Centre
de services scolaire
des Patriotes
Québec

CADRE DE GESTION DE LA SÉCURITÉ DE L'INFORMATION

Version initiale : 3 décembre 2019
Dernière mise à jour : 16 mars 2023

TABLE DES MATIÈRES

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 des Patriotes (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 gouvernementale sur la sécurité de l'information*[1].

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 des Patriotes (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.

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.

DIRECTIVES (PROCESSUS DE GESTION DE SÉCURITÉ DE L'INFORMATION)

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.

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.

[1] Article 12, alinéa 1

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 gouvernementale sur la sécurité de l'information*. 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 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.

Gestion des accès

Une gestion des accès logique et physique est 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 inclut l'approbation, la revalidation et la destruction de ces accès et de conserver ces évidences pour les audits ultérieurs.

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'atteinte 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 gouvernementale sur la sécurité de l'information* et du *Processus de gestion des menaces, des vulnérabilités et des incidents* (GMVI) du Centre gouvernemental de cyberdéfense.

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.

GESTION DES VULNÉRABILITÉS

Pour réduire le nombre de vulnérabilités, le Centre de services scolaire maintient à jour son parc informatique de manière proactive afin de diminuer les probabilités d'une cyberattaque. Un mécanisme de détection des vulnérabilités ainsi qu'un processus de réponse aux vulnérabilités détectées sont mis en place.

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 stratégie inclut la création et 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.

CONTINUITÉ DES AFFAIRES

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

PROTECTION DU PÉRIMÈTRE DU 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.

UTILISATION D'UN APPAREIL PERSONNEL

Une directive sur l'utilisation d'un appareil personnel (iPad, téléphone intelligent, etc.) dans l'exercice de ses fonctions est élaborée pour encadrer cette pratique. Les données du Centre de services 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, le Centre de services scolaire doit procéder à l'effacement de ses données.

PROTECTION DES ACTIFS DE L'INFORMATION FORMAT NON NUMÉRIQUE

Le Centre de services scolaire se dote d'une directive de protection des actifs conservés sous forme papier. Ces actifs peuvent être transportés et produits en plusieurs exemplaires. La notion d'archivage et de destruction est 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.

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, des 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[2] 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 une entente de confidentialité doit être signée avec le fournisseur dans le but de diminuer le risque d'une divulgation de cette information.

RÔLES ET RESPONSABILITÉS

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

Dirigeant

Le Conseil d'administration a délégué au directeur général le pouvoir de désigner le chef de la sécurité de l'information organisationnelle (CSIO) et les coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI) dans le Centre de services scolaire.

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.

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.

---

[2] Audits pouvant être effectués :
NCMC 3416 (Norme Canadienne de Mission de Certification) est une norme servant à démontrer l'intégrité et la sécurité des processus de contrôle interne au sein d'une entreprise de service.
Un rapport SOC 2 permet d'émettre une opinion sur les contrôles en place chez un prestataire, contrôles relatifs à la sécurité, la disponibilité, l'intégrité des traitements, la confidentialité et/ ou la protection des données (appelés « Trust Services Categories »)

Le CSIO assure 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.

Le CSIO 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, le CSIO du Centre de services scolaire met en œuvre un processus de veille sur les menaces et vulnérabilités ainsi que sur les bonnes pratiques de sécurité de l'information.

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

Les COMSI 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.

Les COMSI 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. Les COMSI 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.

Comité pour la sécurité de l'information

Le comité pour la sécurité de l'information a pour objectif d'assister 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.

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 :

- 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 au présent cadre et autorisées par le CSIO.

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.

Service des ressources humaines

En matière de sécurité de l'information, le Service des ressources humaines s'assure que tout nouvel employé 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.

Direction de l'unité administrative

En matière de sécurité de l'information, la direction de l'unité administrative 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 veille 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 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 et tout autre élément du Cadre;

- rapporte au CSIO et aux COMSI toute menace ou tout incident 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'actif de l'information numérique et non numérique;
- 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.

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;
- assurer, le moment venu, la destruction sécuritaire des documents sensibles;
- 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 et ne pas modifier leur configuration ou les désactiver;

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 différentes cartes d'identité et d'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.

Les cadres et les hors-cadres doivent également prendre un engagement écrit de se conformer aux obligations précédentes **en signant la déclaration jointe à l'Annexe 1**.

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.

