POLITIQUE DE SÉCURITÉ DE L'INFORMATION

Mai 2018

Table des matières

1 PRÉFACE

Afin de mener à bien sa mission, la Commission scolaire des Affluents (CSDA) conserve, traite et communique des informations sous plusieurs formes et supports. Ces informations représentant un actif primordial à la mission de la commission scolaire, elles ont une valeur administrative, économique ou légale connue et mesurée.

Par cette Politique, la CSDA s'engage à protéger la vie privée de ses usagers, employés et partenaires et à assurer la sécurité de l'information qui lui est confiée dans le cadre de ses activités.

En support à l'application de la présente politique, différents cadres de gestion (de la sécurité des données informationnelles, des incidents TI et des risques TI) viennent préciser les moyens et les règles mis en place afin de bien remplir cette mission.

La sécurité des systèmes d''information vise ainsi la protection adéquate des informations, indépendamment du support et de leur forme, durant tout leur cycle de vie, de la création jusqu'à la destruction.

La CSDA désire aussi réduire le risque lié à l'exploitation, le risque stratégique et le risque d'atteinte à la réputation, assurer la continuité de ses activités et préserver la disponibilité, l'intégrité et la confidentialité des différentes composantes de ses systèmes d'information.

La sécurité de l'information résulte également de l'application par la CSDA de différentes normes ou lois, ainsi que de dispositions contractuelles assurant la protection de l'information de ses usagers, employés, partenaires et fournisseurs. Ces normes et lois sont énumérées dans la section « Cadre légal et normatif ».

Plus particulièrement :

- la *Loi sur la protection des renseignements personnels*;
- les règles de contrôle concernant l'intégrité et la divulgation de l'information auxquelles la CSDA est tenue de respecter en tant qu'organisation publique.

Pour toutes ces raisons, la sécurité de l'information devient d'une importance stratégique et fondamentale pour la CSDA.

Le conseil des commissaires, agissant à titre de dirigeant de la CSDA doit adopter une politique portant sur la sécurité de l'information.

2. CONTEXTE D'APPLICATION DE LA POLITIQUE

2.1 OBJET DE LA POLITIQUE

La *Politique de sécurité de l'information* stipule l'engagement de la CSDA au regard de la sécurité de ses systèmes d'information. La CSDA reconnaît les risques et les besoins en ce qui a trait à la sécurité de ses systèmes d'information et entend encourager la gestion responsable de ceux-ci.

De ce fait, la CSDA désire démontrer son engagement à protéger l'ensemble de l'information auprès de ses usagers, de sa clientèle et de ses partenaires.

La présente politique représente la fondation du cadre de gouvernance de la sécurité de l'information et découle des bonnes pratiques. Cette politique vise à encadrer la sécurité de l'information, et ce, afin de :

- ***se conformer aux lois et aux directives en vigueur*** ainsi qu'aux normes et aux standards que la CSDA a choisi de déployer;

- ***mettre en œuvre et faire évoluer les mesures nécessaires*** pour adresser les besoins de sécurité de l'information et supporter la mission de l'organisation.

2.2 OBJECTIFS DE LA SÉCURITÉ DE L'INFORMATION

La sécurité de l'information soutient la réalisation de notre mission. Elle se doit d'entretenir ou même de rehausser la confiance de tous les usagers, clients, employés ou partenaires à l'égard de nos services.

La politique se compose d'éléments cohérents intégrés à l'intérieur d'un cycle d'amélioration continue, c'est-à-dire un cycle révisé et optimisé continuellement. Dans le contexte de la CSDA, les mesures de sécurité doivent être proportionnelles à la valeur de l'information gouvernementale à protéger.

