Cégep de Sainte-Foy

5.23

POLITIQUE SUR LA SÉCURITÉ DE L'INFORMATION

Présentée au conseil d'administration le 23 avril 2018

PRÉAMBULE

Dans l'accomplissement de sa mission, le Cégep de Sainte-Foy traite de l'information, en reçoit et en transmet sous plusieurs formes et sur plusieurs supports à l'aide de différents systèmes d'information. L'information comprend des renseignements personnels d'étudiants et de membres du personnel, de l'information professionnelle sujette à des droits de propriétés intellectuelles et de l'information stratégique ou opérationnelle pour l'administration du Cégep. Cette information qui soutient les diverses activités possède une valeur administrative, légale, financière ou patrimoniale et doit, par conséquent, faire l'objet d'une évaluation continue, d'une utilisation appropriée et d'une protection adéquate tout au long de son cycle de vie par toutes les catégories d'usagers. Ainsi, cette politique encadre la mise en œuvre d'un ensemble cohérent de mesures relatives à l'utilisation de l'information et à son traitement sécuritaire, déterminé par une approche de gestion des risques.

Dans ce contexte, l'entrée en vigueur de la *Loi sur la gouvernance des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q., c. G-1.03) et de la *Directive sur la sécurité de l'information gouvernementale* (une directive du Conseil du trésor du Québec) crée des obligations aux cégeps en leur qualité d'organismes publics. L'adoption, la mise en œuvre, l'application et la mise à jour de la Politique sur la sécurité de l'information permet au Cégep de remplir ses obligations. En outre, la Politique établit les orientations relatives au cadre de gestion de la sécurité.

1. OBJECTIF

La présente politique a pour objectif d'assurer la sécurité de l'information traitée par le Cégep tout au long de son cycle de vie, de sa conception, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission jusqu'à sa conservation ou sa destruction. Plus précisément, elle permet de s'assurer de :

- 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 soit conservée selon les normes en vigueur, 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, notamment celle constituant des renseignements personnels.

La Politique soutient la mise en œuvre du cadre de gestion en matière de sécurité de l'information et renforce le maintien de systèmes de contrôles internes offrant une assurance raisonnable de conformité à l'égard des lois, directives et pratiques gouvernementales en la matière.

2. CADRE LÉGAL ET ADMINISTRATIF

La Politique sur la sécurité de l'information s'inscrit notamment dans un contexte régi par :

- le Cadre gouvernemental de gestion de la sécurité de l'information (juin 2014);
- la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (L.R.Q., c. G-1.03);
- la Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1);
- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1);

- la Loi sur le droit d'auteur (L.C., 1985, c. C-42);
- la Loi sur les archives (L.R.Q. c. A-21.1);
- la Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics (Décret no 261-2012 du 28 mars 2012);
- la Directive sur la sécurité de l'information gouvernementale (Décret 7-2014 du 15 janvier 2014).

3. CHAMP D'APPLICATION

L'information et les actifs informationnels visés par la Politique, quels qu'en soient les supports, incluant le papier, sont ceux :

- appartenant au Cégep et détenus par lui;
- appartenant au Cégep, mais détenus par un tiers;
- utilisés par un tiers et détenus par lui au bénéfice ou pour et au nom du Cégep.

Les usagers visés par la Politique sont :

- les personnes à l'emploi du Cégep;
- les étudiants du Cégep;
- toute entité externe autorisée à accéder, à exploiter ou à héberger l'information et les actifs informationnels du Cégep.

Les activités visées par la Politique sont la collecte, la consultation, la production, la transmission, la conservation et la destruction de l'information et des actifs informationnels, peu importe leur support, leur emplacement et le moyen de communication.

4. PRINCIPES DIRECTEURS

Les principes directeurs suivants guident les actions du Cégep en matière de sécurité de l'information :

Connaissance de l'information et de sa sécurité

Les membres de la communauté collégiale ont la responsabilité individuelle de se tenir informés sur l'information à protéger, sur les risques potentiels ainsi que sur les règles de sécurité à respecter, à diffuser et à appliquer. Les instances responsables s'assurent d'informer, de sensibiliser et d'outiller les membres de la communauté quant aux bonnes pratiques de protection de l'information dans le respect des normes internationales, notamment en ce qui concerne les renseignements personnels, en visant la régulation des conduites et la responsabilisation personnelle.

