Centre
de services scolaire
du Chemin-du-Roy
Québec

CADRE DE GESTION

DE LA SÉCURITÉ DE L'INFORMATION

- Responsable : **Service des technologies de l'information**
- Date d'adoption : **22 mai 2024**
- Date de la dernière révision : **---**
- Numéro de référence : **résolution 87-CA/24-05-22**

1. PRÉAMBULE

Le Cadre de gestion de la sécurité de l'information (ci-après « le cadre ») vient en complément de la Politique sur la sécurité de l'information du Centre de services scolaire du Chemin-du-Roy (ci-après « la politique »). Il est élaboré et mis en œuvre en application de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) et de la Directive sur la sécurité de l'information gouvernementale[1].

2. OBJECTIFS

Le présent cadre a pour objectif d'identifier les responsabilités des différents intervenants en sécurité de l'information afin de permettre au Centre de services scolaire Chemin-du-Roy (ci-après « le Centre de services scolaire ») de s'acquitter pleinement de ses obligations à l'égard de la sécurité de l'information. Il vise également à renforcer la gouvernance de la sécurité de l'information du Centre de services scolaire.

3. CHAMP D'APPLICATION

Le présent cadre s'adresse aux utilisateurs de l'information, c'est-à-dire aux dirigeants du Centre de services scolaire, à son personnel, peu importe son statut, à toute personne physique ou morale, qui à titre d'élève, de parent, de consultant, de partenaire, de fournisseur ou de visiteur, utilise les actifs informationnels du Centre de services scolaire ou y a accès ainsi qu'à toute personne dûment autorisée à y avoir accès.

L'information visée est celle que le Centre de services scolaire détient dans le cadre de ses activités, que sa conservation soit assurée par lui-même ou par un tiers. Les formats de l'information visée sont numériques et non numériques.

4. DIRECTIVES

Le présent cadre prévoit la mise en place de processus formels de sécurité de l'information qui permettent d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

4.1 Gestion des risques

Une catégorisation des actifs informationnels à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger, de déterminer les risques encourus si elle devait être divulguée et d'établir une stratégie appropriée.

Cette gestion des risques en matière d'accès et de protection de l'information s'inscrit dans le cadre global de la gestion des risques du Centre de services scolaire. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*. À ce titre, cette analyse de risques ne porte pas uniquement sur l'information colligée, mais aussi sur l'acquisition, le développement et l'exploitation des

[1] Article 7, alinéa 2

systèmes d'information qui assurent la conservation des renseignements. Le niveau de protection de l'information est établi en fonction :

- De la nature de l'information et de son importance;
- Des probabilités de divulgation involontaire, d'erreur ou de malveillance auxquelles elles sont exposées;
- Des conséquences de cette divulgation;
- Du niveau de risque jugé acceptable par le Centre de services scolaire.

4.2 Gestion des accès

Une gestion des accès informatiques et physiques est élaborée, encadrée et contrôlée pour faire en sorte de protéger la disponibilité, l'intégrité et la confidentialité de l'information

4.3 Gestion des incidents

Le Centre de services scolaire déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires à l'obtention des buts suivants :

- Limiter l'occurrence des incidents en matière de sécurité de l'information;
- Gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés au ministère de l'Éducation du Québec (MEQ) conformément à la Directive sur la sécurité de l'information gouvernementale.

Dans la gestion des incidents, le Centre de services scolaire peut exercer ses pouvoirs à l'égard de toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

Pour chacune des dispositions élaborées ci-dessous, il convient de prévoir un mécanisme de révision à fréquence prédéterminée et de procéder à une mise à jour au besoin.

4.3.1 Gestion des vulnérabilités

Le Centre de services scolaire déploie des mesures pour maintenir à jour son parc informatique afin de maintenir les vulnérabilités des actifs de l'information numérique à son niveau le plus bas possible et diminuer les chances d'une cyberattaque. Une mesure de notification des vulnérabilités venant des fournisseurs est mise en place pour les corriger.

4.3.2 Gestion des copies de sauvegardes

Le Centre de services scolaire élabore une stratégie de copie de sauvegarde pour se prémunir contre une perte de données. Cette procédure inclut la création et la rétention des copies, les alertes d'erreurs lors de la prise de copies et les tests de restauration de ces copies à une fréquence adéquate.

4.3.3 Continuité des affaires

Le Centre de services scolaire élabore un plan de continuité des affaires advenant qu'un incident cause l'arrêt partiel ou complet de la prestation de ses services. Ce plan est mis à l'épreuve à une fréquence adéquate et les écarts sont corrigés.