Pour l'ensemble des systèmes d'information, nos mesures de sécurité ont pour objectif d'assurer :

- **la disponibilité :** les systèmes se doivent d'être accessibles aux bonnes personnes, aux bons moments. Ces mesures visent également à prévenir la destruction des données, rendant un système inaccessible;
- **l'intégrité :** afin de prévenir la modification non autorisée, qu'elle soit accidentelle ou intentionnelle;
- **la confidentialité :** les informations des systèmes doivent être utilisées uniquement par les personnes dûment autorisées;
- **l'authentification :** afin de confirmer l'identité d'une personne, d'un document ou d'un périphérique;
- **la non-répudiation :** se protéger contre le déni d'un individu d'admettre sa responsabilité envers toute action, autorisée ou non, qui lui serait attribuée.

Et ce, pour le cycle de vie complet des données.

2.3 PORTÉE DE LA POLITIQUE (USAGERS)

Toute personne détenant un accès à l'actif informationnel de la CSDA ainsi qu'aux biens ou aux lieux pour lesquels la CSDA a la responsabilité d'assurer la sécurité est **visée** par cette politique. Ces usagers regroupent, sans s'y limiter :

- les ***cadres*** et ***administrateurs*** des unités composant la CSDA;
- les ***employés réguliers***;
- les ***représentants liés par contrat*** avec la CSDA;
- les ***sous-traitants***, ***fournisseurs de services***, ***consultants liés par contrat*** avec la CSDA ***ainsi que leurs employés***.

2.4 PORTÉE DE LA POLITIQUE (ACTIFS INFORMATIONNELS)

La *Politique de sécurité de l'information* **s'applique** à l'actif informationnel détenu ou géré par la CSDA.

Cette politique s'applique donc aux informations numériques suivantes :

- les ***informations appartenant à*** la CSDA ***et exploitées par*** la CSDA;
- les ***informations appartenant à*** la CSDA ***et exploitées ou détenues par un tiers*** : partenaire, fournisseur de produits/services ou tout autre intervenant;
- les ***informations appartenant à un tiers*** : partenaire, fournisseur de produits/services ou tout autre intervenant, ***et exploitées par lui au profit de*** la CSDA;

- les ***informations n'appartenant pas à*** la CSDA ***mais qui sont détenues ou exploitées par*** la CSDA.

La *Politique de sécurité de l'information* **S'APPLIQUE** également :

- aux ***actifs informationnels personnels*** utilisés par les employés dans le cadre de leur travail. Les actifs informationnels personnels sont notamment les ordinateurs de bureau ou portables, les imprimantes, les appareils mobiles (tablettes, téléphones intelligents), les logiciels et applications d'affaires, les CD-ROM, les DVD, les clés USB, les copies de sauvegarde, etc.;
- aux ***centres de traitement informatique***, aux salles de télécommunications et de serveurs ainsi qu'aux points de raccordement avec les télécommunicateurs;
- à toutes les activités impliquant la manipulation ou l'utilisation de l'information, peu importe sa forme ou sa valeur, que celles-ci soient conduites dans les locaux de la CSDA ou dans un autre lieu.

2.5 LIMITES ET EXCLUSIONS

La *Politique de sécurité de l'information* **exclut** la sécurité physique des immeubles et des bureaux de l'entreprise.

La CSDA est responsable d'assurer la sécurité physique de l'information non numérique et de l'actif immobilier sous sa responsabilité.

À ce titre, elle doit prévoir des mécanismes de surveillance et d'accès ainsi que des mesures de sécurité physiques contre les principaux risques et dommages connus ou prévisibles.

2.6 RESPONSABILITÉ ET IMPUTABILITÉ

Les gestionnaires détenteurs d'actifs informationnels veillent auprès des membres de leur personnel au respect de la présente politique et de toute mesure en découlant. Chaque utilisateur a l'obligation de protéger les actifs informationnels mis à sa disposition et de les utiliser aux seules fins auxquelles ils sont destinés. La CSDA s'assure que tous les utilisateurs adoptent un comportement éthique et respectueux des lois et règlements encadrant l'utilisation des actifs informationnels et que les rôles et obligations de tous soient connus et compris. Aux fins d'instaurer une culture de sécurité elle met en place des mesures de sensibilisation, de prévention et de formation continue qui s'adressent à tous les utilisateurs pour que ces derniers comprennent et collaborent à la prévention de tout incident de sécurité.

