REGISTRE DE DOCUMENTS OFFICIELS

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Catégorie et code :	**P – 2.18**
Date d'entrée en vigueur :	**29 juin 2020**
Nombre de pages :	**16**
Origine:	**Service de l'Innovation et de la technologie**
Endroit d'application et d'entreposage:	**Service juridique**
Historique :	**Adoptée - résolution 2020-06-#08**

Table des matières

1. CONTEXTE **3**

2. OBJECTIFS **3**

3. CADRE LÉGAL ET ADMINISTRATIF **4**

4. CHAMP D'APPLICATION **4**

5. PRINCIPES DIRECTEURS **5**

6. GESTION DES RISQUES **5**

7. GESTION DES INCIDENTS **6**

8. MESURES **6**

A. Gestion de l'accès 6
B. Gestion de la vulnérabilité 6
C. Gestion des copies de secours 6
D. Continuité des activités 7
E. Protection du périmètre du réseau 7
F. Utilisation d'appareils personnels 7
G. Protection des actifs informationnels non numériques 7
H. Gestion des fournisseurs 7
I. Internet des objets (IdO) 7

9. SENSIBILISATION ET FORMATION **8**

10. COMITÉS **8**

11. SANCTIONS **9**

Annexe A – GLOSSAIRE DE LA SÉCURITÉ DE L'INFORMATION ET DÉFINITION DES RÔLES ET RESPONSABILITÉS

Dans le présent document, le pluriel du genre neutre ou la forme collective ont été utilisés chaque fois que c'était possible dans le contexte.
L'annexe est jointe à titre de référence et de gestion et elle peut être mise à jour ou modifiée sans consultation.

1. CONTEXTE

Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (projet de loi numéro 133) et la Directive sur la sécurité de l'information gouvernementale (une directive du Conseil du Trésor du Québec qui s'applique aux commissions scolaires) impose des obligations aux établissements d'enseignement dans leurs fonctions d'organismes publics.

La *Directive sur la sécurité de l'information gouvernementale*[1] et le *Cadre gouvernemental de gestion de la sécurité de l'information*[2] exigent que les commissions scolaires adoptent, mettent en oeuvre, tiennent à jour et assurent l'application d'une politique de sécurité de l'information pour gérer les risques, l'accès à l'information et les incidents et que chacune nomme un responsable de la sécurité de l'information (RSI) et deux (2) coordonnateurs sectoriels de la gestion des incidents (CSGI).

Cette politique permet à la Commission scolaire Lester-B.-Pearson (CSLBP) d'accomplir ses missions, de préserver sa réputation, de respecter les exigences juridiques et de réduire les risques tout en protégeant l'information qu'elle a créée ou reçue (et dont elle est responsable). Cette information, accessible en formats numérique et non numérique et relevant des ressources humaines, physiques, technologiques et financières, peut être de nature délicate et soumise à des risques d'atteinte à sa disponibilité, intégrité ou confidentialité qui pourraient avoir des conséquences sur :

- La vie, la santé ou le bien-être des personnes
- La protection des renseignements personnels et de 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, où qu'elle soit stockée et comment elle est communiquée. 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.

La commission scolaire a par conséquent adopté cette politique pour orienter et déterminer sa vision, qui est expliquée en détail dans son cadre de gestion de la sécurité de l'information.

[1] https://www.tresor.gouv.qc.ca/ressources-informationnelles/securite-de-linformation/directive-sur-la-securite-de-linformation-gouvernementale/
[2] https://www.tresor.gouv.qc.ca/fileadmin/PDF/ressources_informationnelles/directives/cadre_gestion_securite_information.pdf

