POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Centre de services scolaire Marguerite-Bourgeoys
Québec

ADOPTION :	DATE D'ENTRÉE EN VIGUEUR :	RÉVISÉ LE 28 septembre 2020
Résolution # CC19/20-11-038	LE 20 novembre 2019	Décision # DGCA20/21-09-019

Table des matières

1. PRÉAMBULE 3
2. OBJECTIFS 3
3. ENCADREMENT JURIDIQUE 4
4. CHAMP D'APPLICATION 4
5. PRINCIPES ET OBJECTIFS 5
6. DÉFINITIONS 5
7. CADRE DE GESTION 6
   7.1 Comité de sécurité 6
      7.1.1 Composition 7
      7.1.2 Mandat du Comité 7
   7.2 Gestion des risques 8
   7.3 Gestion des accès 8
   7.4 Gestion des incidents 8
8. RÔLES ET RESPONSABILITÉS 8
Conseil d'administration 8
Directeur général 8
Responsable de la sécurité de l'information (RSI) 9
Coordonnateurs sectoriel de la gestion de l'information (CSGI) 9
Service des ressources informatiques 10
Secrétariat général 10
Service des ressources matérielles 10
Service des ressources humaines 10
Direction d'unité administrative 11
Détenteur de l'information 11
Utilisateur 11
9. MESURES PARTICULIÈRES 12
Sanctions 12
Dérogation 12

ADOPTION : Résolution # CC19/20-11-038	DATE D'ENTRÉE EN VIGUEUR : LE 20 novembre 2019	RÉVISÉ LE 28 septembre 2020 Décision # DGCA20/21-09-019

1. PRÉAMBULE

En vertu de La *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (LGGRI) et de sa *Directive sur la sécurité de l'information gouvernementale* (DSIG), le Centre de services scolaire Marguerite-Bourgeoys (CSSMB), en sa qualité d'organisme public, a l'obligation d'adopter et de mettre en œuvre une Politique sur la sécurité de l'information.

Cette Politique sur la sécurité de l'information doit prévoir 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.

Dans l'exercice de ses activités courantes, le CSSMB crée, recueille et conserve des quantités importantes d'information. Les utilisateurs de ces actifs informationnels utilisent, échangent, traitent et manipulent de nombreuses informations détenues par l'organisation. Ces informations peuvent revêtir, dans certains cas, un caractère sensible ou confidentiel et sont nécessaires à l'exercice des activités du CSSMB. Il est donc essentiel d'en assurer la disponibilité, l'intégrité et la confidentialité, lorsque requis.

Ainsi, la présente politique doit permettre au CSSMB d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'il détient, que cette information soit conservée par lui-même ou par un tiers. Cette information peut être accessible sur des formats numériques et non numériques.

Les risques d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de cette information 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;
- L'image du CSSMB et du gouvernement.

Il importe donc qu'une protection appropriée de cette information soit mise en place afin de prémunir le CSSMB contre des situations qui pourraient mettre à risque son organisation et la conduite de ses activités.

Cette politique énonce les grandes lignes directrices et les responsabilités qui permettent d'encadrer la saine gestion, l'utilisation et la protection des actifs informationnels.

2. OBJECTIFS

La présente politique a pour objectif d'assurer la sécurité de l'information détenue par le CSSMB, tout au long de son cycle de vie. Elle vise à encadrer les modalités d'utilisation et de circulation de l'information ainsi qu'à protéger ses actifs informationnels de façon à assurer la continuité des activités du CSSMB et à minimiser les dommages qui pourraient être causés à l'organisation et à ses utilisateurs en cas d'incident de sécurité, par la prévention de ces incidents ou la réduction de leurs répercussions.

ADOPTION : Résolution # CC19/20-11-038	DATE D'ENTRÉE EN VIGUEUR : LE 20 novembre 2019	RÉVISÉ LE 28 septembre 2020 Décision # DGCA20/21-09-019

De plus, elle vise à renforcer les systèmes de contrôle interne en offrant une assurance raisonnable de conformité à l'égard des lois et autres encadrements gouvernementaux, ainsi qu'aux autres besoins du CSSMB en matière de réduction du risque associé à la protection de l'information.

3. ENCADREMENT JURIDIQUE

La présente politique est adoptée conformément aux règles prévues aux lois et règlements énumérés ci-dessous :

- *Loi sur la gouvernance et la gestion des actifs informationnels des organismes publics et des entreprises du gouvernement* (L.R.Q. c. G-1.03)
- *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q. c. A-2.1)
- *Loi sur les archives* (L.R.Q. c. A-21.1)
- *Loi sur l'instruction publique* (L.R.Q. c. I-13.3)
- *Loi concernant le cadre juridique des technologies de l'information* (L.R.Q. c. c- 1.1)
- *Code civil du Québec* (L.Q. 1991, c64)
- *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)
- *Directive sur la sécurité de l'information gouvernementale*
- Règlements, politiques, procédures et autres encadrements administratifs, notamment la *Politique d'utilisation des ressources informatiques, des technologies de l'information, des médias sociaux et de la vidéosurveillance, la Politique de gestion des documents* et le *Calendrier de conservation* du Centre de services scolaire Marguerite Bourgeoys.

