Centre de services scolaire des Découvreurs Québec	MANUEL DE GESTION	CODIFICATION N^{o} 03.11.11
ENTRÉE EN VIGUEUR 29 mai 2019	**SECTEUR** Direction générale	**NATURE** Politique
APPROBATION Par : Direction générale Date : 28 mai 2019		**AMENDEMENT**

POLITIQUE RELATIVE À LA SÉCURITÉ DE L'INFORMATION

1. PRÉAMBULE

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)* (L.R.Q., chap. G-1.03) et de la *Directive sur la sécurité de l'information gouvernementale (DSIG)* (C.T. – Décret 7-2014) créent des obligations aux établissements scolaires en leur qualité d'organismes publics.

Ainsi, la *Directive sur la sécurité de l'information gouvernementale* oblige le CSS à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique relative à la sécurité de l'information dont les principales modalités sont définies dans la directive gouvernementale. Le recours à des processus formels de sécurité de l'information permet d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents. Ce nouvel encadrement exige que deux nouveaux rôles soient assurés au sein du CSS soit, un responsable de la sécurité de l'information (RSI) et deux (2) coordonnateurs sectoriels de la gestion des incidents (CSGI), ces derniers doivent être désignés par le Centre de services scolaire (ci-après le CSS)

Cette politique permet au CSS des Découvreurs d'accomplir sa mission, de préserver sa réputation, de respecter les lois et de réduire les risques en protégeant l'information qu'elle a créée ou reçue et dont elle est la gardienne. Cette information liée aux ressources humaines, matérielles, technologiques et financières, est accessible sur des formats numériques et non numériques. 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 du CSS et du gouvernement.

2. OBJECTIFS

La présente politique a pour objectif d'affirmer l'engagement du CSS des Découvreurs 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, le CSS 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, le CSS met en place cette politique dans le but d'orienter et de déterminer sa vision qui sera détaillée dans un cadre de gestion de la sécurité de l'information.

3. CADRE LÉGAL ET ADMINISTRATIF

La *Politique relative à la sécurité de l'information* 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) ;
- La *Loi sur les archives* (L.R.Q.A-21.1), incluant le Règlement sur le calendrier de conservation, le versement, le dépôt et l'élimination des archives publiques (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, chap. G-1.03) ;
- 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 (C.T. Décret 7-2014)* ;
- La *Loi sur le droit d'auteur* (LRC, 1985, chapitre C-42) ;
- La *Directive concernant la gestion des documents* (CSDD - 03-13-02) ;
- La *Directive sur le droit d'auteur* (CSDD - 03-03-10) ;
- La *Directive relative à l'utilisation des médias sociaux* (CSDD - 09.13.02) ;
- La *Directive sur l'utilisation des ressources technologiques* (CSDD - 09.13.03).

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 membre du Conseil d'administration, d'élève, de parent, de consultant, de partenaire, de fournisseur, d'organisme externe, de stagiaire, de bénévole, ou de public, utilise les actifs du CSS. Tout utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition par le CSS.

L'information visée est celle que le CSS 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.

5. PRINCIPES DIRECTEURS

Les principes directeurs qui guident les actions du CSS des en matière de sécurité de l'information sont les suivants :

- Reconnaître l'importance de la sécurité de l'information ;
- S'assurer de bien connaître l'information à protéger, en identifier les détenteurs et leurs caractéristiques de sécurité ;
- Reconnaître que l'environnement technologique des actifs de l'information numérique et non numérique est en changement constant et interconnecté avec le monde ;
- Protéger l'information tout au long de son cycle de vie (création, traitement, diffusion, conservation, destruction) ;
- S'assurer que chaque employé ait accès à la seule information requise pour accomplir ses tâches normales ;
- Encadrer l'utilisation des actifs de l'information numérique et non numérique par les utilisateurs en procédant à l'établissement de règles claires qui indiquent ce qui est permis et ce qui ne l'est pas.

6. RÔLES ET RESPONSABILITÉS

Par cette politique et en vertu des principes directeurs énumérés précédemment, le CSS s'attend à ce que chacun assume les rôles et les responsabilités suivants en regard de la sécurité de l'information :

Conseil des commissaires

Le Conseil des commissaires nomme les responsables en sécurité de l'information (RSI et CSGI). Il adopte la *Politique relative à la sécurité de l'information*. Il approuve les modifications apportées à la politique.

Directeur général

Il est le premier répondant de la sécurité de l'information.

Service du secrétariat général et des communications

Le secrétaire général valide la *Politique relative à la sécurité de l'information*. Il prépare les résolutions pour les nominations (RSI ET CSGI) et la politique. Il s'assure de la conformité au cadre législatif.

- Le responsable de la gestion documentaire :
    - S'assure qu'à toutes les étapes du cycle de vie de l'information, les systèmes d'information ont les qualités nécessaires pour permettre une saine gestion des données et le respect des lois ;
    - Collabore étroitement avec les responsables d'actifs informationnels ainsi qu'avec le RSI en vue de mettre en œuvre des mesures de sécurité de l'information indépendamment de son support.
- Le responsable de l'accès à l'information et de la protection des renseignements personnels :
    - Communique au RSI les problématiques et les préoccupations de sécurité en rapport avec la protection des renseignements personnels ou sensibles ;
    - Contribue à assurer la cohérence et l'harmonisation des interventions avec la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels.

