Riverside School Board

Nom de la politique:	Politique relative à la sécurité de l'information
Numéro de la politique :	BXXX-20191217
Date soumise à l'Executif :	1er octobre 2019
Date reçue au Conseil :	15 octobre 2019
Période de la consultation:	18 octobre 2019 – 2 décembre 2019
Date adoptée par le Conseil :	XXX

TABLE DES MATIÈRES

1. CONTEXTE

L'entrée en vigueur de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (LGGRI) (LRQ, Loi 133) et de la Directive sur la sécurité de l'information gouvernementale (DSIG) (une directive du Conseil du trésor du Québec applicable à la commission scolaire) créent des obligations aux établissements scolaires en leur qualité d'organismes publics.

Ainsi, la Directive sur la sécurité de l'information gouvernementale oblige la commission scolaire à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique de sécurité de l'information – dont les principales modalités sont définies dans la directive gouvernementale – en ayant recours, notamment à des 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. Ceci demande que 2 rôles soient comblés au sein de chaque commission scolaire. Tel qu'il est stipulé dans le Guide de nomination, un Responsable de la sécurité de l'information (RSI) et deux (2) Coordonnateurs sectoriels de la gestion des incidents (CSGI) doivent être désignés.

Cette politique permet à la commission scolaire des Trois-Lacs d'accomplir ses missions, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue (dont elle est le gardien). Cette information liée aux ressources humaines, matérielles, technologiques et financières, est accessible sur des formats numériques et non numériques, dont les risques d'atteinte à sa disponibilité, intégrité ou confidentialité peuvent avoir des conséquences liées à :

- La vie, la santé ou le bien-être des personnes;
- L'atteinte à la protection des renseignements personnels et à la vie privée;
- La prestation de services à la population;
- L'image de la commission scolaire et du gouvernement.

2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement de la commission scolaire 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, la commission scolaire doit veiller à :

- La disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- L'intégrité de l'information de manière à ce que celle-ci ne soit ni détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- La confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, surtout si elle constitue des renseignements personnels.

Par conséquent, la commission scolaire met en place cette politique dans le but d'orienter et de déterminer sa vision, qui sera détaillée par le cadre de gestion de la sécurité de l'information de la commission scolaire.

3. CADRE LÉGAL ET ADMINISTRATIF

La politique de sécurité s'inscrit principalement dans un contexte régi par :

- La Charte des droits et libertés de la personne (LRQ, chapitre C-12);
- La loi sur l'instruction publique (L.R.Q. c. I-13.3);
- Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (L.R.Q. c. A-21.1, r.1);
- 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 (LRQ, Loi 133);
- La Loi concernant le cadre juridique des technologies de l'information (LRQ, chapitre C-1.1);
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LRQ, chapitre A-2.1);
- Le Code criminel (LRC, 1985, chapitre C-46);
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (chapitre A-2.1, r. 2);
- La Directive sur la sécurité de l'information gouvernementale;
- La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- La Politique d'utilisation des technologies de l'information, du réseau des télécommunications et des médias sociaux

4. CHAMP D'APPLICATION

La présente politique s'adresse aux utilisateurs de l'information, c'est-à-dire à tout le personnel, à toute personne physique ou morale qui à titre d'employé, de consultant, de partenaire, de fournisseur, d'étudiant ou de public utilise les actifs informationnels de la commission scolaire. Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par la commission scolaire. À cette fin, il doit :

a) Prendre connaissance de la présente politique, des directives, des procédures et autres lignes de conduite en découlant, y adhérer et prendre l'engagement de s'y conformer.

b) Utiliser, dans le cadre des droits d'accès qui lui sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de ses fonctions, les actifs informationnels mis à sa disposition, en se limitant aux fins auxquelles ils sont destinés;

c) Respecter les mesures de sécurité mises en place sur son poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier leur configuration ou les désactiver;

d) Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;

e) Signaler immédiatement à son supérieur tout acte dont il a connaissance, susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels de la commission scolaire.

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

Veuillez vous référer au « Glossaire de la sécurité de l'information » pour une liste détaillée des rôles et des responsabilités.

