Sécurité de l'information

Politique

Adoptée par le conseil d'administration le 29 mai 2018 (2018-TU-CA-060-469)

Références : Guides PR-074 et PR-075 du SCT[1]
Diverses politiques relatives à la sécurité de l'information du milieu universitaire

L'emploi du générique masculin dans le présent document a pour seul objectif d'alléger le texte.

Préambule

Dans l'accomplissement de sa mission d'enseignement et de recherche, l'Université TÉLUQ, ci-après désignée « l'Université », détient de l'information sous plusieurs formes et sur plusieurs supports. Cette information, parfois de nature personnelle et confidentielle, possède une valeur légale, administrative, économique et patrimoniale. Elle doit donc faire l'objet d'une utilisation appropriée et d'une protection adéquate tout au long de son cycle de vie.

Cette politique de sécurité de l'information, ci-après désignée « politique », est adoptée conformément à la Directive sur la sécurité gouvernementale, découlant de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement. Elle comporte notamment l'obligation pour un organisme public, d'adopter et de mettre en œuvre une politique de sécurité de l'information, de la maintenir à jour et d'en assurer l'application.

1. Objectif de la politique

La politique a pour objectif de soutenir la prise en charge des exigences de sécurité de l'information et de mettre de l'avant les moyens nécessaires à leur réalisation afin que l'Université puisse s'acquitter de ses obligations légales à l'égard de la sécurité de l'information. Elle viendra renforcer le cadre de gouvernance de la sécurité de l'information en établissant les conditions générales visant à préserver adéquatement la confidentialité, à garantir l'intégrité et à assurer la disponibilité de l'information dans le respect de la liberté académique, des droits et des obligations des utilisateurs.

[1] Guides réalisés par le Sous-secrétariat du dirigeant principal de l'information et produits par la Direction des communications du Secrétariat du Conseil du trésor.

2. Cadre légal et administratif

La politique s'inscrit principalement dans un contexte régi par :

- La Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (RLRQ, chapitre G-1.03);
- La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1);
- La Loi concernant le cadre juridique des technologies et l'information (RLRQ, chapitre C-1.1);
- La Loi sur le droit d'auteur (LRC, 1985, chapitre C-42);
- La Loi sur les archives (RLRQ, chapitre A-21.1);
- La Loi canadienne sur les droits de la personne (LRC, 1985, chapitre H-6);
- Le Règlement sur la diffusion de l'information et sur la protection des renseignements personnels (RLRQ, chapitre A-2.1, r. 02);
- La Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics (SCT);
- La Directive sur la sécurité de l'information gouvernementale (RLRQ, chapitre G-1.03, a. 20);
- La Charte des droits et libertés de la personne (RLRQ, chapitre C-12);
- Le Code civil du Québec;
- Le Code criminel (LRC, 1985, chapitre C-46);
- Le Code d'éthique et de déontologie institutionnel (2015-TU-CA-027-160);
- La politique Gestion intégrée des risques (2014-TU-CA-020-134);
- Le règlement Régie interne (2015-TU-CA-027-161).

3. Définitions

Dans cette politique, à moins que le contexte n'impose un sens différent, les expressions et mots suivants signifient :

Actif informationnel : Une information, quel que soit son canal de communication (téléphone analogique ou numérique, télécopie, voix, etc.) ou son support (papier, pellicule photographique ou cinématographique, ruban magnétique, support électronique, etc.), un système ou un support d'information, une technologie de l'information, une installation ou un ensemble de ces éléments, acquis ou constitués par une organisation.

CERT/AQ : Équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise relevant du Centre de services partagés du Québec (CSPQ).

Comité de crise en sécurité de l'information : Groupe décisionnel appelé à intervenir pour assurer la continuité ou la reprise rapide des services en cas d'incident critique de sécurité de l'information. Ce comité peut être permanent ou ad hoc selon les besoins et est dirigé par le responsable organisationnel de la sécurité de l'information (ROSI).

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.

Cycle de vie de l'information : L'ensemble des étapes que franchit une information et qui vont de sa création, en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation ou sa destruction, en conformité avec le calendrier de conservation de l'Université.

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

Document normatif : Un règlement, un code, une politique, une directive, une procédure ou tout autre document de l'Université édictant des règles à suivre ou prescrivant des façons de faire, ainsi que de tels documents émanant des organismes subventionnaires applicables à l'Université.

