. Les actifs informationnels visés sont ceux que le CSS des Phares détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers.

4. FONDEMENTS

Le Cadre de gestion s'appuie principalement sur les encadrements suivants :

- La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03) ;
- La *Loi concernant le cadre juridique des technologies de l'information* (RLRQ, c. C-1.1) ;
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, c. A-2.1) ;
- La *Loi sur le droit d'auteur* (LRC, c. C -42) ;
- La *Loi sur les archives* (RLRQ, c. A-21.1) ;
- La *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* ;
- La *Politique gouvernementale de cybersécurité* ;
- Le *Cadre gouvernemental de gestion de la sécurité de l'information* ;
- La *Directive gouvernementale sur la sécurité de l'information* ;

- Les politiques, règlements et directives du CSS des Phares dont notamment la *Politique d'utilisation des technologies de l'information et des médias sociaux* ;
- Les conventions collectives et règlements du personnel cadre et hors cadre ;
- Le *Guide d'élaboration d'un cadre de gestion de la sécurité de l'information*.

5. DÉFINITIONS

Dans ce Cadre de gestion, les expressions et les termes suivants signifient :

5.1. Actif informationnel

Tout actif sur lequel repose de l'information sous forme numérique ou non numérique. Par exemple, une base de données sur un serveur ou un document papier dans un classeur.

Est également considéré comme un actif informationnel tout système d'information, composante d'une infrastructure technologique, banque d'information, support d'information numérique (clé USB, disque compact, bande de copie, disque amovible, etc.), document en format papier ou un ensemble de ces éléments acquis ou constitué par le CSS des Phares qui peut être accessible avec un dispositif des technologies de l'information ou accessible par un dispositif plus traditionnel tels une filière ou un classeur. Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue.

5.2.Événement de sécurité

Toute forme d'atteinte, présente ou appréhendée, telles 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 organisme public ou d'une personne agissant pour ce dernier.

5.3.Incident de confidentialité

On entend par « incident de confidentialité » :

a) L'accès non autorisé par la Loi sur l'accès à un renseignement personnel ;

b) L'utilisation non autorisée par la loi d'un renseignement personnel ;

c) La communication non autorisée par la loi d'un renseignement personnel ;

d) La perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement.

5.4.Personne utilisatrice

Personne physique ou morale qui, à titre de personne employée, de personne consultante, de personne bénévole, de partenaire, de fournisseur, d'élève ou de personne du public, utilise un actif informationnel du CSS des Phares ou y a accès, ainsi que toute personne dûment autorisée à y avoir accès.

5.5. Système d'information

Système constitué des ressources humaines (le personnel), des ressources matérielles (l'équipement) et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents pour le fonctionnement d'une entreprise ou d'une organisation.

6. ORGANISATION FONCTIONNELLE DE LA SÉCURITÉ DE L'INFORMATION

La structure organisationnelle du CSS des Phares en matière de sécurité de l'information est présentée par un organigramme présenté à l'Annexe 1. Cet organigramme présente les personnes intervenantes et les comités gravitants autour de la sécurité de l'information.

7. RÔLES ET RESPONSABILITÉS

Les responsabilités en matière de sécurité de l'information sont attribuées aux intervenants suivants.

7.1. Principaux intervenants

Les rôles et les responsabilités attribués aux principaux intervenants en matière de sécurité de l'information sont définis dans la Politique relative à la sécurité de l'information du CSS des Phares.

7.2. Autres intervenants

7.2.1. Personne détentrice de l'information

La personne détentrice de l'information désignée par la direction générale ou le chef de la sécurité de l'information organisationnelle (CSIO) est une personne cadre détenant l'autorité au sein d'un service ou d'un établissement et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité du service ou de l'établissement. Il peut donc y avoir plusieurs responsables d'actifs informationnels dans un centre de services scolaire. À cette fin, elle :

a) Maintient les informations relatives aux actifs informationnels sous sa responsabilité ;

b) Informe le personnel relevant de son autorité et les tiers avec lesquels transige son service ou son établissement de la Politique relative à la sécurité de l'information et des dispositions du Cadre de gestion dans le but de les sensibiliser à la nécessité de s'y conformer ;

c) Collabore activement à la catégorisation de l'information du service ou de l'établissement sous sa responsabilité, de même qu'à l'analyse de risques ;

d) Agit comme personne responsable des analyses de risques découlant de l'information qu'elle détient et s'assure de la prise en charge des risques ;

e) Prend en charge la préparation et la mise en place d'un plan de continuité des activités ciblées pour les informations qu'elle détient ;

f) Voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel autorisé en conformité avec la Politique relative à la sécurité de l'information et de tout autre élément du Cadre de gestion ;

g) Rapporte au Service des ressources informationnelles toute menace ou tout événement afférent à la sécurité de l'information ;

h) Collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un événement de sécurité ainsi qu'à toute opération de vérification de la sécurité de l'information.

Rapporte au CSIO tout problème lié à l'application de la Politique relative à la sécurité de l'information et du présent Cadre de gestion, dont toute contravention réelle ou apparente d'une personne membre du personnel, d'une personne consultante, d'un partenaire, d'un fournisseur, d'un élève ou du public.

7.2.2. Pilote de système d'information

Cette personne désignée par la personne détentrice de l'information est responsable de mettre en application le Cadre de gestion, les directives et les procédures applicables aux systèmes d'information sous sa gestion. À cette fin, elle :

a) Assure le respect des règles de sécurité par les personnes utilisatrices des systèmes d'information ;

b) Gère les accès logiques aux systèmes d'information et s'assure du respect des règles d'accès par les personnes utilisatrices ;

c) Sensibilise les personnes utilisatrices sur les responsabilités des personnes utilisatrices quant à l'utilisation des systèmes d'information ;

d) Assiste et supporte les personnes utilisatrices avec les systèmes d'information.