3. CADRE LÉGAL ET ADMINISTRATIF

La présente politique s'inscrit, notamment dans le contexte législatif suivant :

- de *la Loi sur l'instruction publique* – RLRQ, chapitre I-13.3;
- de la *Charte des droits et libertés de la personne* – RLRQ, chapitre C-12;
- du *Code civil du Québec*;
- de la *Loi concernant le cadre juridique des technologies de l'information* – RLRQ, chapitre C-1.1;
- de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* – RLRQ, chapitre A-2.1;
- de la *Loi sur les archives* – RLRQ, chapitre A-21.1;
- de la *Loi sur le droit d'auteur* (L.R. 1985, c. C-42);
- du *Code criminel* (L.R.C., 1985, ch. C-46);

- de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* – RLRQ, chapitre G-1.03;
- de la *Loi renforçant la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement 2017* – LQ, c. 28;
- de la directive sur la sécurité de l'information gouvernementale adoptée par voie du décret 7-2014 du 15 janvier 2014 du Conseil du Trésor;
- du Cadre gouvernemental de gestion en matière de sécurité de l'information.

4 PRINCIPES DIRECTEURS

Les principes directeurs représentent les assises fondamentales sur lesquelles reposent la conception et l'organisation de la sécurité de l'information de la CSDA.

4.1 ATTEINTE DES OBJECTIFS

La sécurité de l'information doit supporter les orientations et permettre l'atteinte des objectifs de la CSDA. Les moyens mis en place doivent donc correspondre aux orientations organisationnelles et servir à la protection des activités touchant les informations de la CSDA.

4.2 MEILLEURES PRATIQUES

Afin d'assurer l'application de bonnes pratiques du marché et d'obtenir des barèmes de comparaison avec des organisations similaires, la CSDA s'appuie sur les normes internationales ISO-27000 et les contrôles de sécurité critiques CIS (*Center for Internet Security*). Ces normes et contrôles proposent les meilleures pratiques en matière de sécurité de l'information.

4.3 CONNAISSANCE ET PROTECTION DES ACTIFS INFORMATIONNELS

La sécurité de l'information vise principalement à protéger **convenablement** les actifs informationnels de la CSDA. Les mesures de sécurité doivent être proportionnelles à la valeur de l'information à protéger et aux risques auxquels la CSDA est exposée.

La CSDA s'assure donc de bien connaître les actifs informationnels à protéger, ainsi que leur valeur.

4.4 GESTION DU RISQUE

La gestion du risque est partie intégrante de la sécurité de l'information. Le choix des mesures de sécurité est fondé sur l'identification et l'appréciation des risques liés à la sécurité de l'information. L'appréciation des risques consiste à évaluer et prioriser les risques relatifs aux activités de la CSDA.

4.5 ÉTHIQUE, LOIS

La CSDA favorise un comportement éthique de la part de tous. Elle adhère et applique les lois et règlements auxquels elle est assujettie et voit à leur respect. Toute personne œuvrant pour la CSDA doit adhérer aux règlements s'y référant (Pratique d'utilisation du réseau de télécommunications de la CSDA – Pratique de gestion du réseau informatique – Médias sociaux, Pratique d'utilisation et d'expression de la CSDA).

4.6 CULTURE DE SÉCURITÉ

L'atteinte des objectifs de sécurité de l'information requiert l'octroi de responsabilités à tous les niveaux de l'organisation et la mise en place d'un processus de gestion permettant une reddition de comptes adéquate, incluant la vérification de la conformité et l'imputabilité des actions posées par tout utilisateur de la CSDA.

Toute personne de la CSDA est responsable d'assurer la sécurité et de prendre les mesures adéquates pour protéger les actifs qu'elle utilise et d'en rendre compte au besoin.