Gestionnaire : Toute personne engagée à titre de cadre selon les termes du Protocole établissant les conditions du personnel cadre de la Télé-université ou selon les termes du Protocole des cadres supérieurs de l'Université du Québec, de même que les directeurs de département et d'unité de recherche.

Incident à portée gouvernementale : Conséquence observable de la concrétisation d'un risque, produisant un effet négatif sur le gouvernement et qui nécessite une intervention.

Infonuagique[2] : Modèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation. Exemples : Taleo, Apple iCloud, Dropbox, Google Drive, OneDrive de Microsoft (Office 365).

Intégrité : Propriété associée à une information de ne subir aucune altération ou destruction sans autorisation et d'être conservée sur un support lui procurant stabilité et pérennité.

Membre du personnel : Toute personne embauchée par l'Université, quel que soit son statut ou la catégorie d'emploi dont elle fait partie.

Registre des incidents : Registre dans lequel sont consignés les incidents de sécurité de l'information.

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

Responsable d'actifs informationnels : Gestionnaire qui doit s'assurer de l'utilisation adéquate et de la sécurité des actifs informationnels sous sa responsabilité.

Responsable organisationnel de la sécurité de l'information (ROSI) : Personne qui joue le rôle de porte-parole du dirigeant principal de l'information auprès de son organisation (ou du dirigeant réseau de l'information le cas échéant), à laquelle il communique les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information.

Utilisateur : Toute personne de l'Université de quelque catégorie d'emploi, de statut d'employé ainsi que toute personne qui, par engagement contractuel ou autre, utilise un actif informationnel de l'Université ou y a accès. Les membres du personnel de l'Université ainsi que les étudiants sont les premiers utilisateurs de l'information de l'Université.

[2] Office québécois de la langue française.

4. Champ d'application

Personnes visées : Cette politique s'applique aux utilisateurs, sans égard à leur statut, sous réserve des protocoles et des conventions collectives en vigueur à l'Université. Certaines dispositions ou mesures particulières peuvent continuer à s'appliquer même après la cessation des fonctions à l'Université.

Actifs visés : Cette politique s'applique à l'ensemble des actifs informationnels dont l'Université doit assurer la sécurité, peu importe sa forme, son support ou son emplacement. Ces actifs informationnels peuvent être détenues ou exploités par l'Université ou par un tiers, comme c'est le cas dans l'établissement de partenariats ou d'utilisation de services en infonuagiques.

Activités visées : Cette politique vise l'ensemble des activités composant le cycle de vie de l'information sous la responsabilité de l'Université, que ces activités soient conduites à l'intérieur ou à l'extérieur des locaux de l'Université.

Cette politique ne constitue pas l'unique document de référence relatif à la sécurité de l'information et s'y ajoutent les dispositions légales ou réglementaires, et autres documents normatifs qui établissent également des règles applicables aux membres du personnel.

5. Principes directeurs

5.1 Protection de l'information

L'Université adhère aux orientations et objectifs stratégiques gouvernementaux en matière de sécurité de l'information et s'engage à ce que les pratiques et les solutions retenues en la matière correspondent, dans la mesure du possible, à des façons de faire reconnues et généralement utilisées, tant à l'échelle nationale qu'internationale.

L'Université reconnaît que les actifs informationnels qu'elle détient sont essentiels à ses activités d'enseignement, de recherche et de service à la collectivité, de ce fait, qu'ils doivent faire l'objet d'une évaluation constante, d'une utilisation appropriée et d'une protection adéquate.

5.2 Protection des renseignements confidentiels

Toute information confidentielle doit être préservée de toute divulgation, de tout accès ou de toute utilisation non autorisée.

Sont notamment considérés comme confidentiels, au sens de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels, les renseignements personnels ainsi que tout renseignement dont la divulgation aurait des incidences, notamment sur les relations intergouvernementales, les négociations entre organismes publics, les décisions administratives ou politiques et la vérification.

5.3 Sensibilisation et formation

L'Université s'engage à sensibiliser et à former ses utilisateurs à la sécurité des actifs informationnels de l'Université, aux conséquences d'une atteinte à leur sécurité ainsi qu'à leur rôle et leurs obligations en la matière.