5. **PRINCIPES DIRECTEURS**

Les principes directeurs qui guident les actions de la commission scolaire en matière de sécurité de l'information sont les suivants :

a) S'assurer de bien connaître l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité;

b) Reconnaître l'importance de la politique de sécurité de l'information;

c) Reconnaître que l'environnement technologique des actifs de l'information numérique et non numérique est en changement constant et interconnecté avec le monde;

d) Protéger l'information tout au long de son cycle de vie (création, traitement, destruction);

e) S'assurer que chaque employé doit avoir accès au minimum d'information requis pour accomplir ses tâches normales;

f) L'utilisation des actifs de l'information numérique et non numérique par les utilisateurs doit être encadré par une politique ou directive qui explique une marche à suivre appropriée, qui indique ce qui est permis et ce qui ne l'est pas.

6. **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.

La gestion des risques liés à la sécurité de l'information numérique et non numérique s'inscrit dans le processus global de gestion des risques de la commission scolaire. Les risques à portée gouvernementale sont déclarés conformément à la Directive sur la sécurité de l'information gouvernementale. L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement de la commission scolaire. Le niveau de protection de l'information est établi en fonction :

- De la nature de l'information et de son importance;
- Des probabilités d'accident, d'erreur ou de malveillance auxquelles elles sont exposées;
- Des conséquences de la matérialisation de ces risques;
- Du niveau de risque acceptable par la commission scolaire.

7. **GESTION DES INCIDENTS**

La commission scolaire déploie des mesures de sécurité de l'information de manière à assurer la continuité de ses services. À cet égard, elle 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 MEES conformément à la Directive sur la sécurité de l'information gouvernementale.

Dans la gestion des incidents, la commission scolaire peut exercer ses pouvoirs et ses prérogatives en égard de toute utilisation inappropriée de l'information qu'il détient ou de ses systèmes d'information.

8. **DIRECTIVES**

Pour chacune des directives élaborées ci-dessous, prévoir une révision à fréquences prédéterminées et procéder à une mise à jour au besoin.

A. Gestion des accès

Une gestion des accès logique et physique doit être élaborée, encadrée et contrôlée pour faire en sorte de protéger la disponibilité, l'intégrité et la confidentialité de l'information numérique et non numérique. Cette gestion doit inclure l'approbation, la revalidation et la destruction de ces accès et de conserver ces évidences pour les audits ultérieurs.

B. Gestion des vulnérabilités

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

C. Gestion des copies de sauvegardes

La commission scolaire doit élaborer une stratégie de copie de sauvegarde pour se prémunir contre une perte de données numériques et non numériques. Cette stratégie doit inclure la rétention des copies, les alertes d'erreurs lors de la prise de copie et les tests de restauration de ces copies à une fréquence adéquate.

D. Continuité des affaires

La commission scolaire doit élaborer une stratégie de continuité des affaires advenant qu'un incident cause l'arrêt de la prestation de service d'une commission scolaire. Cette stratégie doit

être testée à une fréquence adéquate et les écarts corrigés.

E. Protection du périmètre du réseau

La commission scolaire doit instaurer des exercices de tests d'intrusion et balayages de vulnérabilités pour identifier les points d'entrées susceptibles de donner un accès inapproprié à des individus ou des programmes malicieux. De plus, un système de prévention et de détection d'intrusion devrait être mis en place pour augmenter le niveau de protection. Aussi, segmenter son réseau permet à la commission scolaire de diminuer les chances de propagation d'un virus ou d'une attaque.

F. Utilisation d'un appareil personnel (B.Y.O.D)

Une directive sur l'utilisation d'un appareil personnel (iPad, téléphone intelligent, etc.) dans l'exercice de ses fonctions doit être élaborée pour bien encadrer cette pratique. Les données de la commission scolaire doivent être protégées.

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

G. Protection des actifs de l'information format non numérique

La commission scolaire doit se doter d'une directive de protection des actifs de l'information non numérique qui sont en lien principalement aux classeurs et imprimantes. Une notion de bureau propre doit être instaurée. Ces actifs non numériques peuvent être transportés et produits en plusieurs exemplaires. La notion d'archivage et de destruction doit être considérée dans l'élaboration de cette directive. Cette protection inclut la gestion des accès physiques aux salles, aux imprimantes ou autres endroits qui détiennent des actifs de l'information non numérique. Cette directive de la protection du périmètre prévoit faire des tests d'intrusions ainsi de les protéger lors du transit d'un endroit à un autre.