3. CADRE LÉGAL ET ADMINISTRATIF

La présente politique sur la sécurité est régie principalement 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, c. 64)
- *La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* (LRQ, c. G-1.03)
- *La Loi concernant le cadre juridique des technologies de l'information* (LRQ, c. C-1.1)
- *La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (LRQ, c. A-2.1)
- *La Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42);
- *Le Code criminel* (LRC, 1985, chapitre C-46);
- Secrétariat du Conseil du Trésor références :
    - *Cadre gouvernemental de gestion de la sécurité de l'information*
    - *Politique-cadre sur la gouvernance et la gestion des RI des organismes publics et des entreprises du gouvernement,*
    - *Directive sur la sécurité de l'information gouvernementale*
- Autres politiques et documents administratifs de la CSLBP :
    - Politique concernant l'utilisation appropriée des ressources et des technologies numériques
    - Politique en matière de surveillance vidéo
    - Politique sur la gestion des documents

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'élève 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, en signant la déclaration jointe en annexe;

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, qu'elle soit numérique ou non numérique, 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.

5. PRINCIPES DIRECTEURS

Les principes directeurs suivants guident les actions de la commission scolaire sur la sécurité de l'information :

a) Acquérir une compréhension complète de l'information à protéger;

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

c) Comprendre que l'environnement technologique de l'information numérique et non numérique change constamment et est 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 seulement à l'information requise 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

Un classement à jour par catégories des actifs informationnels sert à l'analyse des risques en déterminant la valeur de l'information à protéger.

La gestion des risques associés à la sécurité de l'information numérique et non numérique fait partie du processus général de gestion des risques de la commission scolaire. Les risques ayant des incidences gouvernementales sont traités dans la *Directive sur la sécurité de l'information gouvernementale*. L'analyse des risques comprend aussi l'achat, le développement et le fonctionnement des systèmes d'information en précisant les mesures de sécurité à mettre en œuvre dans le cadre du déploiement de systèmes dans l'environnement de la commission scolaire.

Le degré de protection de l'information est déterminé par :

- la nature de l'information et son importance
- la probabilité d'un accident, d'une erreur ou d'un acte malveillant auxquels l'information est exposée
- les conséquences qu'un tel risque se réalise
- le degré de risque jugé acceptable par la commission scolaire.

7. GESTION DES INCIDENTS

La commission scolaire adopte des mesures sur la sécurité de l'information pour assurer la continuité de ses services. À cette fin, elle met en œuvre les mesures nécessaires pour atteindre les objectifs suivants :

- Limiter la possibilité d'incidents de la sécurité de l'information
- Gérer adéquatement ces incidents pour réduire les conséquences et reprendre les activités ou les opérations

Les incidents à la sécurité de l'information ayant des répercussions gouvernementales doivent être signalés 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 prérogatives relativement à toute utilisation inappropriée de l'information qu'elle détient ou de ses systèmes d'information.

8. MESURES

Des mesures sont mises en place pour gérer la sécurité de l'information dans l'organisme (consulter l'annexe A - GLOSSAIRE SUR LA SÉCURITÉ DE L'INFORMATION ET DÉFINITION DES RÔLES ET RESPONSABILITÉS) :

A. <u>Gestion de l'accès</u>

La gestion de l'accès physique doit être planifiée et contrôlée pour protéger la disponibilité, l'intégrité et la confidentialité des données numériques et non numériques. Cette gestion doit comprendre l'approbation, la revalidation et la destruction des accès ainsi que l'archivage de la preuve de ces processus de gestion pour des vérifications futures.

B. <u>Gestion des vulnérabilités</u>

La commission scolaire met en œuvre des mesures pour garder à jour ses stocks informatiques afin de réduire la vulnérabilité et des actifs informationnels numériques et non numériques et de réduire la probabilité d'une cyberattaque. Les mesures doivent être prises pour prévenir les vulnérabilités provenant des fournisseurs pour les corriger.

C. <u>Gestion des copies de secours</u>

La commission scolaire doit élaborer une stratégie de copies de secours pour assurer une protection contre la perte d'information numérique et non numérique. Cette stratégie doit comprendre la conservation des copies, des messages d'erreur générés pendant la prise de copies et des essais sur la restauration de copies à des intervalles appropriés.