REGISTRE DES ÉVÈNEMENTS DE SÉCURITÉ

Le Centre de services scolaire centralise dans un document sécurisé, l'ensemble des informations relatives aux incidents de sécurité qui surviennent dans le périmètre couvert par le présent cadre. Dans un objectif d'amélioration continue, les mesures prises pour corriger la situation ainsi que les recommandations pour prévenir les incidents similaires à l'avenir y sont consignés.

DIFFUSION ET MISE À JOUR

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

ANNEXE 1 | DÉCLARATION D'ENGAGEMENT PAR LES EMPLOYÉS CADRES ET HORS-CADRES QUANT AU RESPECT DES RÈGLES DE SÉCURITÉ DE L'INFORMATION

Les utilisateurs, cadres et hors cadres, ont l'obligation de protéger les actifs informationnels mis à leur disposition par le Centre de services scolaire. À cette fin, ils doivent :

- Se conformer aux directives du Centre de services scolaire, à la politique sur la sécurité de l'information ainsi qu'aux procédures et aux autres lignes de conduite se rapportant à la sécurité de l'information du Centre de services scolaire;
- Utiliser, dans le cadre des droits d'accès qui leur sont attribués et uniquement lorsqu'ils sont nécessaires à l'exercice de leurs fonctions, les actifs informationnels mis à leur disposition, en se limitant aux fins auxquelles ils sont destinés;
- Respecter les mesures de sécurité mises en place sur leur poste de travail et sur tout équipement contenant des données à protéger et ne pas modifier la configuration des mesures de sécurité ou les désactiver;
- Se conformer aux exigences légales portant sur l'utilisation des produits à l'égard desquels des droits de propriété intellectuelle pourraient exister;
- Signaler immédiatement à leur supérieur tout acte dont ils ont 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 du Centre de services scolaire;
- Au moment de leur départ du Centre de services scolaire, remettre les différentes cartes d'identité et d'accès, les actifs informationnels ainsi que tout l'équipement informatique ou de téléphonie qui avaient été mis à leur disposition dans le cadre de l'exercice de leurs fonctions.

Je soussigné(e), _____, reconnais avoir pris connaissance des règles, ci-dessus reproduites, sur la sécurité de l'information du Centre de services scolaire et m'engage à les respecter.

Année	Mois	Jour

_____
Signature

Date

GLOSSAIRE

« Actif informationnel numérique »

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 inclut 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.

« Authentification »

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

« Autorisation »

L'attribution par le centre de services 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.

« 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.

« 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 du centre de services scolaire.

« 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.

« 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.

« 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.

« Imputabilité »

Le principe selon lequel une violation ou une tentative de violation d'un système informatique est attribuée à l'entité qui en est responsable.

« Mesure de sécurité de l'information »

Un moyen concret assurant partiellement ou totalement la protection d'information du Centre de services 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, 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.

« Norme »

Accord entériné par un organisme officiel de normalisation comme l'Organisation internationale de normalisation (ISO), le Conseil canadien des normes (CCN), etc., contenant des spécifications techniques ou autres critères précis destinés à être utilisés systématiquement en tant que règles, lignes directrices ou définitions de caractéristiques pour assurer que des matériaux, produits, processus et services sont aptes à leur emploi.

« 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.

« 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 du centre de services 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.

« Pratique »

Savoir ou manière de faire qui, dans une organisation, conduisent au résultat souhaité 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'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, dont celles prévues à la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels que sont les incidences sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, l'administration de la justice et de la sécurité publique, les décisions administratives ou politiques et la vérification.

« 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.

« Responsable d'actifs informationnels »

Le membre du personnel cadre détenant la plus haute autorité au sein d'une unité pédagogique ou administrative et dont le rôle consiste notamment, du point de vue décisionnel, fonctionnel ou opérationnel, à veiller à l'accessibilité, à l'utilisation adéquate, à la gestion efficiente et à la sécurité des actifs informationnels sous la responsabilité de cette unité. Aux fins de l'application de la présente politique, il peut s'agir d'un autre membre du personnel-cadre de l'unité désigné par la personne qui détient la plus haute autorité au sein de l'unité.

« 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.

« Standard »

Norme qui n'a été ni définie ni entérinée par un organisme officiel de normalisation comme l'Organisation internationale de normalisations (ISO), le Conseil canadien des normes (CCN), etc., mais qui s'est imposée par la force des choses parce qu'elle fait consensus auprès des utilisateurs, d'un groupe d'entreprises ou encore d'un consortium.

« 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).

« 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.