L'humain demeurera toujours la base fondamentale et critique de la sécurité. Conséquemment, la sensibilisation et la formation continue du personnel sont essentielles afin que chaque personne comprenne les impacts d'un incident de sécurité. De plus, les rôles et obligations de tous doivent être connus et compris. La CSDA officialisera et précisera les responsabilités de chacun.

De cet engagement continu émergera une culture de sécurité qui se traduira par le respect des bonnes pratiques dans les faits et gestes quotidiens des utilisateurs.

4.7 RELATIONS AVEC LES TIERCES PARTIES

Seules les personnes identifiées par la CSDA doivent avoir accès à ses informations. Elles s'engagent à se conformer en tout point à la présente Politique de sécurité de l'information.

Toute relation avec un fournisseur ou un partenaire de l'organisation doit être encadrée par des ententes écrites formelles qui incluent un volet sur la sécurité de l'information. Chaque entente définit ainsi l'information échangée autant que les mesures de protection appliquées de part et d'autre. Toute entente qui touche les actifs informationnels doit suivre les orientations de la présente politique.

4.8 TÂCHES INCOMPATIBLES

La séparation des tâches incompatibles consiste à s'assurer que certaines tâches ou fonctions complémentaires sont exécutées par différentes personnes. Elle est nécessaire afin d'atteindre correctement l'ensemble des objectifs de sécurité de la CSDA. Elle permet de prévenir et de détecter des erreurs ou des fraudes, mais aussi d'éviter de placer des personnes dans une situation où elles pourraient les dissimuler.

La séparation des tâches incompatibles doit être un élément clé lors de l'élaboration ou la révision de processus en lien direct ou indirect avec la gestion de la sécurité de l'information.

4.9 ÉVOLUTION DES MESURES

Les mesures de sécurité de l'information de la CSDA doivent être réévaluées périodiquement afin de refléter les changements technologiques, juridiques ou organisationnels, ainsi que l'évolution des menaces et des risques.

5 ÉNONCÉS DE SÉCURITÉ

Les énoncés de sécurité représentent les pratiques et orientations que la CSDA met de l'avant pour encadrer, mettre en œuvre, suivre et améliorer sa gestion de la sécurité de l'information.

5.1 CATÉGORISATION DE L'ACTIF INFORMATIONNEL

La CSDA possède plusieurs systèmes d'information supportant les actifs informationnels et les processus d'affaires.

Pour cette raison, l'ensemble des systèmes d'information ont fait l'objet d'une catégorisation de leurs actifs. Cette catégorisation permet d'évaluer la valeur des actifs et, conséquemment, de justifier les mesures de sécurité devant être appliquées afin de fournir le niveau de sécurité adéquat.

5.2 PROTECTION DES ACTIFS INFORMATIONNELS TOUT AU LONG DE LEUR CYCLE DE VIE

Les actifs informationnels de la CSDA sont indispensables à la réalisation de ses opérations critiques. De ce fait, la disponibilité, l'intégrité et la confidentialité de ces actifs doivent être protégés durant l'entièreté de leur cycle de vie.

Le cycle de vie des données inclut l'ensemble des phases que traversent les actifs informationnels : création des environnements de développement et des données, distribution des données, utilisation ou maintenance, archivage et destruction des données.

Les mesures de sécurité doivent être proportionnelles à la valeur de l'information à protéger et aux risques auxquels elle est exposée.

Les actifs de la CSDA sont inventoriés, catégorisés et ont un propriétaire, ce derniers étant le plus souvent un directeur d'unité administrative.

Les accès à l'information, aux systèmes et aux applications de la CSDA sont octroyés selon le besoin de savoir, le besoin d'utiliser et le privilège minimum possible.

5.3 PROTECTION DE LA PROPRIÉTÉ INTELLECTUELLE

La CSDA se conforme aux exigences légales en regard des droits de propriété intellectuelle.

Ainsi, tout utilisateur de l'actif informationnel doit voir au respect du droit de propriété intellectuelle qui s'y rattache en s'assurant notamment que les fichiers, logiciels ou systèmes d'exploitation sont utilisés conformément aux exigences légales.