D. Continuité des activités

La commission scolaire doit dresser une stratégie de continuité des affaires pour répondre rapidement, efficacement et avec sécurité si un incident interrompt la prestation d'un service. Cette stratégie doit être testée à des intervalles appropriés et les disparités doivent être corrigées.

E. Protection du périmètre du réseau

La commission scolaire doit planifier des tests de pénétration et une analyse de vulnérabilité pour déterminer les points d'entrée qui ouvriraient un accès inapproprié aux personnes ou aux maliciels. De plus, un système pour éviter et détecter les intrusions doit être installé pour accroître le degré de protection. En outre, la commission scolaire peut réduire la probabilité d'une attaque par virus ou d'une attaque qui se propage en segmentant le réseau.

F. Utilisation d'appareils personnels

Des mesures doivent être prises pour régir l'utilisation d'appareils personnels (tablettes, téléphones intelligents, etc.) pour exécuter des tâches, car il est essentiel de protéger les données de la commission scolaire.

Si un appareil est volé ou perdu, toutes les mesures nécessaires pour en protéger l'information et les systèmes seront prises par la commission scolaire, y compris la suppression des données sur l'appareil manquant.

G. Protection d'actifs informationnels non numériques

La commission scolaire doit assurer la protection des actifs informationnels non numériques se trouvant principalement dans les classeurs et les imprimantes. Ces actifs non numériques peuvent être transportés et produits en plusieurs copies, par conséquent, les notions de verrouiller les documents, de les archiver et de procéder à leur destruction adéquatement doivent être prises en compte. Les mesures de protection doivent comprendre la gestion de l'accès physique aux salles, aux imprimantes et aux autres endroits où les actifs informationnels non numériques sont conservés. La protection du périmètre doit prévoir des essais d'intrusion et des mesures de protection pendant le transit de l'information d'un endroit vers un autre.

H. Gestion des fournisseurs

La commission scolaire doit lancer un processus de gestion des fournisseurs pour veiller à ce qu'ils ne sont pas la source d'incidents, à ce que l'information ne soit pas dévoilée ni perdue et à ce que des virus n'entrent pas dans le réseau. Pour ce faire, elle doit rédiger des contrats qui stipulent les objectifs et le niveau de service à recevoir de la part du fournisseur ainsi que les mesures de sécurité à développer et à respecter. Les fournisseurs ont accès à des données sensibles de la commission scolaire et il faut donc signer un contrat de confidentialité avec chacun pour réduire le risque de dévoilement de cette information.

I. Internet des objets (IOT)

La commission scolaire doit mettre un processus en place pour surveiller l'Internet des objets. L'IoT peut présenter des risques dans plusieurs secteurs dont la confidentialité, le consentement, la collecte de données et le piratage et les cyberattaques. La commission scolaire doit prendre des mesures raisonnables pour réduire ces risques.

9. SENSIBILIBATION ET FORMATION

La sécurité de l'information dépend grandement de l'encadrement de la conduite personnelle et de la responsabilisation individuelle. Voilà pourquoi les membres de la communauté de la commission scolaire doivent être formés ou sensibilisés à :

- La sécurité de l'information et aux systèmes d'information de la commission scolaire
- Les directives sur la sécurité
- La gestion des risques
- La gestion des incidents
- Les menaces existantes
- Les conséquences d'une violation de sécurité
- Leur rôle et responsabilités dans les questions de sécurité.

10. COMITÉS

1. Comité de la sécurité de l'information

   Pour la gestion des risques, un comité de la sécurité de l'information est créé et a pour mandat :

   - D'analyser la situation et les risques potentiels pour la sécurité de l'information de la commission scolaire;
   - De consulter les politiques, les directives, les cadres, les plans d'action applicables de la commission scolaire, etc.;
   - D'évaluer les mesures prises par la commission scolaire entre autres sur l'accès et la gestion des incidents;
   - De faire des recommandations à la direction.

