



**Commission  
scolaire  
de Montréal**

Commission scolaire de Montréal

# Glossaire de la sécurité de l'information et de l'utilisation des technologies

Direction générale de la Commission scolaire de Montréal

*Cette page est laissée vide intentionnellement*

## HISTORIQUE

Auteur	Rôle	Description	Date
André Bachand	Conseiller principal de la SI – Projet SICS	<ul style="list-style-type: none"> <li>• Création</li> </ul>	2017-11-28
André Bachand	Conseiller principal de la SI – Projet SICS	<ul style="list-style-type: none"> <li>• Modif déf pour CSIG, détenteur de l'information, incidents à portée gouvernementale, imputabilité, mesure de sécurité de l'information, renseignement confidentiel et RSI</li> <li>• Retrait déf du responsable de l'actif informationnel</li> </ul>	2018-03-20
Lucie Perreault et comité de sécurité	Directrice du STI Resp. Sécurité de l'information	<ul style="list-style-type: none"> <li>• Adaptation pour la CSDM</li> </ul>	2019-01-14
Guy Nicol	Analyste au STI	<ul style="list-style-type: none"> <li>• Intégration du glossaire de la Directive sur l'utilisation des technologies</li> <li>• Ajouts au glossaire</li> </ul>	2019-03-18 au 2019-03-25
Guy Nicol	Analyste au STI	<ul style="list-style-type: none"> <li>• Uniformisation</li> </ul>	2019-03-26 au 2019-05-02
Guy Nicol Comité de sécurité Geneviève Laurin Sylvie Gallant	Analyste au STI Membres du comité de sécurité Coordonnatrice du bureau des affaires juridiques Secrétaire générale	<ul style="list-style-type: none"> <li>• Révision finale</li> </ul>	2019-05-03 au 2019-06-13

## TABLE DES MATIERES

Historique .....	1
Table des matières .....	2
Actif informationnel .....	5
Actif informationnel numérique.....	5
Actif informationnel non numérique .....	5
Authentification.....	6
Autorisation .....	6
Cadre de gestion.....	6
Catégorisation .....	6
Confidentialité .....	6
Continuité des services.....	6
Coordonnateur sectoriel de la gestion des incidents (CSGI) .....	6
Cybercivisme .....	6
Cyberintimidation.....	7
Cyberflânage.....	7
Cycle de vie de l'information.....	7
Détenteur .....	7
Détenteur de l'information .....	7
Dérogation.....	8
Direction générale.....	8
Directive de sécurité.....	8
Disponibilité.....	8
Document .....	9
Droit d'auteur .....	9
Filtrage Web .....	9
Guide de nomination.....	9
Incident.....	9
Incident de sécurité de l'information à portée gouvernementale.....	9
Information.....	10
Imputabilité .....	10

Infrastructure technologique .....	10
Intégrité .....	10
Intranet.....	10
Internet.....	10
Licence logicielle.....	10
Lien SSL-RPV / Lien RPV / Lien VPN .....	11
Lignes directrices d'utilisation .....	11
Logiciel.....	11
Logiciel libre.....	11
Logiciel propriétaire .....	11
Messagerie numérique.....	11
Mesure de sécurité de l'information.....	11
Mesure compensatoire .....	12
Outil technologique.....	12
Outil technologique personnel.....	12
Pare-feu institutionnel .....	12
Plan de continuité.....	12
Plan de relève .....	12
Registre d'autorité.....	12
Registre d'incident.....	13
Renseignement confidentiel .....	13
Renseignement personnel.....	13
Réseaux sociaux.....	13
Responsable de la sécurité de l'information (RSI).....	13
Risque de sécurité de l'information .....	13
Risque de sécurité de l'information à portée gouvernementale .....	14
Secrétariat général .....	14
Sécurité de l'information (SI) .....	14
Serveur .....	14
Service des ressources humaines* .....	14
Service des ressources matérielles (SRM) .....	14

Service des technologies de l'information (STI) .....	15
Système d'information .....	15
Technologie de l'information .....	15
Utilisateur ou utilisatrice .....	15
Utilisateur interne .....	16
Utilisateur externe.....	16
Téléchargement.....	16
Traçabilité.....	16

# Définitions :

## ACTIF INFORMATIONNEL

Tout actif sur lequel repose des données numériques ou non numériques.