7.2.3. Analyste en sécurité

L'analyste en sécurité est responsable de la surveillance, de l'évaluation et de l'amélioration continue de la posture de sécurité du CSS des Phares. Il contribue à la mise en œuvre des mesures de protection des actifs informationnels conformément aux politiques, procédures et directives en vigueur.

7.2.4. Service des ressources informationnelles

En matière de sécurité de l'information, le Service des ressources informationnelles s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que dans la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels il intervient. À ce rôle :

a) Il participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre et à l'anticipation de toute menace en matière de

sécurité des systèmes d'information faisant appel aux technologies de l'information ;

b) Il applique des mesures de réaction appropriées à toute menace ou à tout événement de sécurité, comme l'interruption ou la révocation temporaire — lorsque les circonstances l'exigent — des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause ;

c) Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes au présent Cadre de gestion et à la Politique relative à la sécurité de l'information autorisée par la direction générale.

7.2.5. Service des ressources matérielles

Le service des ressources matérielles participe, avec le CSIO, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du CSS des Phares.

7.2.6. Service des ressources humaines

En matière de sécurité de l'information, le Service des ressources humaines s'assure que toute nouvelle personne employée du CSS des Phares est informée et sensibilisée à la Politique relative à la sécurité de l'information et au Cadre de gestion. Il s'assure également que la nouvelle personne employée ait signé son engagement au respect de la Politique et du Cadre de gestion.

7.2.7. Personnes cadres

En plus d'agir comme personne détentrice de l'information qui est sous leur responsabilité, les personnes cadres ont pour mandat d'assurer la mise en œuvre de la Politique relative à la sécurité de l'information et du Cadre de gestion au sein de leur service ou de leur établissement. À ce titre, les personnes cadres :

a) Informe le personnel relevant de son autorité et les tiers avec lesquels transige son service ou son établissement de la Politique relative à la sécurité de l'information et des dispositions du Cadre de gestion dans le but de les sensibiliser à la nécessité de s'y conformer ;

b) Voit à la protection de l'information et des systèmes d'information sous sa responsabilité et veille à ce que ceux-ci soient utilisés par le personnel autorisé en conformité avec la Politique relative à la sécurité de l'information et de tout autre élément du Cadre de gestion.

8. LES COMITÉS

8.1. Comité de sécurité de l'information

Le Comité de sécurité de l'information a comme objectif d'aider le CSIO à mettre en place des actions pouvant être nécessaires pour assurer la protection du CSS des Phares et être conforme à la réglementation. C'est un comité qui est tactique et opérationnel.

Ce Comité est chargé de mettre en place les plans d'action et les bilans de sécurité de l'information, les activités de sensibilisation et de formation ainsi que toute proposition d'action en matière de sécurité de l'information. C'est aussi un forum d'échange entre les parties prenantes ou d'observations de l'évolution des projets en sécurité de l'information.

Le Comité est formé des membres du comité d'accès à l'information et de l'analyste en sécurité. Il peut également s'adjoindre des participants complémentaires en fonction de la situation.

8.2. Comité de crise et de continuité des services

Le Comité de crise et de continuité des services est sous la responsabilité de la direction générale. Il peut être mis en place en cas d'événement de sécurité critique ou à portée gouvernementale, lorsque la situation n'a pu être rétablie à la normale suivant les actions posées par le Comité de gestion des événements de sécurité.

Son rôle consiste à supporter le Comité de gestion des événements de sécurité, recevoir ses recommandations et prendre les décisions de manière à assurer la continuité des services ou le rétablissement rapide des activités. À ce titre, il doit :

a) Assurer les communications envers les personnes utilisatrices et les médias ;

b) Entériner les décisions et approbations découlant de l'application des recommandations qui peuvent lui être remontées ;

c) Déployer les plans de contingence ou de continuité des activités du CSS des Phares, si la situation le requiert.

Ce Comité est composé de la Direction générale, de la personne responsable de l'accès et de la protection des renseignements personnels, du secrétaire général, du CSIO, de la direction des ressources informationnelles, de la personne responsable des communications et de toute personne qui peut avoir un apport en fonction de la situation.

8.3. Comité de gestion des événements de sécurité

Le Comité de gestion des événements de sécurité est un comité de niveau opérationnel sous la direction du CSIO qui se met en place lorsque la situation le requiert à l'occasion d'un événement de sécurité visant un actif informationnel. Il rend compte au Comité de crise et de continuité des services.

Ce Comité doit s'assurer de l'application du plan de gestion des événements et de la réalisation des actions nécessaires afin de limiter la menace, atténuer les impacts et revenir à une situation normale. Il a également comme rôle de suivre l'évolution des

événements, d'assurer la coordination des travaux des personnes intervenantes et de fournir des recommandations au comité de crise et de continuité des services.

Ce Comité regroupe le CSIO, la direction du Service des ressources informationnelles, la personne responsable de l'accès et de la protection des renseignements personnels, le secrétaire général, les deux coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI) de même que les personnes détentrices et pilotes de système d'information ciblés par l'événement. Il peut également s'adjoindre de personnel complémentaire et spécialisé dans certains secteurs ou technologies en mesure d'apporter l'aide nécessaire.

9. ADOPTION ET ENTRÉE EN VIGUEUR

Le présent Cadre de gestion a été adopté par le Conseil d'administration à la séance du 24 février 2026 par la résolution 26-02-24-670 et entre en vigueur le 25 février 2026.

10. ANNEXE

Structure organisationnelle de sécurité de l'information :