   Le comité de la sécurité de l'information est composé de :

   - La personne responsable de la sécurité de l'information
   - Les coordonnateurs sectoriels de la gestion des incidents
   - Le RARC ou un représentant des vérifications internes
   - La personne responsable de l'accès à l'information
   - Un représentant des archives
   - Un représentant des ressources matérielles ou des achats

2. Comité de crise et de continuité du fonctionnement

   Pour gérer les crises et assurer la planification du fonctionnement, on fonde un comité de crise et de continuité et on lui attribue le mandat suivant :

   - Autoriser l'application de stratégies pour assurer la gestion des incidents à la sécurité de l'information;
   - Créer le plan de continuité du fonctionnement;
   - Décider quand déployer le plan de continuité du fonctionnement et selon quelle portée;
   - Proposer des orientations ou des mesures à prendre en cas de sinistre;
   - Coordonner avec les personnes concernées et communiquer avec les médias.

Le comité de crise et de continuité est composé de :

- La directrice générale ou un représentant
- Le responsable de la sécurité de l'information
- Un représentant des services concernés
- Un représentant des communications

11. SANCTIONS

Tout employé de la commission scolaire qui contrevient au cadre légal, à la présente politique ou 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 et des règlements de la commission scolaire).

Les élèves, les fournisseurs, les partenaires, les invités, les consultants et les organismes externes peuvent faire l'objet des sanctions jugées appropriées par la commission scolaire.

Annexe A

GLOSSAIRE SUR LA SÉCURITÉ DE L'INFORMATION ET DÉFINITION DES RÔLES ET RESPONSABILITÉS

1. Responsabilisation
   Principe selon lequel une action ou activité peut être attribuée sans équivoque à l'entité responsable (non-répudiation).

2. Authentification
   Confirmation de l'identité d'une personne ou d'un document ou appareil.

3. Registre de l'autorité
   Répertoire, journal ou dossier dans lesquels les attributions et délégations d'autorité servant à gérer la sécurité de l'information, et les responsabilités associées, sont officiellement consignées.

4. Autorisation
   Attribution par la commission scolaire à une personne ou à un groupe du droit d'accès, en tout ou en partie, à de l'information précise ou à un système d'information.

5. Disponibilité
   Propriété de l'information à être disponible au moment et de la manière dont elle est requise par l'utilisateur autorisé.

6. Catégorisation
   Attribution d'une valeur à certaines caractéristiques pour qualifier son degré de sensibilité sur le plan de la disponibilité, de l'intégrité et de la confidentialité et par conséquent, le degré approprié de protection requis.

7. Mesure compensatoire
   Mesure concrète qui sert à réduire la probabilité d'un risque de matérialisation en raison du non-respect.

8. Renseignements confidentiels
   Information dont l'accès est soumis à une restriction ou plus énoncée dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et qui requiert le consentement du détenteur de l'information (ou une exception applicable de la loi) avant d'être dévoilé à quiconque.

9. Confidentialité
   Propriété d'une information selon laquelle elle doit être disponible et dévoilée seulement aux personnes ou entités désignées et autorisées.

10. Plan de continuité
    Toutes les mesures de planification déterminées et appliquées dans le but de ré-établir la disponibilité de l'information essentielle à la poursuite des activités de la commission scolaire.

11. Actif informationnel numérique
    Toute information stockée en format numérique sur l'un des médias suivants : disque, base de données, disquette, ruban magnétique, cassette, clé USB, disque flash, vidéo, photographie numérique, ordinateur portable, ordinateur portatif, tablette, téléphone intelligent, etc. L'information de l'actif numérique sur média peut être écrite, effacée, réécrite, encodée ou copiée.

12. Document
    Ensemble d'information enregistré sur un support. L'information est délimitée et structurée et dépend tangiblement ou logiquement du support média; elle est intelligible en format de mots, de sons ou d'images. Elle peut être rendue par tout moyen écrit, dont un système de symboles transcrits sous forme intelligible ou dans un autre système de symboles. La notion de document comprend toute base de données dont la structure peut être utilisée pour créer des documents en délimitant et en structurant l'information qu'elle contient.