4.3.4 Protection du périmètre réseau

Le Centre de services scolaire instaure des exercices de test d'intrusion et balayages de vulnérabilités pour identifier les points d'entrée susceptibles de donner un accès inapproprié à des individus ou des programmes malicieux. De plus, un système de prévention et de détection d'intrusion est mis en place pour augmenter le niveau de protection. Aussi, segmenter son réseau permet au Centre de services scolaire de diminuer les chances de propagation d'un virus ou d'une attaque.

4.3.5 Utilisation d'un appareil personnel

Une directive sur l'utilisation d'un appareil personnel (iPad, téléphone intelligent, etc.) est élaborée pour encadrer cette pratique. Les données du Centre de services scolaire doivent être protégées par les mécanismes mis en place. Ainsi, les élèves et les employés qui utilisent un appareil personnel pourront le faire uniquement par un accès « invité ».

Une entente doit être signée entre les parties énumérant leurs responsabilités respectives et qu'advenant le vol ou la perte de l'appareil, le Centre de services scolaire doit procéder à l'effacement de ces données.

4.3.6 Protection des actifs de l'information format non numérique

Le Centre de services scolaire se dote d'une politique de gestion documentaire. La notion d'archivage et de destruction est considérée dans l'élaboration de cette politique. **Cette protection inclut la gestion des accès physiques aux salles, aux imprimantes ou autres endroits qui détiennent des actifs de l'information.**

4.3.7 Gestion des fournisseurs

Le Centre de services scolaire met en place un processus de gestion de ses fournisseurs afin que ceux-ci ne soient pas source d'incidents, de divulgations/pertes de données ou de virus sur son réseau. Pour ce faire, une entente doit être signée avec le fournisseur qui stipule qu'il s'engage à répondre aux exigences, en cybersécurité, du Centre de services scolaire et que le Centre de services scolaire est en droit de voir les résultats des audits faits quant à ce fournisseur. Cette entente doit aussi inclure les objectifs/niveaux de services attendus par ce fournisseur. Les fournisseurs ont accès à l'information sensible du Centre de services scolaire, c'est pourquoi ces derniers s'engagent à respecter la confidentialité en conformité avec les clauses des documents d'appels d'offres.

5. DÉFINITIONS

Actif informationnel : Tout système ou équipement du Centre de services scolaire fourni, pouvant être sa propriété ou loué, permettant le traitement, le transport et l'entreposage de toute forme de communication ou d'information, notamment, les équipements informatiques (poste de travail, ordinateur portable, imprimante, etc.), les réseaux de communication (Internet, réseau local, réseau sans fil, réseau étendu, etc.), les systèmes de téléphonie, les systèmes de vidéosurveillance et de télécommunication, le courrier électronique, les bases de données, les images numérisées, les vidéos, les applications informatiques et les progiciels ainsi que la documentation nécessaire à leur bon fonctionnement. L'actif informationnel inclus aussi toute forme de communication ou d'information inscrite sur support papier, électronique ou autre, produite, transmise ou reçue par une personne utilisatrice dans le cadre des opérations du Centre de services scolaire.

Catégorisation : Le processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant son degré de sensibilité en termes de disponibilité, d'intégrité et de confidentialité et, par conséquemment, le niveau adéquat de protection à lui accorder.

Détenteur : Une personne qui a la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels du centre de services scolaire.

Document : Un ensemble constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcrits sous l'une de ces formes ou en un autre système de symboles. Est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.

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.

Incident de sécurité de l'information à portée gouvernementale : La conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale, nécessitant une intervention concertée au plan gouvernemental.

Information : Un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

Plan de continuité : L'ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité du centre de services scolaire.

Pratique : Savoir ou manière de faire qui, dans une organisation, conduisent aux résultats souhaités et qui sont portés en exemple auprès des paires afin de leur faire partager l'expérience qui leur permettra une amélioration collective.

Procédure : Ensemble des étapes à franchir, des moyens à prendre et des méthodes à suivre dans l'exécution d'une tâche.

Processus : Suite cohérente d'activités et d'opérations d'une organisation traduisant les besoins de la clientèle et des employés dans une logique de création de valeur.

Registre d'incident : Un recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, l'impact, le problème à la source, les mesures prises pour le rétablissement à la normale.