H. Gestion des fournisseurs

La commission scolaire doit mettre en place un processus de gestion de ses fournisseurs pour s'assurer qu'ils ne viendront pas causer des incidents, des divulgations/pertes de données ou introduire des 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 de la commission scolaire et que la commission scolaire est en droit de voir les résultats des audits (3416, SOC2, etc.) conduits sur ce fournisseur. Cette entente doit aussi inclure les objectifs/niveaux de services attendus par ce fournisseur. Les fournisseurs ont accès à l'information sensible de la commission scolaire, c'est pourquoi qu'une entente de confidentialité doit être signée avec le fournisseur dans le but de diminuer le risque d'une divulgation de cette information.

I. Internet des objets (*Internet of things*)

La commission scolaire doit mettre en place un processus de supervision de l'IOT, y compris une force de frappe cyber-attaque multipliée par dix, du type DDOS (Distributed Denial of Services), augmenter la surface d'attaque et permettre de stocker les données à caractère personnel dans un plus grand nombre de lieux.

9. **SENSIBILISATION ET FORMATION**

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la communauté de la commission scolaire doivent être formés et sensibilisés :

- À la sécurité de l’information et des systèmes d’information de la commission scolaire;
- Aux directives de la sécurité;
- À la gestion des risques;
- À la gestion des incidents;
- Aux menaces existantes;
- Aux conséquences d’une atteinte à la sécurité;
- À leur rôle et à leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement. De plus, des documents explicatifs sont disponibles sur le site Internet de la commission scolaire.

10. **SANCTIONS**

Tout employé de la commission scolaire qui contrevient au cadre légal, à la présente politique et aux mesures de sécurité de l’information qui en découlent, 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 internes applicables (dont celles des conventions collectives de travail et des Règlements de la commission scolaire).

Les fournisseurs, partenaires, invités, consultants ou organismes externes sont passibles à ces sanctions.

11. **DIFFUSION ET MISE À JOUR DE LA POLITIQUE**

Le RSI, assisté du comité de travail pour la sécurité de l’information, s’assure de la diffusion et de la mise à jour de la politique. La politique de sécurité de l’information sera révisée périodiquement selon les mises à jour effectuées.

12. **ENTRÉE EN VIGUEUR**

La présente politique est entrée en vigueur à la date de son adoption par le conseil des commissaires, soit le JJ mois AAAA.

GLOSSAIRE DE LA SÉCURITÉ DE L'INFORMATION

Auteur :
André Bachand, Directeur projet SICS et conseiller principal en sécurité de l'information

Direction générale de la commission scolaire « ABC »
Projet de sécurité de l'information dans les commissions scolaires (SICS

HISTORIQUE

Auteur	Rôle	Description	Date
André Bachand	Conseiller principal de la SI	Création	2017-11-28
André Bachand	Conseiller principal de la SI	Modif déf pour CSGI, Détenteur de l'information, incidents à portée gouvernementale, imputabilité, mesure de sécurité de l'information, renseignement confidentiel et RSI Retrait déf du responsable de l'actif informationnel	2018-03-20

Table des matières

Actif informationnel

Tout actif sur lequel reposent des données numériques ou non numériques. Base de données sur un serveur, un document papier dans un classeur.

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 la commission scolaire qui peut être accessible 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) ou accessible par un dispositif plus traditionnel tel 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 (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

Actif informationnel numérique

Toute information stockée dans un format numérique sur un de ces médias : disque, base de données, disquettes, ruban magnétique, cassette, clé USB, mémoire flash, vidéo, photo numérique, ordi portable, desktop, tablettes, téléphone intelligent, etc. L'information sur le média de l'actif numérique peut être écrite, effacée, réécrite, cryptée et copiée.

Actif informationnel non numérique

Toute information autre que numérique telle : papier, microfilm, pellicule, photo papier, etc.