13. Entrée en double pour exemption du détenteur d'information
    Formulaire qui a été approuvé par l'autorité pertinente pour autorises une exception à une exigence de sécurité pour une période précise après que le risque, les répercussions et toutes les mesures compensatoires aient été déterminés.

14. Directeur général ou directrice générale
    Personne qui détient la responsabilité générale de la sécurité de l'information.

15. Service des ressources humaines
    En ce qui concerne la sécurité de l'information, le service des ressources humaines veille à ce que tous les employés de la commission scolaire soient avisés de la politique sur la sécurité de l'information et qu'ils acceptent de s'y conformer.

16. Incident
    Événement qui met en danger ou menace de mettre en danger la disponibilité, l'intégrité ou la confidentialité de l'information ou, plus généralement, la sécurité des systèmes d'information, particulièrement en interrompant les activités ou en réduisant la qualité des services.

17. Registre des incidents
    Journal dans lequel la nature d'un incident portant sur la sécurité de l'information, ses répercussions, le problème sous-jacent et les mesures prises pour ré-établir les opérations normales sont inscrits.

18. Information
Données enregistrées sur un support pour les stocker, les traiter ou les communiquer comme élément de connaissance.

19. Actif informationnel
Tout actif contenant de l'information numérique ou non numérique comme une base de données dans un serveur ou un document en papier dans une armoire de classement.

Un élément ou une banque de données, un système ou un support informatique, un document, une technologie d'information ou du matériel ou une combinaison de tout ce qui précède, qu'ils soient acquis ou constitué par la commission scolaire et qui peuvent être accessibles avec un appareil de technologie de l'information (application, logiciel, logiciel didactique, base de données ou banque d'information d'information textuelle, audio, symbolique ou visuelle stockée dans du matériel ou sur un support d'information, un système de courrier électronique ou de messagerie vocale) ou par un moyen plus traditionnel comme un dossier ou un classeur. Cela comprend l'information et les supports tangibles et intangibles utilisés pour traiter, transmettre ou stocker l'information pour les fins voulues (ordinateurs, ordinateurs personnels, tablettes électroniques, téléphones intelligents, etc.) et l'information inscrite sur un support analogique comme le papier.

20. Détenteur d'information
Le détenteur de l'information est le directeur du service pédagogique ou administratif autorisé à superviser l'accès, l'utilisation adéquate et la sécurité des actifs informationnels dont son service est responsable. Par conséquent, il peut y avoir plusieurs détenteurs de l'information dans une commission scolaire. Ils peuvent déléguer leur responsabilité en tout ou en partie à un autre membre du service. Voici leurs responsabilités :
   - Informer le personnel sous leur autorité et les tiers avec lesquels traite le service de la politique sur la sécurité de l'information et des dispositions du cadre de gestion pour qu'ils connaissent l'exigence de les respecter
   - Collaborer activement à classer par catégories l'information du service dont ils sont responsables et à analyser les risques
   - Assurer la protection de l'information et des systèmes d'information sous leur responsabilité et veiller ensuite à ce que ces derniers soient utilisés sous leur autorité en respectant la politique sur la sécurité de l'information et toute autre disposition se trouvant dans le cadre de gestion
   - Veiller à ce que les exigences sur la sécurité de l'information soient prises en compte dans tous les processus d'achat et les contrats de service sous leur responsabilité et s'assurer ensuite que tous les consultants, fournisseurs, partenaires, invités, organismes et cabinets externes acceptent de respecter la politique sur la sécurité de l'information et toutes les dispositions du cadre de gestion
   - Signaler au CSGI toutes les menaces et tous les incidents concernant la sécurité de l'information numérique ou non numérique
   - Collaborer à mettre en œuvre les mesures visant à améliorer la sécurité de l'information ou à résoudre un incident relatif à la sécurité et à appliquer toute opération pour vérifier la sécurité des actifs informationnels

- Signaler au CSGI tout problème relié à l'application de la politique sur la sécurité de l'information y compris une infraction réelle ou apparente par un membre du personnel relativement à l'application de la politique sur la sécurité de l'information.