**Exemples** : Base de données sur un serveur, un document papier dans un classeur.

Information, banque d'information, système ou support d'information, document, technologie de l'information, installation ou ensemble de ces éléments acquis ou constitués par la CSDM qui peuvent être accessibles 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 accessibles par un dispositif plus traditionnel tel une filière ou un classeur.

Cela inclut l'information ainsi que les supports tangibles ou intangibles permettant son traitement, sa transmission ou sa conservation aux fins d'utilisation prévue (ordinateurs fixes ou portables, tablettes électroniques, téléphones intelligents, etc.) de même que l'information fixée sur un support analogique, dont le papier.

### Actif informationnel numérique

Toute information stockée dans un format numérique sur un de ces médias : disque, base de données, disquette, ruban magnétique, cassette, clé USB, mémoire flash, vidéo, photo numérique, ordinateur portable, ordinateur de table, tablettes, téléphone intelligent, etc.

L'information sur le média de l'actif numérique peut être écrite, effacée, réécrite, cryptée et copiée.

### Actif informationnel non numérique

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

- L'information sur le média de l'actif non numérique, une fois produite, ne peut être effacée, réécrite, cryptée et copiée.
- Les actifs non numériques peuvent se retrouver dans une pièce, sur un mur, dans un classeur, dans une valise, dans un sac à dos, etc.
- Les actifs non numériques peuvent être facilement déplacés.
- Les actifs non numériques peuvent être produits en plusieurs copies et être à plus d'un endroit.
- Le suivi à la trace des actifs non numériques est ardu.
- Un actif non numérique qui est numérisé est considéré comme un actif numérique.
- L'information d'un actif non numérique peut varier d'une copie à une autre. Ex. : un plan d'intervention d'un élève peut être numérisé une première fois et ensuite numérisé une seconde fois quand tous les intervenants impliqués l'ont signé.

## AUTHENTIFICATION

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

## AUTORISATION

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

## CADRE DE GESTION

Ensemble des consignes, politiques, règlements, directives, procédures, bonnes pratiques reconnues, comités qui encadrent les activités d'une organisation telle une commission scolaire.

## CATÉGORISATION

Processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant son degré de sensibilité en matière de disponibilité, d'intégrité et de confidentialité et, par conséquent, le niveau adéquat de protection à lui accorder.

## CONFIDENTIALITÉ

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

## CONTINUITÉ DES SERVICES

Capacité d'une organisation d'assurer, en cas de sinistre, la poursuite de ses processus d'affaires selon un niveau de service prédéfini.

## COORDONNATEUR SECTORIEL DE LA GESTION DES INCIDENTS (CSGI)

Personne nommée par le Conseil des Commissaires pour collaborer étroitement avec le COGI-réseau du MEES. Le CSGI 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 la CSDM auprès du CERT/AQ.

Voir le **Guide de nomination** pour plus d'information.

## CYBERCIVISME

Respect d'un utilisateur envers la collectivité dans laquelle il vit et les individus qui composent cette collectivité, comme démontré par ses actes et paroles au sein d'un réseau social ou, de manière plus générale, sur Internet, de même que le respect pour les conventions qui balisent le vivre-ensemble.



## CYBERINTIMIDATION

Action de harceler une personne ou de tenir à son endroit des propos menaçants, haineux, injurieux ou dégradants, qu'ils soient illustrés ou écrits, en recourant à l'Internet ou à un outil technologique, par l'intermédiaire notamment du courriel, du clavardage, de groupes de discussion, de sites Web ou de la messagerie instantanée.