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 l'interruption ou la révocation temporaire, lorsque les circonstances l'exigent, des services ou 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.

Responsable de la sécurité de l'information (RSI)

Nommé par le Conseil d'administration, le responsable de la sécurité de l'information a un rôle stratégique et relationnel avec la haute direction. Il communique au CSS les orientations et les priorités en matière de sécurité de l'information et s'assure de l'arrimage et de la participation de tous les intervenants du CSS.

Coordonnateur sectoriel de la gestion des incidents (CSGI)

Nommé par le Conseil d'administration, le coordonnateur sectoriel de la gestion des incidents collabore étroitement avec le COGI-réseau du Ministère (coordonnateur organisationnel de gestion des incidents). Le CSGI du CSS 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 l'organisation auprès du CERT/AQ.

Service des ressources matérielles

Le Service des ressources matérielles participe, avec le RSI, à l'identification des risques traditionnels et des mesures physiques de sécurité permettant de protéger adéquatement les actifs informationnels traditionnels du CSS.

Détenteur de l'information

La direction détenant l'autorité au sein d'un service ou d'un établissement est le détenteur de l'information. Son rôle consiste à veiller à l'accessibilité, à l'utilisation adéquate et à la sécurité des actifs informationnels sous la responsabilité du service ou de l'établissement. Il y a plusieurs détenteurs de l'information dans le CSS. Le détenteur de l'information peut déléguer la totalité ou bien une partie de sa responsabilité à un autre gestionnaire du service ou de l'établissement. Il doit :

- Informer le personnel relevant de son autorité et les tiers avec lesquels transige le service ou l'établissement de la *Politique relative à la sécurité de l'information* et des directives en découlant dans le but de le sensibiliser à la nécessité de s'y conformer ;
- Collaborer activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques ;
- Voir à la protection de l'information et des systèmes d'information sous sa responsabilité et veiller à ce que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la *Politique relative à la sécurité de l'information* ;
- S'assurer 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 voir à ce que tout consultant, fournisseur, partenaire, public, stagiaire, bénévole ou firme externe s'engage à respecter la *Politique relative à la sécurité de l'information ;*
- Rapporter au CSGI toute menace ou tout incident numérique ou traditionnel afférant à la sécurité de l'information ;
- Collaborer 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 ;
- Rapporter au RSI tout problème lié à l'application de la *Politique relative à la sécurité de l'information*, dont toute contravention réelle ou apparente d'un membre du personnel en ce qui a trait à l'application de celle-ci.

Utilisateur

Tout utilisateur doit :

- 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.

- 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 ;
- 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 ;
- 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 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 du CSS des Découvreurs.

7. SANCTIONS

Tout employé du CSS des Découvreurs 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 du CSS).

Les élèves, les parents, les membres du Conseil d'administration, les fournisseurs, les partenaires, les organismes externes, les bénévoles, les consultants, les stagiaires et le public sont passibles de ces sanctions.

8. 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 relative à la sécurité de l'information* sera révisée périodiquement selon les mises à jour effectuées.

9. ENTRÉE EN VIGUEUR

La présente politique est entrée en vigueur dès son adoption par le Conseil des commissaires le 28 mai 2019.

ANNEXE 1

DÉFINITIONS

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 le CSS 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.

1) 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, ordinateur portable et de table, tablettes, téléphone intelligent, etc. L'information sur le média de l'actif numérique peut être écrite, effacée, réécrite, cryptée et copiée.

2) Actif informationnel non numérique

Toute information autre que numérique tels : 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, etc. ;
- 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 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 ont signé.

CERT/AQ

Le CERT/AQ, soit le *Computer Emergency Response Team/Administration Québécoise*, une appellation reconnue internationalement pour les équipes spécialisées en gestion des incidents de sécurité, qui assiste les ministères et les organismes en réduisant les délais d'intervention lors des incidents et en les informant des vulnérabilités et des nouvelles menaces.

Confidentialité

Propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et autorisées et de n'être divulguée qu'à celles-ci.

Document

L'ensemble constitué d'informations portées 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 à une personne autorisée en temps voulu et de la manière requise.

Incident

L'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 du CSS et du gouvernement et nécessitant une intervention concertée au plan gouvernemental.

Information

Le renseignement consigné sur un support quelconque afin d'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

Les moyens concrets assurant partiellement ou totalement la protection d'informations du CSS 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.

Renseignement confidentiel

L'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 dont le consentement de divulgation a été accordé par son détenteur avant de pouvoir être transmise.

Renseignement personnel

L'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 relative à la sécurité de l'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 du CSS.

Risque de sécurité de l'information à portée gouvernementale

Le 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.

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).

Utilisateur

Membre du personnel du CSS des Découvreurs et toute personne physique ou morale qui, à titre d'employé, de commissaire, de consultant, de bénévole, de stagiaire, de partenaire, de fournisseur, d'organisme externe, d'élève, de parent ou de public, utilise un actif informationnel du CSS des Découvreurs.