- L'information sur le média de l'actif non numérique, une fois produite, ne peut être effacée, réécrite, cryptée et copiée.
- Les actifs non numériques peuvent se retrouver dans une pièce, sur un mur, dans un classeur, dans une valise, dans un sac à dos.
- Ils peuvent être facilement déplacés.
- Ils peuvent être produits en plusieurs copies et être à plus d'un endroit.
- Leur suivi à la trace est ardu.

- Un actif non numérique qui est numérisé est considéré comme un actif non numérique.
- L'information de cet actif peut varier d'une copie à une autre. Ex. : un plan d'intervention d'un élève peut être numérisé une première fois et ensuite numérisé une seconde fois quand tous les intervenants impliqués l'ont signé.
-

Authentification

Permettre de confirmer l'identité d'une personne ou l'identification d'un document ou d'un dispositif.

Autorisation

L'attribution par la commission scolaire à une personne ou à un groupe de personnes d'un droit d'accès, complet ou restreint, à une information ou à un système d'information.

Cadre de gestion

L'ensemble des consignes qu'elles soient les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues, les comités qui encadrent les activités d'un établissement qu'est une commission 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.

Confidentialité

La propriété d'une information d'être accessible uniquement aux personnes ou entités désignées et autorisées et d'être divulguée qu'à celles-ci.

Coordonnateur sectoriel de la gestion des incidents (CSGI)

Personne nommée par le Conseil des Commissaires pour occuper ce rôle. Collaborant étroitement avec le COGI-réseau du MEES, le CSGI d'une commission scolaire agit aux points de vue tactique et opérationnel. Il apporte le soutien nécessaire au RSI pour qu'il puisse s'acquitter de ses responsabilités et est l'interlocuteur officiel de son organisation auprès du CERT/AQ. Voir le guide de nomination pour plus d'information.

Cycle de vie de l'information

L'ensemble des étapes que franchit l'information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation de la commission scolaire.

Détenteur

Une personne qui a la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels de la commission scolaire.

Détenteur de l'information

Le détenteur de l'information est le cadre détenant l'autorité au sein d'un service, qu'elle soit d'ordre pédagogique ou d'ordre administratif, et dont le rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de ce service. Il peut donc y avoir plusieurs détenteur de l'information dans une commission scolaire. Le détenteur de l'information peut déléguer la totalité ou bien une partie de sa responsabilité à un autre membre du service. Il :

- Informe le personnel relevant de son autorité et les tiers avec lesquels transige le service de la politique de sécurité de l'information et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s'y conformer;
- Collabore activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques;
- 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 relevant de son autorité en conformité avec la politique de sécurité de l'information et de tout autre élément du cadre de gestion;
- S'assure que les exigences en matière de sécurité de l'information sont prises en compte dans tout processus d'acquisition et tout contrat de service sous sa responsabilité et voit à ce que tout consultant, fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la politique de la sécurité de l'information et tout autre élément du cadre de gestion;
- Rapporte au CSGI toute menace ou tout incident numérique ou traditionnel afférant à la sécurité de l'information;
- 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'information;
- Rapporte au directeur général tout problème lié à l'application de la politique de sécurité de l'information, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de la politique de la sécurité de l'information.
-

Dérogation

Formulaire rempli et dûment approuvé par les intervenants appropriés permettant de déroger pour une durée de temps déterminée à un requis de sécurité après avoir identifié le risque, l'impact et la ou les mesures compensatoires.

Directeur général

Il est le premier répondant de la sécurité de l'information. Voir le guide de nomination pour plus d'information.

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.

Disponibilité

La propriété d'une information d'être accessible en temps voulu et de la manière requise à 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.

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 dont les risques d'atteinte à sa disponibilité, à son intégrité ou à sa confidentialité peuvent avoir des conséquences liées à la vie et la santé ou le bien-être des personnes, à l'atteinte à la protection des renseignements personnels et à la vie privée, à la prestation de services à la population ou à l 'image de la commission scolaire et du gouvernement et 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.

Imputabilité

Le principe selon lequel une action/activité peut sans équivoque être attribuée à l'entité qui en est responsable (non-répudiation).