## CYBERFLÂNAGE

Action d'utiliser un outil technologique à des fins qui n'ont rien à voir avec la tâche attendue de la part d'un utilisateur, élève, employé ou autre, au cours de ses heures de travail.

## CYCLE DE VIE DE L'INFORMATION

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

## DÉTENTEUR

Personne qui a la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels de la CSDM.

## DÉTENTEUR DE L'INFORMATION

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

Le détenteur de l'information :

- Doit informer le personnel relevant de son autorité et les tiers avec lesquels transige le service de la **Directive de sécurité de l'information** et des dispositions du cadre de gestion dans le but de le sensibiliser à la nécessité de s'y conformer.
- Doit collaborer activement à la catégorisation de l'information du service sous sa responsabilité et à l'analyse de risques.
- Doit 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 **Directive de sécurité de l'information** et de tout autre élément du cadre de gestion.
- Doit 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, invité, organisme ou firme externe

s'engage à respecter la **Directive de sécurité de l'information** et tout autre élément du cadre de gestion.

- Doit rapporter au CSGI toute menace ou tout incident numérique ou traditionnel afférant à la sécurité de l'information.
- Doit 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.
- Doit rapporter à la direction générale tout problème lié à l'application de la **Directive de sécurité de l'information**, dont toute contravention réelle ou apparente d'un membre du personnel à ce qui a trait à l'application de la **Directive de sécurité de l'information**.

## DÉROGATION

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

## DIRECTION GÉNÉRALE

Groupe dont le dirigeant est le premier responsable de la sécurité de l'information.

La Direction générale :

- Doit désigner les principaux intervenants en sécurité de l'information.
- Doit mettre en œuvre une directive et un cadre de gestion de la sécurité de l'information.
- Doit définir et mettre en place les processus majeurs de sécurité de l'information.
- Doit présenter régulièrement au Ministère un plan d'action et un bilan de sécurité de l'information.
- Doit déclarer au CERT/AQ les incidents de sécurité de l'information à portée gouvernementale.
- Doit déclarer au Ministère les risques de sécurité de l'information à portée gouvernementale.

Voir le **Guide de nomination** pour plus d'information.

## DIRECTIVE DE SÉCURITÉ

Forme abrégée de la **Directive sur la sécurité de l'information à la CSDM**.

La Directive de sécurité est un document officiel de la CSDM concernant les mesures mises en place au sujet de la sécurité de l'information à la CSDM. Ce document décrit les objectifs, le cadre légal et administratif, le champ d'application, les principes directeurs ainsi que les sanctions qui concernent la sécurité de l'information à la CSDM.

## DISPONIBILITÉ

Propriété d'une information d'être accessible en temps voulu et de la manière requise à une personne autorisée.

## DOCUMENT

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.

## DROIT D'AUTEUR

Droit exclusif de produire ou de reproduire une œuvre ou une partie importante de celle-ci, sous une forme matérielle quelconque, de la représenter en public, de la publier, de permettre l'un des actes ci-dessus énumérés ainsi que tous les droits accessoires y afférents, le tout tel que défini par la Loi sur le droit d'auteur.

## FILTRAGE WEB

Activité réalisée par le pare-feu institutionnel, par un serveur ou par un autre dispositif et permettant de bloquer l'accès à certaines ressources d'Internet à partir du réseau interne de la CSDM.

## GUIDE DE NOMINATION

Document utilisé avec la **Directive de sécurité** ainsi qu'avec le **Cadre de gestion de la sécurité de l'information et de l'utilisation des technologies** pour permettre de comprendre les rôles et les compétences requises afin d'identifier et de nommer des responsables pour les rôles de **Coordonnateur sectoriel de la gestion des incidents (CSGI)** et de **Responsable de la sécurité de l'information (RSI)**.