5.4 PROTECTION DES ACTIFS CONFIDENTIELS

Le degré de sensibilité de l'actif informationnel influence les mesures de sécurité de l'information à mettre en place. De façon générale, plus un actif détient un niveau de catégorisation élevé, plus l'actif doit être sécurisé à l'aide de contrôles et de mesures. Les actifs classés confidentiels ou ayant une valeur gouvernementale élevée feront l'objet d'une attention particulière.

5.6 PROTECTION DE L'INTÉGRITÉ ET DE LA VALEUR JURIDIQUE

La CSDA doit maintenir l'intégrité de tout document servant à l'établissement de la preuve d'un acte juridique afin de préserver son admissibilité éventuelle devant les tribunaux.

À cette fin, les processus, procédés et mécanismes qui encadrent la copie, le classement, la saisie, la transmission ou le transfert de support d'un document doivent assurer le maintien de son intégrité et, conséquemment, de sa valeur probante.

5.7 USAGE DES RESSOURCES INFORMATIQUES

Afin de contribuer à la protection des actifs informationnels de la CSDA, toute personne doit en faire une utilisation de manière acceptable et aux seules fins prévues.

Lorsqu'elle est autorisée par un gestionnaire, l'utilisation des ressources informatiques à des fins personnelles est permise, conditionnellement à ce que l'utilisation ne présente pas de nuisance à la productivité et respecte les règlements et pratiques existants.

5.8 GESTION DES INCIDENTS DE SÉCURITÉ

Tous les individus dans la portée de la politique doivent impérativement, et sans délai, alerter le Service des TI, à l'adresse **securite.ti@csda.ca** lors de l'observation et la détection de tout événement ou action pouvant représenter un manquement ou une infraction des règles de sécurité informatique, que cette action s'avère concrète et authentique ou simplement hypothétique.

Un processus de gestion des incidents de sécurité doit exister afin de supporter l'ensemble des individus et des actions à prendre dans la gestion de l'incident. Les différents niveaux de gravité doivent être inclus dans ce processus de gestion.

5.9 GESTION DES RISQUES

Les mesures de sécurité à appliquer dans le contexte de la CSDA devront évoluer et être déterminées selon une évaluation régulière des risques liés à la sécurité de l'information. L'évaluation des risques doit donc être une activité incluse dès les premiers stades de tout projet affectant les actifs informationnels.

La gestion des risques s'effectue selon les étapes suivantes :

- **identification et catégorisation des actifs**;
- **évaluation des risques :** évaluer l'exposition aux menaces et leurs impacts (pertes financières, dommages matériels, atteintes à la réputation, pertes de productivité et problèmes juridiques);
- **évaluation des mesures de mitigation :** les efforts à mettre en œuvre afin de réduire les risques, de transférer les risques à un tiers ou d'accepter le risque. Le coût des mesures à mettre en place ne devrait jamais être supérieur à la valeur de l'actif à protéger;
- **prise en charge du risque** – la criticité du risque résiduel dicte le portrait des mesures de sécurité à mettre en place. Si le risque résiduel est raisonnable, il peut être accepté (géré) sans mesure de sécurité additionnelle.

5.10 PLAN DE CONTINUITÉ D'ACTIVITÉ

Dans le but d'assurer la disponibilité des services critiques, la CSDA a mis en place un plan de continuité d'activité afin de minimiser les impacts d'une crise ou d'une catastrophe naturelle, sociale ou technologique. Ce plan couvre différents scénarios permettant notamment de se préparer à la non-disponibilité des actifs informationnels ou du personnel.

Le plan de continuité n'est jamais définitif ; il se doit d'évoluer et d'être adapté non seulement au contexte et à l'environnement changeants, mais aussi à l'analyse des retours d'information suite à des exercices de simulation.