4. CHAMP D'APPLICATION

La présente politique vise autant l'information contenue ou échangée par le biais des systèmes informatiques que l'information sur support papier ou physique. Le contenu d'une clé USB, un espace infonuagique, un courrier électronique, un message texte ou le contenu d'un téléphone cellulaire sont notamment visés.
La présente politique s'adresse aux détenteurs et utilisateurs de l'information. Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le CSSMB.

L'information visée est celle que le CSSMB 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.

5. PRINCIPES ET OBJECTIFS

Les mesures de sécurité doivent être proportionnelles à la valeur de l'information à protéger. Elles sont établies en fonction des risques, de leur probabilité d'occurrence et de leurs conséquences.

Les utilisateurs doivent contribuer à la saine gestion, à l'utilisation et à la protection des actifs informationnels contre les menaces qui risquent d'affecter la confidentialité, l'intégrité, l'accessibilité, la disponibilité, l'usage prévu et la valeur de ces ressources.

Les utilisateurs ont l'obligation de protéger les actifs informationnels mis à leur disposition en les utilisant avec discernement et aux seules fins auxquelles elles sont prévues.

Les actifs informationnels du CSSMB sont réputés être la propriété de ce dernier et non celle des utilisateurs.

Pour ce faire, le CSSMB vise à :

a) Assurer la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise par une personne autorisée;

b) Assurer l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ou altérée de quelque façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;

c) Limiter la divulgation de l'information aux seules personnes autorisées à en prendre connaissance et pour qui l'information est nécessaire dans le cadre de leurs fonctions, assurant ainsi une stricte confidentialité;

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

6. DÉFINITIONS

Actif informationnel
Désigne une information, quel que soit son support (papier, microfilm, clé USB, disque dur, espace infonuagique, etc.) ou son canal de communication (courriel, téléphone, réseau informatique, etc.), un système ou une technologie de l'information ou un ensemble de ces éléments.

Responsable de la sécurité de l'information (RSI)
Désigne la personne responsable de la présente politique. Elle est nommée par le Conseil d'administration.

Coordonnateur sectoriel de la gestion d'incidents (CSGI)
Désigne les personnes qui mettent en œuvre la présente politique et le plan d'action qui en découle. Elles apportent le soutien nécessaire au RSI pour qu'il puisse s'acquitter de ses responsabilités et sont l'interlocuteur officiel du CSSMB auprès du CERT/AQ (Computer emergency response team / administration québécoise). Elles sont nommées par le Conseil d'administration.

Cycle de vie de l'information
L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation du CSSMB.

Détenteur de l'information
Toute personne qui, dans le cadre de ses fonctions, conserve l'information que le CSSMB détient dans le cadre de ses activités, ainsi que les ressources qui la sous-tendent, relevant de la responsabilité de son unité administrative.

Incident
Conséquence observable de la concrétisation d'un risque de sécurité de l'information, nécessitant une intervention concertée. Tout bris de sécurité ou acte susceptible de constituer ou constituant une violation des règles de sécurité dont notamment le vol, la perte, l'intrusion dans un réseau ou un système, les dommages délibérés ou non, l'utilisation ou la diffusion abusive, la fraude, la destruction ou la négligence.

Risque de sécurité de l'information
Risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information détenue par le CSSMB 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 de 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.

Systèmes informatiques
Tout dispositif d'emmagasinage, de reproduction, de transmission de réception et de traitement de l'information dont le CSSMB est propriétaire ou locataire ou sur lesquels il possède un droit à l'utilisation. Sont notamment considérés comme des systèmes informatiques tous les ordinateurs, tablettes, appareils connectés, téléphones intelligents, montres intelligentes, tableaux numériques interactifs (TNI) et projecteurs, imprimantes, moniteurs, bornes sans-fil, caméras de surveillance et serveurs.

Utilisateurs
Membres du Conseil d'administration, membres du personnel, élèves, parents, bénévoles, fournisseurs de service et toute autre personne qui utilise les actifs informationnels du CSSMB.

7. CADRE DE GESTION

7.1 Comité de sécurité

La gestion de la sécurité de l'information nécessite la contribution de plusieurs acteurs du CSSMB ayant des expertises complémentaires. Ainsi, afin de remplir ses obligations en matière de sécurité de l'information, le CSSMB met en place un comité de sécurité conformément aux dispositions de la présente politique.