## INCIDENT

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, par exemple en causant 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 au bien-être des personnes, à l'atteinte à la protection des renseignements personnels et à la vie privée, à la prestation de services à la population ou à l'image de la CSDM et du gouvernement et nécessitant une intervention concertée au plan gouvernemental.

## INFORMATION

Renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme élément de connaissance.

## IMPUTABILITÉ

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

## INFRASTRUCTURE TECHNOLOGIQUE

Ensemble des dispositifs mis à la disposition des utilisateurs par la CSDM permettant à des outils technologiques d'accéder à des données ou à des services, notamment :

- Serveurs hébergés à la CSDM
- Serveurs hébergés à l'extérieur de la CSDM et utilisés dans le cadre des activités d'un utilisateur à la CSDM (Infonuagique)
- Équipements de routage et de commutation
- Réseau interne de la CSDM
- Bornes sans fil (wifi)
- Internet

## INTÉGRITÉ

Propriété d'une information de ne subir aucune altération ni destruction sans autorisation ou de façon erronée. L'information doit être conservée sur un support et doit être préservée avec des moyens lui procurant stabilité et pérennité.

L'intégrité fait référence à l'exactitude et à la complétude.

## INTRANET

Ensemble des éléments de l'infrastructure technologique dont la CSDM est propriétaire et qui sont réservés aux seuls utilisateurs internes, incluant les équipements, les applications et les systèmes qui ne sont disponibles qu'à partir de l'intérieur de la CSDM ou par lien SSL-RPV.

## INTERNET

Réseau informatique mondial, également désigné sous l'épithète Web, WWW ou World Wide Web, composé de millions de réseaux aussi bien publics que privés et permettant l'accès à un ensemble d'applications et de services offerts par l'entremise des serveurs qui y sont raccordés.

## LICENCE LOGICIELLE

Contrat par lequel le propriétaire des droits du logiciel autorise un utilisateur à poser les gestes suivants selon des termes prescrits : installer le logiciel, l'utiliser, faire une copie de sauvegarde. La licence logicielle définit les droits d'utilisation pour un logiciel propriétaire ou libre.

## LIEN SSL-RPV / LIEN RPV / LIEN VPN

Type de connexion cryptée permettant un accès sécurisé à l'intranet à partir d'un outil technologique situé à l'extérieur du réseau interne de la CSDM. L'acronyme SSL réfère au protocole de cryptage des données (*Secure Socket Layer*), alors que l'acronyme RPV, peu utilisé en informatique sous sa forme française, représente l'expression « réseau privé virtuel ». L'acronyme habituellement reconnu pour désigner ce type de connexion est VPN, pour *Virtual Private Network*.

## LIGNES DIRECTRICES D'UTILISATION

Forme abrégée des **Lignes directrices sur l'utilisation des technologies à la CSDM**. Les Lignes directrices d'utilisation est un document officiel de la CSDM concernant les mesures mises en place au sujet de l'utilisation des technologies à la CSDM. Ce document décrit la nature, le champ d'application, les principes directeurs ainsi que les droits, responsabilités et obligations des utilisateurs et des divers intervenants en ce qui concerne l'utilisation des technologies à la CSDM.

## LOGICIEL

Ensemble d'informations relatives à des traitements effectués automatiquement par un outil technologique et stockées sous forme d'un ensemble de fichiers dans une mémoire, un disque dur ou un média prévu à cette fin; un logiciel est généralement destiné à assister un utilisateur dans une de ses activités, d'où le synonyme d'application souvent utilisé pour désigner un logiciel requis pour l'exécution d'une tâche donnée (traitement de texte, production de la paie, jeu ou autre).

### Logiciel libre

Logiciel dont l'utilisation, l'étude, la modification et la duplication en vue de sa diffusion sont permises, techniquement et légalement, sans frais.

### Logiciel propriétaire

Logiciel dont l'utilisation, l'étude, la modification et la duplication en vue de sa diffusion sont régies par une licence logicielle qui doit être acquise et généralement achetée.