5.11 DROIT DE REGARD ET D'INTERVENTION

Pour garantir la sécurité de ses actifs informationnels, la CSDA se réserve un droit de regard et d'intervention sur toute activité susceptible d'affecter ses actifs. Les accès aux actifs informationnels, réussis ou refusés, sont surveillés et journalisés afin de permettre de futures vérifications.

Des enquêtes sur les actions d'un individu peuvent être enclenchées si une demande est justifiée et approuvée par un gestionnaire supérieur. Le Service des ressources humaines est responsable de l'ouverture d'une enquête.

Ce droit de regard est exercé conformément au cadre légal et normatif applicable et au respect de la vie privée.

6 PRINCIPAUX RÔLES ET RESPONSABILITÉS DE SÉCURITÉ

Le directeur du service des technologies de l'information ou la personne qu'il désigne ou qu'il s'adjoint

- est responsable de la diffusion et de l'application de la présente politique;
- assiste le conseil des commissaires et la direction générale dans la détermination des orientations stratégiques et des priorités d'intervention en matière de sécurité informatiques des données informationnelles.

Le conseil des commissaires

- est le dirigeant de la Commission scolaire au sens de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement RLRQ chapitre G-1.03;
- adopte la présente politique;
- désigne les détenteurs de l'information qui sont les directeurs d'unités administratives ;
- désigne directement ou par délégation de pouvoir à la direction générale le Responsable de la sécurité de l'information (RSI), le Coordonnateur sectoriel de la gestion des incidents (CSGI) et son substitut.

La direction générale

- est le premier répondant de la sécurité à la CSDA et à ce titre est informé de toute alerte ou incident;
- autorise la vérification des données personnelles d'un utilisateur, reçoit les résultats des analyses de risque et détermine si un risque peut être pris en charge, il institue et préside le comité de gestion des incidents.

Le secrétaire général

- est responsable de l'accès aux documents et de la protection des renseignements personnels;
- valide les ententes de transmission et d'échanges de renseignements avec un partenaire.

Le directeur du service des ressources humaines

- autorise la vérification des données personnelles d'un utilisateur.

Les directions des unités administratives

- sont désignées détenteurs de l'information et à ce titre, collabore conjointement avec le Service des technologies de l'information, à la catégorisation des actifs informationnels dont elles sont réputés détenteurs et responsables selon les dispositions de la présente politique prévues à cet effet;
- s'assurent du respect de la politique et veillent notamment à ce que les mesures de sécurité et de protection des soient mises en place et appliquées au sein de leur unité administrative.

L'utilisateur

- doit se conformer aux différentes pratiques, politiques, directives, lignes directrices et autres règles de l'organisation lors de l'utilisation des actifs informationnels, équipements, systèmes et réseaux et de toute fonctionnalité.

7. DISPOSITIONS FINALES

7.1 SANCTIONS

Toute violation de la *Politique de sécurité de l'information* sera considérée comme une faute qui pourrait se traduire par le retrait de privilèges, des pénalités, des mesures disciplinaires pouvant mener au congédiement, voire des poursuites civiles et criminelles. Toute sanction imposée à un individu sera proportionnelle à la gravité des actes posés.

7.2 DIFFUSION

La présente politique doit être diffusée à l'ensemble de la CSDA, sous la présente forme ou sous une forme abrégée incluant l'ensemble des points de la politique.

Une version électronique de la politique doit être publiée et rendue disponible. La version électronique sera toujours considérée comme la version à jour. Elle est disponible à l'adresse suivante http://csaffluents.qc.ca, sous l'onglet Commission scolaire, Centre de documentation, Politiques.

7.3 MISE EN ŒUVRE, SUIVI ET RÉVISION

La coordination de la mise en œuvre de la *Politique de sécurité de l'information* ainsi que la mise à jour de ce document relèvent du directeur des technologies de l'Information.

Afin d'assurer son adéquation aux besoins de la sécurité de l'information, la présente politique doit être révisée annuellement après son entrée en vigueur ou lors de changements significatifs.

7.4 DÉROGATIONS

Aucune dérogation à la présente politique n'est permise sans l'autorisation écrite ou électronique de la Direction générale.