Mesures de sécurité et imputabilité

Le Cégep met en place les mesures de protection, de détection, de prévention et de correction, et il s'assure de l'engagement à l'égard de la Politique des organismes avec lesquels des ententes contractuelles sont convenues. Ces mesures permettent d'assurer la disponibilité, la confidentialité et l'intégrité de l'information ainsi que la continuité des services à rendre. De même, elles couvrent la protection de l'information, la détection de tout usage abusif ou inapproprié de l'information et le traitement des menaces. Elles doivent être reconnues, tenir compte des différents changements qui surviennent ou de l'évolution du contexte et prévoir le recouvrement des services lorsque nécessaire.

Les accès à l'information

Le Cégep donne aux membres du personnel et aux étudiants les accès nécessaires à l'accomplissement des tâches qui leur sont confiées ou à leur cheminement scolaire. Pour les membres du personnel, il revient au supérieur immédiat d'identifier les besoins et de donner l'autorisation exécutée par la Direction des systèmes et des technologies de l'information avec la confirmation du pilote de système. En ce qui concerne les étudiants, le Service du cheminement scolaire de la Direction des études confirme à la Direction des systèmes et des technologies de l'information le statut d'étudiant, ce qui constitue l'autorisation donnant les accès nécessaires à l'étudiant.

5. CADRE DE GESTION

L'efficacité des mesures de sécurité de l'information exige l'attribution claire de rôles et de responsabilités aux différents intervenants du Cégep par la mise en place d'un cadre de gestion de la sécurité permettant notamment une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des menaces et des risques.

La Politique sur la sécurité de l'information établit les orientations concernant les trois axes fondamentaux de gestion, soit la gestion des accès, la gestion des risques et la gestion des incidents.

Des directives découlent de cette politique afin de préciser les comportements attendus en matière de sécurité de l'information.

5.1 GESTION DES ACCÈS

La sécurité de l'information est assurée par des mesures d'encadrement et un contrôle adéquat de l'accès, de la divulgation et de l'utilisation de l'information par les personnes autorisées afin d'en protéger la confidentialité et l'intégrité, en portant une attention particulière à l'information confidentielle et aux renseignements personnels.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités et une imputabilité des usagers, à tous les niveaux de personnel du Cégep.

5.2 GESTION DES RISQUES

Une catégorisation de l'information à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement du Cégep. La gestion des risques reliés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques du Cégep. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Le niveau de protection de l'information est établi en fonction :

- de la nature de l'information et de son importance;
- des probabilités d'occurrence d'accident, d'erreur et de malveillance auxquelles elle est exposée;
- des conséquences de la matérialisation de ces risques;
- du niveau de risque acceptable pour le Cégep.

5.3 GESTION DES INCIDENTS

Le Cégep déploie des mesures de sécurité de l'information afin d'assurer la continuité de ses services. À cet égard, il met en place les mesures nécessaires afin de :

- 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 conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Dans la gestion des incidents, le Cégep peut exercer ses pouvoirs et ses prérogatives eu égard à toute utilisation inappropriée de l'information qu'elle détient ou de ses systèmes d'information.

6. RÔLES ET RESPONSABILITÉS

6.1 DIRECTEUR GÉNÉRAL

Le directeur général est responsable de l'application de cette politique et le conseil d'administration lui délègue l'autorité d'entreprendre toute action pour en assurer le respect. Il peut se faire assister de tout membre du personnel en lui accordant les mandats pertinents.

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

Le conseil d'administration délègue à un cadre la fonction de RSI et nomme ce dernier. Le RSI est le principal interlocuteur en ce qui concerne la sécurité de l'information au Cégep et relève du directeur général. Il veille à l'application de la Politique et met en place le cadre de gestion de la sécurité de l'information en s'assurant que le niveau de maturité en gestion de la sécurité de l'information répond aux besoins. Plus spécifiquement, le RSI :