7.1.1 Composition

- Le responsable de la sécurité de l'information (RSI);
- Les coordonnateurs sectoriels de la gestion l'information (CSGI);
- Un représentant de la direction générale;
- Le responsable de l'accès à l'information et de la protection des renseignements personnels;
- Un représentant du secteur de la gestion de l'information du Secrétariat général;
- Un représentant du secteur juridique du Secrétariat général;
- Un représentant du Bureau des communications.

Une même personne peut assumer plus d'une responsabilité au sein du Comité de sécurité.

Le RSI assure le bon fonctionnement du Comité.

7.1.2 Mandat du Comité

Le Comité de sécurité a pour mandat d'assurer la gestion de la sécurité de l'information. Pour se faire, il voit à :

- Maintenir et diffuser la présente politique à tous les utilisateurs des actifs informationnels essentiels, fournir des conseils et guider son implantation;

- Créer et mettre en œuvre un plan d'action annuel visant à améliorer la sécurité de l'information et tenant compte du présent cadre de gestion des risques;

- Créer et mettre en œuvre un plan de formation des utilisateurs;

- Mettre en place une équipe de réponses aux incidents de sécurité concernant des actifs informationnels numériques ou non numériques et établir une procédure de réponses à ces incidents. Le Comité doit s'assurer que les contrôles sont en place pour identifier un incident lorsqu'il se produit ou s'est produit. Il doit aussi s'assurer que des tests aux réponses d'incidents doivent être conduits périodiquement pour vérifier leur efficacité;

- Apporter les actions correctives et faire des recommandations à la suite d'un incident de sécurité;

- Établir, annuellement, avec la collaboration des détenteurs de l'information, la catégorisation des actifs informationnels et identifier les niveaux de risques de sécurité;

- Rendre compte annuellement de ses activités au Directeur général.

7.2 Gestion des risques

La gestion des risques est assurée par le Comité de sécurité. Pour ce faire, le Comité doit notamment prévoir dans son plan d'action de :

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

7.3 Gestion des accès

La sécurité de l'information est assurée par des mesures d'encadrement et un contrôle adéquat de l'accès, de la divulgation et de l'utilisation de l'information par les personnes autorisées. Ces mesures d'encadrement doivent viser à en protéger la confidentialité et l'intégrité de l'information, en portant une attention particulière à l'information confidentielle et aux renseignements personnels. L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités et une imputabilité des utilisateurs, à tous les niveaux de l'organisation.

7.4 Gestion des incidents

Les incidents doivent être signalés par tout utilisateur à la direction de l'établissement ou du service. Celle-ci doit informer le responsable de la sécurité de l'information (RSI), lequel fait le lien avec le CSGI afin que des mesures de corrections soient prises.

En cas d'incident majeur, le Comité de sécurité est convoqué par le RSI dans les meilleurs délais.

8. RÔLES ET RESPONSABILITÉS

Conseil d'administration
Le Conseil d'administration nomme le responsable de la sécurité de l'information et les coordonnateurs sectoriels de sécurité de l'information. Il adopte la présente politique ainsi que toute modification.

Directeur général
Le Directeur général du Centre de services scolaire, en tant que premier responsable de la sécurité de l'information, entérine le plan d'action et les mesures proposées par le Comité de sécurité. Il nomme également le représentant de la Direction générale au Comité de sécurité.

Responsable de la sécurité de l'information (RSI)
Le RSI est responsable de l'application de la présente politique. À ce titre, il doit :

- Conseiller la Direction générale du CSSMB en ce qui a trait à la détermination des orientations stratégiques et des priorités en matière de sécurité de l'information;

- Assurer l'arrimage de toutes les préoccupations en matière de sécurité de l'information;
- Communiquer au Conseil d'administration, à la demande de la Direction générale, les orientations et les priorités d'intervention gouvernementales en matière de sécurité;

- S'assurer de la participation du CSSMB à la mise en œuvre des processus officiels de gestion de la sécurité de l'information;

- Assurer la coordination et la cohérence des actions de sécurité de l'information menées au sein du CSSMB par d'autres acteurs, tels que les détenteurs de l'information ainsi que les unités responsables des actifs informationnels, 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;

- Coordonner et s'assurer de la mise en œuvre des processus officiels de sécurité de l'information au sein du CSSMB permettant, notamment, d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

Coordonnateurs sectoriel de la gestion de l'information (CSGI)
Les CSGI voient à la mise en œuvre de la présente Politique en ce qui a trait à tous les systèmes de technologies de l'information. Pour ce faire, ils doivent :