Renseignement personnel : Tout renseignement qui concerne une personne physique et permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins du présent cadre.

Ressources informationnelles : Les actifs informationnels, ainsi que les ressources humaines, matérielles et financières directement affectées à la gestion, à l'acquisition, au développement, à l'entretien, à l'exploitation, à l'accès, à l'utilisation, à la protection, à la conservation et à l'aliénation de ces actifs.

Risque de sécurité de l'information : Le degré d'exposition d'une information ou d'un système d'information à une menace d'interruption ou de réduction de la qualité des services ou d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information et qui peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ou sur l'image du centre de services scolaire.

Risque de sécurité de l'information à portée gouvernementale : Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information gouvernementale et qui peut avoir des conséquences sur la prestation de services à la population, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits fondamentaux à la protection des renseignements personnels qui les concernent et au respect de leur vie privée, sur l'image du gouvernement, ou sur la prestation de services fournie par d'autres organismes publics.

Sécurité de l'information : La protection de l'information et des systèmes d'information contre les risques et les incidents.

Système d'information : L'ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

Technologie de l'information : Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

6. PRINCIPES

Rôles et responsabilités

Les responsabilités en matière de sécurité de l'information au Centre de services scolaire sont attribuées aux intervenants suivants :

6.1 Dirigeant (Conseil d'administration)

Le Conseil d'administration délègue au directeur général le pouvoir de nommer le chef de la sécurité de l'information organisationnelle (CSIO) ainsi que les coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI) du Centre de services scolaire et adopte la *Politique sur la sécurité de l'information* ainsi que toute modification à celle-ci.

6.2 Direction générale

La Direction générale du Centre de services scolaire détermine les mesures visant à favoriser l'application de la *Politique sur la sécurité de l'information* et du présent cadre ainsi que le respect des Lois et règles en matière de sécurité de l'information. Elle détermine les orientations stratégiques et les plans d'action en matière de sécurité de l'information et reçoit les bilans de sécurité de l'information. Elle convient également des directives, des processus et des procédures qui viennent préciser ou soutenir l'application de la politique et du cadre.

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

Le CSIO conseille la Direction générale en ce qui a trait à la détermination des orientations stratégiques et priorités d'intervention en sécurité de l'information pour le Centre de services scolaire. Il a également la responsabilité de les communiquer au personnel du Centre de services scolaire.

Le CSIO assure par ailleurs la coordination des actions en matière de sécurité de l'information des actifs informationnels de l'organisation et la participation des intervenants à la mise en œuvre des processus officiels de gestion. Il veille à la coordination et à la cohérence des actions de la sécurité de l'information menées par les autres acteurs tels que les détenteurs de l'information ainsi que les unités administratives responsables des ressources informationnelles, de l'accès à l'information et de la protection des renseignements personnels, de la gestion documentaire, de la sécurité physique et de l'éthique.

Il met en place et anime le comité pour la sécurité de l'information. Il coordonne l'élaboration et la mise en œuvre d'un programme officiel et continu de formation et de sensibilisation du personnel en matière de sécurité de l'information.

En collaboration avec le ministère et les autres CSIO du réseau de l'éducation, il met en œuvre un processus de veille sur les menaces et vulnérabilités ainsi que sur les bonnes pratiques de sécurité de l'information.

6.4 Coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI)

Les COMSI, au nombre de deux, contribuent à la mise en œuvre des processus officiels de la sécurité de l'information. Ils assurent une veille continue sur les risques, les menaces et les vulnérabilités.

Ils gèrent les incidents de sécurité de l'information à portée gouvernementale. Avec les membres de l'équipe de réponse aux incidents, ils développent, mettent en place et testent le plan de réponse aux incidents de sécurité de l'information.

Les COMSI contribuent aux analyses des risques en sécurité de l'information, à définir les menaces et les situations de vulnérabilité et à mettre en œuvre les solutions appropriées. Ils procèdent à l'autoévaluation de la sécurité des actifs informationnels, notamment par des exercices d'audit de sécurité, des tests d'intrusion pour les systèmes jugés à risque. De plus, ils tiennent à jour les guides portant sur la sécurité opérationnelle des actifs informationnels et des processus et maintiennent une veille continue sur les risques, les menaces et les vulnérabilités.

6.5 Comité sur la sécurité de l'information (jumelé au Comité sur l'accès à l'information)

Le comité sur la sécurité de l'information a pour objectif d'aider le CSIO à mettre en place le cadre de gestion de la sécurité de l'information et autre élément pouvant être nécessaire pour assurer la protection du Centre de services scolaire et être conforme à la réglementation.