- élabore et propose le programme de sécurité de l'information du Cégep et rend compte de son implantation au directeur général;
- formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information et assure un suivi pour la mise à jour de la Politique;
- assure la coordination et la cohérence des actions menées au sein du Cégep en matière de sécurité de l'information, en conseillant les responsables d'actifs informationnels dans les unités;
- produit les plans d'action, les bilans et les redditions de comptes du Cégep en matière de sécurité de l'information;
- propose des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;
- s'assure de la déclaration par le Cégep des risques et des incidents de sécurité de l'information à portée gouvernementale auprès de l'organisme désigné par le gouvernement (CERT/AQ);
- collabore à l'élaboration du contenu du plan de communication, du programme de sensibilisation et de formation en matière de sécurité de l'information et veille au déploiement de ceux-ci;
- procède aux enquêtes dans des transgressions sérieuses ayant trait présumément à la Politique à la suite de l'autorisation du directeur général;

- effectue des veilles normatives, juridiques, gouvernementales et technologiques afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information;
- s'assure de la contribution du Cégep au processus de gestion des risques et des incidents de sécurité de l'information à portée gouvernementale.

6.3 COORDONNATEUR SECTORIEL DE GESTION DES INCIDENTS

Le coordonnateur sectoriel de gestion des incidents (CSGI) représente le Cégep en matière de déclaration des incidents à portée gouvernementale. Le responsable de la sécurité de l'information désigne les personnes agissant à titre de CSGI au Cégep. Ce dernier a la responsabilité :

- de participer activement au réseau d'alerte gouvernemental;
- d'assurer le relais entre le Cégep et le CERT/AQ et de mettre en œuvre les stratégies de réaction appropriées;
- de déclarer les incidents au CERT/AQ;
- de contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information du Cégep;
- de contribuer aux analyses de risques de sécurité de l'information, d'identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
- de seconder le RSI.

6.4 SECRÉTAIRE GÉNÉRAL

En sa qualité de responsable des archives, de l'accès aux documents et de la protection des renseignements personnels, le secrétaire général agit comme personne-ressource pour toute question ou problématique relative à la sécurité des renseignements personnels détenus par le Cégep. Il veille à l'établissement des mesures de protection des renseignements personnels à l'égard des documents, à l'application de telles mesures et à ce que des correctifs soient apportés, le cas échéant.

6.5 RESPONSABLES D'ACTIFS INFORMATIONNELS

Les responsables d'actifs informationnels sont les membres du personnel cadre détenant la plus haute autorité au sein d'une unité 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. Le responsable d'actifs informationnels peut déléguer la totalité ou une partie de sa responsabilité à un autre membre du personnel cadre de l'unité.

Les responsables d'actifs informationnels :

- informent le personnel relevant de leur autorité et les tiers avec lesquels leur unité transige de la Politique sur la sécurité de l'information et des dispositions du cadre de gestion afin de les sensibiliser à la nécessité de s'y conformer;
- collaborent activement à la catégorisation de l'information de l'unité sous leur responsabilité et à l'analyse de risques;
- voient à la protection de l'information et des systèmes d'information sous leur responsabilité en veillant à ce que ceux-ci soient utilisés par le personnel relevant de leur autorité en conformité avec la Politique sur la sécurité de l'information et de tout autre élément du cadre de gestion;

- s'assurent 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 leur 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 de gestion;
- rapportent à la Direction des systèmes et des technologies de l'information toute menace ou tout incident afférant à la sécurité de l'information numérique;
- collaborent 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;
- rapportent au RSI tout problème lié à l'application de la présente politique dont toute contravention réelle ou apparente d'un membre du personnel à l'égard de l'application de cette politique.

6.6 DIRECTION DES SYSTÈMES ET DES TECHNOLOGIES DE L'INFORMATION

- Contribue à l'élaboration et à la mise en œuvre de directives visant à assurer la sécurité de l'information numérique ;
- met en œuvre les mesures permettant d'assurer la sécurité de l'information numérique, dont les plans de reprise informatique en cas d'incident ou de sinistre ;
- met en place un cadre normatif de développement assurant la prise en charge des exigences de sécurité de l'information, y compris celles liées au respect des exigences légales de protection des renseignements personnels, lors de la réalisation d'un projet de développement ou lors de l'acquisition d'un système d'information.