## MESSAGERIE NUMÉRIQUE

Toute forme de système conçu pour la communication entre utilisateurs, notamment les systèmes suivants : courriel, messagerie texte, téléphonie IP, visioconférence ou clavardage.

## MESURE DE SÉCURITÉ DE L'INFORMATION

Moyen concret assurant partiellement ou totalement la protection d'information contre un ou plusieurs risques (panne majeure du réseau informatique ou des serveurs, acte involontaire, acte malveillant tel intrusion, divulgation ou vol de documents, etc.). La mise en œuvre de cette

mesure vise à amoindrir la probabilité d'apparition de ces risques ou à réduire les pertes qui en résultent.

#### MESURE COMPENSATOIRE

Moyen concret permettant de diminuer la probabilité de matérialisation d'un risque découlant d'une non-conformité à la Directive de sécurité.

#### OUTIL TECHNOLOGIQUE

Tout dispositif exploité par un utilisateur comportant des composantes électroniques et lui permettant d'accomplir une activité donnée, notamment les suivants :

- Ordinateur de table ou portable
- Tablette numérique
- Téléphone cellulaire
- Téléphone IP
- Tableau numérique interactif/Écran interactif et autres périphériques d'entrée de données
- Imprimante et autres outils permettant la reproduction de données
- Tout autre outil permettant un lien à Internet

#### Outil technologique personnel

Tout outil technologique appartenant en propre à l'utilisateur et permettant un accès à Internet ou à un élément de l'infrastructure technologique de la CSDM.

#### PARE-FEU INSTITUTIONNEL

Point de démarcation entre l'intranet et Internet, le pare-feu institutionnel protège le caractère privé de l'intranet tout en permettant aux utilisateurs liés au réseau interne de la CSDM d'avoir accès à Internet selon des règles de sécurité.

#### PLAN DE CONTINUITÉ

Ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité de la CSDM.

#### PLAN DE RELÈVE

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

#### REGISTRE D'AUTORITÉ

Répertoire, recueil ou 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

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

Renseignement ou 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 sur la protection des renseignements personnels**. Le consentement du détenteur de l'information doit être obtenu avant de pouvoir divulguer ce renseignement à qui ce soit.

#### RENSEIGNEMENT PERSONNEL

Information concernant une personne physique et qui permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré comme un renseignement personnel aux fins de la politique de la sécurité de l'information.

#### RÉSEAUX SOCIAUX

Ensemble de personnes réunies virtuellement par un lien social. Sur Internet, un réseau social est un média permettant à un utilisateur de publier des données (vidéos, musique, textes, photographies et autres messages) à l'intention des interlocuteurs de son choix ou publiquement. L'utilisateur peut également voir des données qui lui sont destinées ou pour lesquelles il dispose de droits d'accès. Les réseaux sociaux sur le Web visent à faciliter l'interaction, la collaboration ainsi que le partage et la diffusion de contenus entre utilisateurs.

#### RESPONSABLE DE LA SÉCURITÉ DE L'INFORMATION (RSI)

Personne nommée par le Conseil des Commissaires pour occuper un rôle stratégique et relationnel avec la haute direction. Le RSI communique à la CSDM 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 de la CSDM.

Voir le **Guide de nomination** pour plus d'information.

#### RISQUE DE SÉCURITÉ DE L'INFORMATION

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.

Un risque de sécurité de l'information peut avoir des conséquences sur la prestation des services, sur la vie, la santé ou le bien-être des personnes, sur le respect de leurs droits

fondamentaux à la protection des renseignements personnels et au respect de leur vie privée, ou sur l'image de la CSDM.

### 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. Ce risque 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 leurs renseignements personnels et au respect de leur vie privée, sur l'image du gouvernement ou sur la prestation de services fournie par d'autres organismes publics.