C'est aussi un forum d'échange et d'observation de l'évolution du projet en sécurité de l'information.

6.6 Service des technologies de l'information

Le Service des technologies de l'information 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 des systèmes d'information dans lesquels il intervient :

- 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;
- Il applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, par exemple, 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;
- Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes au présent cadre et autorisées par le CSIO.

6.7 Service des ressources matérielles

Le Service des ressources matérielles participe, avec le CSIO et les COMSI à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Centre de services scolaire.

6.8 Service des ressources humaines

En matière de sécurité de l'information, le Service des ressources humaines s'assure que tout nouvel employé, cadre ou hors cadre du Centre de services scolaire, soit avisé de la Politique sur la sécurité de l'information et du présent cadre et s'assure d'obtenir son engagement au respect de la politique.

6.9 Direction de l'unité administrative

En matière de sécurité de l'information, la direction de l'unité administrative, qu'il s'agisse d'un établissement scolaire ou d'un service, veille à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de son unité administrative. À cette fin, elle :

- Voit à la protection de l'information et des systèmes d'information sous sa responsabilité et contribue à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la politique et de tout autre élément du cadre;
- S'assure, en collaboration avec les autres cadres, que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service et voit à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique et tout autre élément du présent cadre;
- Rapporte au CSIO toute menace ou tout incident afférant à la sécurité de l'information en utilisant le formulaire électronique dans Octopus;
- Collabore à la mise en œuvre de toute mesure visant à améliorer la sécurité de l'information ou à remédier à un incident de sécurité de l'information ainsi qu'à toute opération de vérification de la sécurité de l'actif de l'information;
- Rapporte au CSIO tout problème lié à l'application de la politique et du cadre, dont toute contravention réelle ou apparente d'un membre du personnel en ce qui a trait à l'application de ces encadrements.

6.10 Utilisateurs

La responsabilité de la sécurité de l'information incombe à tous les utilisateurs des actifs informationnels du Centre de services scolaire.

Tout utilisateur, y compris les dirigeants, les employés, les élèves, les visiteurs, les mandataires, les partenaires, les fournisseurs et ceux qui agissent pour leur compte, a l'obligation de protéger l'information mise à sa disposition. L'utilisateur a notamment les responsabilités suivantes :

- S'assurer de l'intégrité et de la confidentialité de l'information du Centre de services scolaire;
- Suivre les directives et respecter les consignes qui lui sont présentées;
- Utiliser l'information, quel que soit le support sur lequel elle se trouve, avec discernement, aux seules fins auxquelles elle est destinée et exclusivement selon les droits qui lui sont accordés;
- S'assurer, le moment venu, de la destruction sécuritaire des documents sensibles en conformité des modalités établies par le Centre de services scolaire ;
- Utiliser uniquement l'équipement et les logiciels autorisés;
- Agir avec précaution, notamment en s'abstenant d'utiliser l'information s'il a des doutes sur les règles applicables;
- Respecter les droits de propriété intellectuelle au moment de l'utilisation des produits et des documents;

- Signaler sans tarder à la direction de l'unité administrative toute situation, incident ou anomalie susceptible de compromettre la sécurité des actifs informationnels du Centre de services scolaire;
- Respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger.

De plus, les dirigeants et employés du Centre de services scolaire ont les obligations suivantes :

- Prendre connaissance du présent cadre, de la politique, des directives, des procédures et autres lignes de conduite en découlant;
- Au moment de leur départ, ils doivent remettre les différents accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie mis à leur disposition dans le cadre de l'exercice de leurs fonctions.

Sensibilisation et formation

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les utilisateurs des actifs informationnels du Centre de services scolaire doivent être formés et sensibilisés à la sécurité de l'information, aux menaces existantes, aux conséquences d'une atteinte à la sécurité et à leur rôle et à leurs responsabilités en la matière. À ces fins, des activités de sensibilisation et de formation sont offertes par le Centre de services scolaire.

7. ENTRÉE EN VIGUEUR

Le présent cadre de référence entre en vigueur à compter du 22 mai 2024.

8. MISE À JOUR

Le CSIO est responsable de la diffusion et de la mise à jour du présent cadre, lequel sera révisé périodiquement.

La mise à jour de ce cadre de référence sera effectuée au minimum dans les cinq ans de la date d'entrée en vigueur.