Intégrité

La propriété d'une information de ne subir aucune altération ni destruction sans autorisation ou de façon erronée, et qui est conservée sur un support et préservée avec des moyens lui procurant stabilité et pérennité. L'intégrité fait référence à l'exactitude et à la complétude.

Mesure de sécurité de l'information

Un moyen concret assurant partiellement ou totalement la protection d'information de la commission scolaire contre un ou plusieurs risques (panne majeure du réseau informatique ou des serveurs institutionnels, acte involontaire, acte malveillant tel que l'intrusion dans un système informatique, la divulgation ou le vol de documents, etc.) et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

Mesure compensatoire

Un moyen concret permettant de diminuer la probabilité d'une occurrence de matérialisation d'un risque découlant d'une non-conformité.

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 de la commission scolaire.

Plan de relève

Le plan de reprise hors site mis en œuvre lorsqu'il y a détérioration ou destruction d’actifs informationnels consécutive à un incident exigeant le transfert de l’exploitation dans un autre lieu. Le plan de relève décrit les procédures visant à assurer, dans des conditions de continuité adaptées aux critères de survie de la commission scolaire, la mise à la disposition rapide et ordonnée des moyens de secours ainsi que la reprise éventuelle de l'exploitation normale après réfection ou remplacement des actifs détruits ou endommagés.

Registre d’autorité

Le répertoire, le recueil ou le fichier dans lequel sont notamment consignées les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l’information ainsi que les responsabilités qui y sont rattachées.

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 confidentiel

Un renseignement, une information dont l’accès est assorti d’une ou de plusieurs restrictions prévues par la Loi sur l’accès aux documents des organismes publics et par La loi sur la protection des renseignements personnels et qui doit obtenir le consentement du détenteur de l’information avant de pouvoir la divulguer à qui ce soit..

Renseignement personnel

Une information concernant une personne physique et qui 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 de la politique de la sécurité de l’information.

Responsable de la sécurité de l’information (RSI)

Personne nommée par le Conseil des Commissaires pour occuper ce rôle. Il a un rôle stratégique et relationnel avec la haute direction. Il communique à sa commission scolaire les orientations et le priorités en matière de sécurité de l’information et s’assure de l’arrimage et de la participation de tous les intervenants de sa commission scolaire. Voir le guide de nomination pour plus d’information.

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 de la commission 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.

Secrétaires généraux

Les secrétaires généraux valident et approuvent les politiques en SI. Ils préparent les résolutions pour les nominations et les politiques et s'assurent de la conformité au cadre législatif.

Sécurité de l'information

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

Service des ressources humaines

En matière de sécurité de l'information, le service des ressources humaines s'assure que tout nouvel employé de la commission scolaire soit avisé de la politique de sécurité de l'information et obtient son engagement au respect de la politique.

Service des ressources matérielles

Le service des ressources matérielles participe, avec le CSGI/RSI, à l'identification des risques traditionnels et des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels traditionnels de la commission scolaire.

Service des technologies de l'information

En matière de sécurité 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 de 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, tel que 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 à la présente politique et autorisées par le directeur général.

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).

Utilisatrice ou utilisateur

Toute personne, employé, parent ou toutes autres personnes physiques qui accède par le truchement des réseaux numérique et non numérique à de l’information que la commission scolaire détient dans l’accomplissement de sa mission. Les membres du personnel de la commission scolaire ainsi que les étudiants sont les premiers utilisateurs de l’information de la commission scolaire. Tout utilisateur de ces réseaux doit se conformer aux politiques et aux directives en vigueur dans une entreprise ou un organisme avec lequel il est en relation dans le cadre de ses activités professionnelles ou d’études lorsqu’il y partage des actifs informationnels, des dispositifs de technologies de l’information ou des systèmes d’information.

Traçabilité

La traçabilité désigne la situation où l'on dispose de l'information nécessaire et suffisante pour connaître (éventuellement de façon rétrospective) la composition de l’actif tout au long de sa chaîne de production, de transformation et de distribution. Et ce, en quelque endroit que ce soit, et depuis l'origine première du produit jusqu'à sa fin de vie.