6.7 PILOTE DE SYSTÈME

- Applique et fait appliquer par le personnel sous sa responsabilité les directives de sécurité concernant l'actif informationnel dont il est responsable;
- rédige les procédures concernant le système dont il est responsable;
- confirme les accès pour chacun des usagers et tient un registre décrivant ceux-ci;
- s'assure de la cohérence des accès selon les statuts définis pour les usagers et les exigences de la présente politique.

6.8 DIRECTION DU PERSONNEL ET DES AFFAIRES CORPORATIVES

- Informe la Direction des systèmes et des technologies de l'information (DSTI) d'une embauche, d'un changement de fonction et de la fin d'emploi d'une personne, afin de mettre à jour les accès aux actifs informationnels du Cégep;
- informe tout nouvel employé de ses obligations découlant de la présente politique et obtient son engagement à son respect.

6.9 DIRECTION DES RESSOURCES MATÉRIELLES

- Contribue à l'identification de mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels du Cégep, notamment en ce qui concerne les systèmes et les installations stratégiques ou des supports de l'information confidentielle;
- sécurise et contrôle les accès physiques aux locaux du Cégep;
- gère les moyens d'accès physique (clefs, cartes magnétiques, etc.) aux locaux à accès restreint (salles informatiques, entreposage, etc.).

6.10 PERSONNEL D'ENCADREMENT

- S'assure que le personnel placé sous sa responsabilité est au fait de ses obligations découlant de la présente politique ainsi que des normes, directives et procédures en vigueur en matière de sécurité de l'information;
- communique à la DSTI tout problème d'importance en matière de sécurité de l'information.

6.11 USAGER

- Prend connaissance de la Politique et y adhère en respectant les normes, directives et procédures en vigueur en matière de sécurité de l'information;
- utilise les technologies de l'information mises à sa disposition aux fins auxquelles elles sont destinées et dans le cadre des accès qui lui sont accordés;
- est responsable des actions résultant de l'usage de son identifiant, de son code d'accès ou de son mot de passe, que ces actions soient posées par lui-même ou par un tiers;
- informe son responsable, son professeur ou la DSTI de toute violation des mesures de sécurité de l'information dont il pourrait être témoin.

7. MANQUEMENT AUX RÈGLES DE LA POLITIQUE

Tout membre de la communauté collégiale 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 et des règles disciplinaires internes applicables (dont celles des conventions collectives de travail et du Règlement n^{o} 14 du Cégep).

Toute contravention à la Politique, qu'elle soit perpétrée par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe, est passible des sanctions prévues au contrat le liant au Cégep ou en vertu des dispositions de la législation applicable en la matière.

8. ENTRÉE EN VIGUEUR ET RÉVISION DE LA POLITIQUE

La présente politique entre en vigueur au moment de son adoption par le conseil d'administration. Le Cégep procède à l'examen de la Politique et à sa révision lorsque l'évolution du cadre juridique ou social le commande ou au plus tard 8 ans après son adoption.

Politique adoptée par le conseil d'administration à sa réunion du 23 avril 2018.

Christian Morin
Secrétaire du conseil

GLOSSAIRE

Actif informationnel

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 Cégep habituellement accessible ou utilisable 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). 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.

Autorisation

L'attribution par le Cégep 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

L'ensemble des consignes, c'est-à-dire les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues, qui encadrent les activités d'un établissement.

Confidentialité

La 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.

Cycle de vie de l'information

L'ensemble des étapes que franchit l'information, de sa conception 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 Cégep.

Détenteur de l'information

Un employé désigné par son organisme public, appartenant à la classe d'emploi de niveau cadre ou à une classe d'emploi de niveau supérieur, et dont le rôle est, notamment, de s'assurer de la sécurité de l'information et des ressources qui la sous-tendent, relevant de la responsabilité de son service. Le terme « détenteur de processus d'affaires » est utilisé lorsque ce rôle se limite à un processus d'affaires déterminé.

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.

Disponibilité

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

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.

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

Un moyen concret assurant partiellement ou totalement la protection d'information du Cégep 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.

Pilote de système

Le gestionnaire responsable des aspects opérationnels d'un système corporatif (notamment les systèmes de gestion des dossiers étudiants, de gestion financière, de paie-personnel).

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 Cégep.

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 Cégep, 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.

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

Une 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 présente politique.

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.

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 Cégep.

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.