21. Cycle de vie de l'information
    Toutes les étapes par lesquelles passe l'information, de la création à l'enregistrement, au transfert à la consultation, au traitement et à la transmission, jusqu'au stockage permanent ou à la destruction conformément au calendrier de conservation de la commission scolaire.

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

23. Directeur ou directrice de la sécurité de l'information
    Cette personne est nommée et elle joue un rôle stratégique tout en ayant un lien avec les cadres supérieurs. Elle communique les orientations de la commission scolaire et ses priorités sur la sécurité de l'information et elle s'assure que tous les intéressés de la commission scolaire sont inclus et participent.

24. Mesure de la sécurité de l'information
    Moyen concret d'assurer la protection partielle ou totale de l'information de la commission scolaire contre un ou plusieurs risques (panne majeure du réseau informatique ou des serveurs de l'établissement, geste involontaire, acte malveillant comme une intrusion dans le système informatique, divulgation ou vol de documents, etc.) qui est mis en œuvre pour réduire la probabilité que ces risques se concrétisent ou les pertes en découlant.

25. Risque pour la sécurité de l'information
    Degré auquel l'information ou un système informatique est exposé à une menace d'interruption ou de réduction de la qualité des services ou à un arrêt de la disponibilité, une violation de l'intégrité ou de la confidentialité de l'information qui pourrait avoir des conséquences sur la prestation des services; la vie, la santé ou le bien-être des personnes, le respect de leurs droits fondamentaux à la protection et à la confidentialité des renseignements personnels; ou l'image de la commission scolaire.

26. Risque pour la sécurité de l'information ayant des répercussions gouvernementales
    Toute menace à la disponibilité, l'intégrité ou la confidentialité d'information gouvernementale qui pourrait avoir des conséquences sur la prestation de services publics; la vie, la santé ou le bien-être de personnes; le respect de leurs droits fondamentaux à la protection et à la confidentialité des renseignements personnels; à l'image du gouvernement; ou la prestation des services fournis par d'autres organismes publics.

27. Système d'information

Tout moyen organisé mis en place pour recueillir, stocker, traiter, communiquer, protéger ou supprimer de l'information afin de répondre à un besoin précis, comportant spécifiquement les applications, les logiciels et les progiciels, les technologies de l'information et les méthodes pour exécuter ces fonctions.

28. Technologie de l'information

Tout logiciel ou matériel ou combinaison des deux servant à recueillir, stocker, traiter, communiquer, protéger ou supprimer de l'information sous toutes ses formes (texte, symbole, audio ou image).

29. Service de l'Innovation et de la technologie

Service responsable des exigences en matière de sécurité de l'information sur le plan du fonctionnement des systèmes informatiques et des projets à développer ou des systèmes à acquérir. Plus précisément, ce service :

- Participe activement à l'analyse des risques, à l'évaluation des besoins et des mesures à appliquer et à la prévision des menaces à la sécurité des systèmes informatiques à l'aide de technologies de l'information.
- Prend des mesures appropriées pour réagir à toute menace à la sécurité ou incident (par exemple, interruption temporaire ou révocation), quand les circonstances l'exigent, concernant les services d'un système informatique utilisant des technologies informatiques afin d'assurer la sécurité de l'information concernée
- Participe aux enquêtes autorisées par la direction générale sur les contraventions réelles ou apparentes à la politique sur la sécurité de l'information.

30. Internet des objets (IdO)

Réseau décentralisé d'appareils, d'applications et de services qui peuvent détecter, traiter, communiquer et agir sur les entrées de données, notamment contrôler les éléments du monde physique.

31. Intégrité

Propriété de l'information selon laquelle celle-ci n'est jamais altérée ni détruite sans autorisation ou alors accidentellement et elle est stockée sur un support et conservée selon des moyens qui assurent leur stabilité et leur pérennité. Par intégrité, on entend l'exactitude et intégralité de l'information.

32. Cadre de gestion

Structure décisionnelle qui offre un cadre pour les activités de la commission scolaire dont le personnel de gestion, les comités et toutes les références pertinentes (politiques, règlements, directives, procédures, pratiques éprouvées reconnues, etc.)