Généralement, une dérogation est permise suite à la production d'un avis de sécurité obtenu auprès du responsable de la politique de sécurité opérationnelle ou de son représentant.

7.5 APPROBATION ET DATE D'ENTRÉE EN VIGUEUR

La *Politique de sécurité de l'information* est approuvée par le Conseil des commissaires et entre en vigueur à la date d'approbation, le 22 mai 2018.

8. DÉFINITIONS

Actif informationnel

Une information numérique, une banque d'informations numériques, un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitué par une organisation.

Confidentialité

Propriété d'une information qui doit être utilisée seulement par les personnes dûment autorisées.

Continuité

Propriété qu'ont les ressources informationnelles d'être accessibles de la manière requise (sans interruption, délai ou dégradation) et utilisables au moment voulu.

Courriel

Service de correspondance sous forme d'échange de messages électroniques à travers un réseau de télécommunications.

Cycle de vie de l'information numérique

Période de temps couvrant toutes les étapes d'existence de l'information numérique dont celles de la définition, de la création, de l'enregistrement, du traitement, de la diffusion, de la conservation et de la destruction de cette information.

Détenteur d'actifs informationnels

La direction des unités administratives de la Commission à qui est assignée la responsabilité de la sécurité d'un actif informationnel et/ou d'un processus d'affaires.

Disponibilité

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

Équipement informatique

Tout équipement de lecture, d'emmagasinage, de reproduction, d'impression, de transmission, de réception et de traitement de l'information et tout équipement de télécommunication.

Fichier

Collection d'informations consignées et stockées comme une entité unique et spécifique sur un support de stockage.

Habilitation

Fonction permettant d'attribuer à un utilisateur l'autorisation de porter des actions sur les ressources.

Information numérique

Information dont l'usage n'est possible qu'au moyen d'une technologie informatique.

Inforoute

Réseau étendu d'information à haut débit et à grande vitesse, capable de transmettre des données de toutes sortes, notamment des données multimédias, et destiné à jouer le rôle d'infrastructure globale de communication au service de l'ensemble des populations, sur les plans national et international.

Intégrité

Propriété d'une information ou d'une technologie de l'information de n'être ni modifiée, ni détruite sans autorisation. L'intégrité fait référence à l'exactitude ou à l'état complet de l'information.

Irrévocabilité

Propriété d'une action ou d'un document d'être indéniable et clairement attribué à son auteur ou au dispositif qui l'a généré.

Mesure de sécurité

Moyen organisationnel, technologique, humain ou juridique permettant d'assurer la réalisation des objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des dispositifs et des personnes et de l'irrévocabilité des actions qu'elles posent.

Renseignement de nature confidentielle

Renseignement qui ne doit pas être divulgué à des personnes non autorisées comme l'indiquent des dispositions de la Loi sur l'accès aux documents des organismes publics et la protection des renseignements personnels.

Renseignement personnel ou nominatif

Renseignement qui concerne une personne physique et qui permet de l'identifier.

Sécurité de l'information

Assurance, par un ensemble de mesures de sécurité, de rencontrer les objectifs de disponibilité, d'intégrité et de confidentialité de l'information ainsi que d'authentification des dispositifs et des personnes et de l'irrévocabilité des actions qu'elles posent.

Système d'information

Système constitué de l'équipement, des procédures, des ressources humaines, ainsi que des données qui y sont traitées, et dont le but est de fournir de l'information.

Technologie de l'information

Tout logiciel, matériel électronique ou combinaison de ces éléments utilisé pour recueillir, emmagasiner, traiter, communiquer, reproduire, protéger ou éliminer de l'information numérique.

Utilisateur

Toute personne de la commission, quels que soient sa catégorie d'emploi et son statut d'employé, ayant accès à l'actif informationnel, ainsi que toute personne morale ou physique qui, par engagement contractuel ou autrement, accède à l'actif informationnel d'un ministère ou organisme.