- Contribuer à la mise en œuvre des processus officiels de la sécurité au sein du CSSMB tels que :
  - Un registre d'autorité;
  - La catégorisation des actifs;
  - Des mesures de sécurité pour les actifs critiques;
  - Un processus formel de gestion des risques en sécurité;
  - Un processus formel de gestion et de déclaration des incidents;
  - Un processus formel de gestion des droits d'accès à l'information;
  - Un processus formel de gestion des vulnérabilités de sécurité (correctifs);
  - Un processus formel de gestion des sauvegardes;

- Coordonner la gestion des incidents à portée gouvernementale;

- Contribuer aux analyses de risques de la sécurité, définir les menaces et les situations de vulnérabilité et mettre en œuvre les solutions appropriées pour le CSSMB;

- Contribuer à l'autoévaluation de la sécurité des systèmes informatiques et des réseaux informatiques du CSSMB, notamment par des exercices d'audit de sécurité et des tests d'intrusion aux systèmes jugés à risques;

- Tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunication mis en place au CSSMB;

- Maintenir une veille continue sur les risques, les menaces et les vulnérabilités.

Service des ressources informatiques
Le Service des ressources informatiques 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. Pour ce faire, il doit :

- Participer 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 informatiques;

- Appliquer des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, tel que l'interruption ou la révocation temporaire - lorsque les circonstances l'exigent - des accès aux utilisateurs ou 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;

- Participer, avec le Secrétariat général, à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique.

Secrétariat général
Le Secrétariat général veille à la protection des renseignements personnels et à la conservation de l'information détenue par le CSSMB. Il met en place et voit à l'application des règles en matière de protection, d'utilisation, d'accessibilité et de conservation des actifs informationnels. Il effectue les enquêtes nécessaires lors de contraventions réelles ou apparentes à la présente politique.

Il s'assure que les ententes de services et les contrats conclus avec des fournisseurs, des partenaires, des consultants et des organismes externes sont conformes aux exigences en matière de sécurité de l'information.

Service des ressources matérielles
Le Service des ressources matérielles participe à l'identification des mesures de sécurité physique, incluant l'accès aux équipements, permettant de protéger adéquatement les actifs informationnels du CSSMB. Il participe également à la mise en place et aux recommandations des correctifs permettant d'assurer cette sécurité.

Service des ressources humaines
Le Service des ressources humaines s'assure que tout nouvel employé du CSSMB soit informé de la présente politique et obtient son engagement au respect de celle-ci.

Direction d'unité administrative
La direction d'unité administrative, qu'il s'agisse d'un service ou d'un établissement, a la responsabilité de diffuser et de veiller au respect de la présente politique, ainsi que de prendre les mesures nécessaires pour la communiquer et la faire appliquer.

Détenteur de l'information
Le détenteur de l'information doit veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité de son unité.

Utilisateur
L'utilisateur a l'obligation de se conformer à la présente politique et de protéger les actifs informationnels du CSSMB qui sont mis à sa disposition. Il est responsable d'en assurer la confidentialité, l'intégrité et la disponibilité. Il doit les utiliser uniquement aux fins pour lesquelles elles ont été mises à sa disposition.

À cette fin, il doit :

a) Prendre connaissance de la présente politique, des procédures et autres encadrements en découlant, y adhérer et prendre l'engagement de s'y conformer;

b) Utiliser les actifs informationnels mis à sa disposition uniquement dans le cadre des droits d'accès qui lui sont attribués et lorsqu'ils sont nécessaires à l'exercice de ses fonctions, 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 sa configuration ou les désactiver;

d) Respecter les règles applicables relativement à la sécurité et la confidentialité des dossiers physiques et électroniques;

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

f) Signaler immédiatement à son supérieur ou à toute personne responsable tout acte dont il a connaissance et susceptible de constituer une violation réelle ou présumée des règles de sécurité ainsi que toute anomalie pouvant nuire à la protection des actifs informationnels du CSSMB.

Par le seul fait d'utiliser l'information et les systèmes du CSSMB, les utilisateurs reconnaissent que les actifs informationnels, y compris ceux qui sont créés par eux, sont la propriété du CSSMB, à moins d'entente préalable.

9. MESURES PARTICULIÈRES

Sanctions
Toute personne qui contrevient à cette Politique ou aux modalités qui en découlent s'expose à des mesures disciplinaires, pouvant aller jusqu'au congédiement.

Dérogation
Toute dérogation à la présente politique doit faire l'objet d'une demande écrite de l'utilisateur au responsable de la sécurité

Centre
de services scolaire
Marguerite-Bourgeoys
Québec

©Centre de services scolaire Marguerite-Bourgeoys, 2020

Tous droits réservés.

Toute reproduction d'une partie quelconque de ce document par quelque procédé que ce soit est strictement interdite sans l'autorisation écrite du Centre de services scolaire Marguerite-Bourgeoys.