5.4 Éthique

La protection des actifs informationnels de l'Université est soutenue par une démarche éthique visant à assurer la régulation des conduites et la responsabilisation individuelle. À cet effet, les membres du personnel sont soumis au Code d'éthique et de déontologie institutionnel[3] qui les aidera à accomplir leur travail dans le respect des valeurs de l'Université.

6. Cadre de gestion

Ce cadre de gestion de la sécurité de l'information précise les rôles et responsabilités des différents intervenants de l'Université en considération des principes fondamentaux suivants : la gestion des accès, la gestion des risques et la gestion des incidents.

6.1 Gestion de la sécurité de l'information

6.1.1 Gestion des accès

La gestion des accès est constituée de l'ensemble des processus mis en œuvre par l'Université quant à la gestion des droits des utilisateurs aux systèmes d'information organisationnels ou tout autre système contenant de l'information protégée. Tout en s'assurant de protéger l'intégrité et la confidentialité de cette information, cette gestion permet de déterminer qui a accès à quelle information ou système d'information, et ce, en fonction des rôles et responsabilités des utilisateurs.

6.1.2 Gestion des risques

La gestion des risques en sécurité de l'information consiste à la mise en œuvre de moyens raisonnables afin de minimiser la probabilité que survienne un événement portant atteinte à l'information détenue par l'Université. Les moyens mis en place sont proportionnels à la valeur de l'information, au degré de sensibilité de celle-ci ainsi qu'aux probabilités d'occurrence du risque. Cette gestion des risques s'inscrit dans le processus existant de gestion intégrée des risques de l'Université[4].

6.1.3 Gestion des incidents

La gestion des incidents comprend le processus permettant à l'Université de s'assurer de la continuité de ses activités tout en diminuant la portée d'un incident. Les activités du processus de gestion des incidents concernent les éléments suivants : prévention, détection, réaction, rétablissement et suivis. Conformément à la Directive sur la sécurité de l'information gouvernementale, les incidents de sécurité de l'information à portée gouvernementale sont déclarés au CERT/AQ dès leur confirmation.

[3] Politique Code d'éthique et de déontologie institutionnel (2015-TU-CA-027-160)
[4] Politique Gestion intégrée des risques (2014-TU-CA-020-134)

6.2 Rôles et responsabilités

Conseil d'administration

- Adopte la présente politique ainsi que toutes les modifications afférentes à celle-ci.

Comité des finances et d'audit

- Recommande au conseil d'administration l'adoption de cette politique ainsi que ses mises à jour;
- S'assure de l'application des règles de gouvernance et de gestion des ressources informationnelles.

Secrétaire général

- Agit en tant que responsable organisationnel de la sécurité de l'information (ROSI) et réalise les activités liées à ce rôle;
- Participe à la mise en œuvre des activités permettant la réduction des risques de sécurité de l'information;
- Est responsable ou désigne un responsable du registre des incidents de sécurité de l'information;
- Dirige le comité de crise en sécurité de l'information;
- Reçoit les plaintes et coordonne toute enquête relative à la sécurité de l'information.

Direction des services administratifs

- Est responsable de l'application de la politique et de son évolution;
- Procède à toutes vérifications d'usage qu'elle estime nécessaire afin de s'assurer du respect de la présente politique;
- Applique les sanctions administratives en cas d'infraction à la politique.

Direction du Service des technologies de l'information

- S'assure de la prise en charge des exigences de sécurité dans le développement et l'exploitation de l'ensemble des systèmes informatiques et d'informations de l'Université;
- Engage les moyens appropriés afin de répondre à toute menace ou tout incident et ainsi rétablir le plus rapidement possible le fonctionnement normal des services lors d'incidents de sécurité de l'information de nature technologique;
- Veille à la réalisation périodique d'audits de sécurité informatique, tests d'intrusion et de vulnérabilité conformément à la Directive sur la sécurité de l'information gouvernementale et planifie les actions requises afin de répondre aux recommandations formulées à la suite de ces activités;
- S'assure de la participation du Service des technologies de l'information aux différentes activités relatives à la sécurité de l'information et à la sécurité informatique (comités internes et externes, CERT/AQ, etc.);
- Participe à toute enquête relative à une mauvaise utilisation des actifs informationnels de l'Université;
- Participe aux activités d'information et de sensibilisation des utilisateurs en matière de sécurité dans l'utilisation des actifs informationnels de l'Université;
- Maintient le registre des incidents de sécurité de l'information.