33. Service des ressources matérielles

Avec le CSGI/RSI, ce service participe à déterminer les risques traditionnels et les mesures de sécurité physique qui protégeront adéquatement les actifs informationnels non numériques de la commission scolaire.

34. Actif informationnel non numérique
Toute information dans un format autre que numérique dont le papier, le microfilme, la pellicule, des photos imprimées, etc.

- Les actifs non numériques se trouvent dans une salle, sur un mur, dans un classeur, dans une mallette, dans un sac à dos et elles se transportent facilement, elles peuvent être reproduites en plusieurs copies et elles sont entreposées à plus d'un endroit.
- Les informations non numériques peuvent varier d'une copie à l'autre (par exemple, le PIA d'un élève peut être numérisé au début pour renumérisé quand tous les professionnels concernés l'ont signé.

35. Renseignements personnels
L'information sur une personne physique peut être utilisée pour l'identifier. Consultez la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

36. Plan de reprise
Plan de restauration hors site à appliquer quand les actifs informationnels se détériorent ou sont détruits en raison d'un incident qui nécessite le transfert des opérations à un autre endroit. Ce plan décrit les procédures visant, dans les conditions de continuité respectant les critères de survie de la commission scolaire, à appliquer rapidement et méthodiquement des mesures de secours et éventuellement à rétablir le fonctionnement normal quand les actifs endommagés ou détruits ont été réparés ou remplacés.

37. Coordonnateurs sectoriels de la gestion des incidents (CSGI)
Ces coordonnateurs sont nommés et travaillent en étroite collaboration avec ceux de la commission scolaire et le réseau OCIM du MEES. Ils sont responsables des actions opérationnelles et tactiques. Ils offrent le soutien que nécessite le RSI pour s'acquitter de ses responsabilités et ils sont les personnes-ressources officielles à contacter du CERT/AQ.

38. Incident à la sécurité ayant des répercussions gouvernementales
Conséquence observable de la concrétisation d'un risque à la sécurité de l'information qui pourrait nuire aux activités du gouvernement en compromettre la disponibilité, l'intégrité ou la confidentialité de l'information et par conséquent avoir des répercussions négatives sur la vie, la santé ou le bien-être des personnes; la protection des renseignements personnels et de la confidentialité; ou l'image de la commission scolaire et du gouvernement et par conséquent nécessiter une réaction harmonisée à l'échelle gouvernementale.

39. Traçabilité
Situation où existe assez d'information pour connaître (probablement en rétrospective) le contenu d'un actif dans toute la chaîne de production, de transformation de distribution, peu importe l'endroit, de l'origine du produit à la fin de son cycle de vie.

40. Utilisateur
Personne, employé, parent ou autre personne physique qui utilisent un réseau numérique ou non numérique pour accéder à de l'information détenue par la commission scolaire aux fins de réaliser sa mission. Le personnel et les élèves de la commission scolaire sont les principaux utilisateurs de son information. Tous les utilisateurs de réseau de la commission scolaire doivent respecter les politiques et les directives en vigueur dans le contexte de leurs activités professionnelles ou de leurs études quand ils partagent des actifs informationnels, des appareils informatiques ou des systèmes informatiques.

41. Critères d'évaluation de la sécurité pour l'information numérique et non numérique (pour des documents de toutes les formes)

- Disponibilité
  Propriété de l'information à être disponible au moment et de la manière dont elle est requise par l'utilisateur autorisé.

- Intégrité
  Propriété de l'information selon laquelle celle-ci n'est jamais altérée ni détruite sans autorisation ou alors accidentellement et elle est stockée sur un support et conservée selon des moyens qui assurent leur stabilité et leur pérennité. Par intégrité, on entend l'exactitude et intégralité de l'information.

- Confidentialité
  Propriété d'une information selon laquelle elle doit être disponible et dévoilée seulement aux personnes ou entités désignées et autorisées.