## SECRÉTARIAT GÉNÉRAL

Le Service du secrétariat général s'assure de l'adoption de la **Directive de sécurité** par le Conseil des commissaires et la publie sur le site Web de la CSDM.

## SÉCURITÉ DE L'INFORMATION (SI)

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

Le terme sécurité fait autant référence à la cybersécurité qu'à la sécurité de l'information.

## SERVEUR

Dispositif informatique qui offre des services à différents clients, par exemple le partage de fichiers, l'accès aux informations sur Internet, le courrier électronique, le partage d'imprimantes, le commerce électronique, le stockage en base de données, le jeu ou la mise à disposition d'applications.

## SERVICE DES RESSOURCES HUMAINES\*

Service qui s'assure que tout nouvel employé de la CSDM soit avisé de la **Directive de sécurité** et de la **Directive d'utilisation** et obtient du nouvel employé son engagement au respect de ces Directives.

*\*Note : À la CSDM, le Service de la gestion des personnes et du développement des compétences (SGPDC) correspond au Service des ressources humaines.*

## SERVICE DES RESSOURCES MATÉRIELLES (SRM)

Service qui participe, avec le CSGI et le RSI, à l'identification des risques traditionnels et des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels traditionnels de la CSDM.





## SERVICE DES TECHNOLOGIES DE L'INFORMATION (STI)

Service qui 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 élabore une stratégie concernant la sécurité de l'information et l'utilisation des technologies à la CSDM.
- Il participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre et à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information.
- Il applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information, tel que par exemple l'interruption ou la révocation temporaire – lorsque les circonstances l'exigent – des services d'un système d'information faisant appel aux technologies de l'information, et ce, en vue d'assurer la sécurité de l'information en cause.
- Il participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la Directive de sécurité et autorisées par la direction générale.
- Il met en place une structure permettant l'évaluation régulière de sa stratégie de sécurité et d'utilisation et effectue les corrections nécessaires à son bon fonctionnement.

## SYSTÈME D'INFORMATION

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, 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 OU UTILISATRICE

Toute personne, employé, parent ou toute autre personne physique qui accède par le truchement des réseaux numériques et non numériques à de l'information que la CSDM détient dans l'accomplissement de sa mission. Les membres du personnel de la CSDM ainsi que les élèves sont les premiers utilisateurs de l'information de la CSDM. Tout utilisateur de ces réseaux doit se conformer aux politiques et aux directives en vigueur dans la CSDM dans le cadre de toutes ses activités lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

Quiconque utilise un outil technologique fourni par la CSDM ou une composante de l'infrastructure informatique de la CSDM et ayant un lien fonctionnel avec la CSDM, notamment les personnes suivantes :

- Membres du personnel
- Élèves jeunes et adultes
- Parents
- Membres du Conseil des commissaires
- Bénévoles
- Stagiaires
- Consultants
- Employés contractuels
- Sous-traitants
- Organismes externes

### Utilisateur interne

Utilisateur disposant d'un code d'identification et d'un mot de passe lui permettant d'utiliser un outil technologique fourni par la CSDM.

### Utilisateur externe

Utilisateur ne disposant pas d'un code d'identification fourni par la CSDM.

## TÉLÉCHARGEMENT

Opération de transmission d'informations — logiciels, données, images, sons, vidéos ou autres — d'un ordinateur à un autre par l'intermédiaire d'un réseau, en général Internet. Le téléchargement inclut ici la réception d'informations à partir d'un ordinateur distant (téléchargement ou download) de même que le téléchargement vers un ordinateur distant (téléversement ou upload).

## TRAÇABILITÉ

Situation où l'on dispose de l'information nécessaire et suffisante pour connaître (éventuellement de façon rétrospective) la composition de l'actif informationnel tout au long de sa chaîne de production, de transformation et de distribution et ce, en quelque endroit que ce soit, depuis son origine première jusqu'à sa fin de vie.