Direction du Service des ressources humaines et direction du Service des ressources académiques

- Informe les nouveaux employés de cette politique et d'autres documents de référence relatifs à la sécurité de l'information, notamment le Code d'éthique et de déontologie institutionnel, et s'assure de leur engagement à les respecter;
- Participe à l'imposition des sanctions appropriées lors de violation des politiques ou directives touchant la sécurité de l'information (sous réserve des protocoles et des conventions collectives en vigueur dans l'Université);
- Participe à la formation et aux activités de sensibilisation des employés relativement à la sécurité de l'information.

Direction du Service des ressources matérielles

- S'assure de la protection physique des locaux et sécurise leur accès en fonction des rôles des utilisateurs;
- S'assure d'offrir un espace sécurisé (salle d'archivage) réservé à l'entreposage physique de certaines informations détenues par l'Université;
- Est responsable du processus de disposition des actifs informationnels en collaboration avec le Service des technologies de l'information;
- Participe, au besoin, à toute enquête relative à une mauvaise utilisation des actifs informationnels de l'Université;
- Participe aux activités d'information et de sensibilisation des utilisateurs en matière de sécurité dans l'utilisation des actifs informationnels de l'Université.

Responsable d'actifs informationnels

- S'assure de la gestion de la sécurité des actifs informationnels sous sa responsabilité en réalisant les mesures de sécurité et en veillant à ce qu'elles soient connues et respectées par les utilisateurs;
- S'assure de la révision des accès aux actifs informationnels des employés sous sa responsabilité;
- S'assure de la prise en compte de la sécurité de l'information lors de la réalisation d'activités avec des fournisseurs, consultants et partenaires;
- Collabore à l'analyse et à la gestion des risques en sécurité de l'information et contribue à la catégorisation des actifs informationnels sous sa responsabilité.

Utilisateur

- Prend connaissance de la politique et autres documents de référence relatifs à la sécurité de l'information et s'engage à s'y conformer;
- Protège la confidentialité des données et utilise adéquatement les actifs informationnels de l'Université à l'intérieur des accès accordés et en se limitant aux fins auxquelles ils sont destinés;
- Protège les accès à son poste de travail ainsi qu'aux différents systèmes d'information dont il a accès dans le cadre de ses fonctions et respecte les mesures de sécurité mises en place sur son poste de travail et sur le réseau;
- Signale à son gestionnaire ou au responsable organisationnel de la sécurité de l'information (ROSI) toute situation ou tout incident susceptible de compromettre la sécurité d'un actif informationnel.

7. Sanctions

Lorsqu'un utilisateur contrevient à la politique ou aux directives de l'Université, il s'expose à des mesures disciplinaires, administratives ou légales, en fonction de la gravité de son geste. Ces mesures peuvent inclure la suspension des privilèges, la réprimande, la suspension, le congédiement ou autre, et ce, conformément aux dispositions des conventions collectives, des protocoles, des ententes ou des contrats.

L'Université peut transmettre à toute autorité judiciaire les renseignements colligés et qui le portent à croire qu'une infraction à toute loi ou tout règlement en vigueur a été commise.

8. Dispositions finales

- La politique entre en vigueur à la date de son adoption par le conseil d'administration;
- La politique ne constitue pas l'unique document de référence relatif à la sécurité de l'information. Les obligations qui en découlent sont précisées notamment dans une directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels de l'Université;
- La politique remplace la Politique sur la sécurité des systèmes d'information de la Télé-université (CA-100-661) adoptée par le conseil d'administration le 25 février 2003.

Table des matières

Préambule 1
1. Objectif de la politique 1
2. Cadre légal et administratif 2
3. Définitions 2
4. Champ d'application 4
5. Principes directeurs 4
5.1 Protection de l'information 4
5.2 Protection des renseignements confidentiels 4
5.3 Sensibilisation et formation 4
5.4 Éthique 5
6. Cadre de gestion 5
6.1 Gestion de la sécurité de l'information 5
6.1.1 Gestion des accès 5
6.1.2 Gestion des risques 5
6.1.3 Gestion des incidents 5
6.2 Rôles et responsabilités 6
7. Sanctions 8
8. Dispositions finales 8
Table des matières 9