Sécurité de l'information

Politique

Adoptée par le conseil d'administration le 21 avril 2026 (2026-TU-CA-138-1254)

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

Préambule

Dans l'accomplissement de sa mission, 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 gouvernementale sur la sécurité de l'information, découlant de la *Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement* (RLRQ, c. G-1.03). 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 le déploiement des exigences de sécurité de l'information afin que l'Université puisse s'acquitter de ses obligations légales à l'égard de la sécurité de l'information. Elle vient 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 Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics (SCT);
- La Directive gouvernementale sur la sécurité de l'information (RLRQ, chapitre G-1.03, a. 20);
- 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 ont comme signification :

Actif informationnel : Une information, quel que soit son canal de communication (téléphone, courriel, visioconférence, 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.

Cadre de gouvernance de la sécurité de l'information : L'ensemble de politiques, de directives, de procédures ou de tout autre écrit de gestion ou normatif adopté par l'Université afin de protéger ses actifs informationnels.

CERT/QC : Une équipe de réponse aux incidents de sécurité de l'information de l'administration québécoise relevant du ministère de la Cybersécurité et du Numérique (MCN).

Confidentialité : La propriété qu'a 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 : La propriété qu'a 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, un guide, 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 l'Université ou selon les termes du Protocole des cadres

supérieurs de l'Université du Québec, de même que les directions de département et d'unité de recherche.

Habilitations : Une catégorie établie en fonction de niveaux de sécurité définis, dans laquelle est classée une personne en matière d'accès à des informations ou à des ressources informatiques.

Incident : Un incident relatif à la sécurité de l'information[2] ou à portée gouvernementale[3].

Infonuagique[4] : Un 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. Exemple : OneDrive de Microsoft Office 365.

Intégrité : La propriété qu'a 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 sa catégorie d'emploi.

Registre des événements de sécurité : Le registre dans lequel sont consignés les événements de sécurité de l'information. Un événement consiste en une menace, une vulnérabilité ou un incident.

Registre des incidents de confidentialité : Le registre dans lequel sont consignés les incidents de sécurité touchant la confidentialité de renseignements personnels.

Registre d'autorité en sécurité informationnelle : Le registre dans lequel sont consignées les personnes désignées aux différents rôles liés à la sécurité de l'information.

Renseignement personnel : Tout renseignement qui concerne une personne physique et qui permet de l'identifier directement ou indirectement. 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 de l'information.

Propriétaire d'actifs informationnels : Un ou une gestionnaire qui doit s'assurer de l'utilisation adéquate et de la sécurité des actifs informationnels sous sa responsabilité.

Utilisateur, utilisatrice : Toute personne embauchée par l'Université de quelque catégorie d'emploi ou de statut, 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 étudiantes et étudiants sont les premiers utilisateurs de l'information de l'Université.

4. Champ d'application

Personnes visées : Cette politique s'applique aux utilisateurs et utilisatrices, 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.

[2] Un ou une série d'événements de sécurité de l'information indésirables ou inattendus qui ont une probabilité de compromettre les opérations de l'organisation et de menacer la sécurité de l'information (ISO/IEC (2018). Technologies de l'information – Techniques de sécurité – Systèmes de management de la sécurité de l'information – Présentation et vocabulaire (ISO/IEC 27000:2018)).
[3] Conséquence observable de la concrétisation d'un risque produisant un effet négatif sur le gouvernement et qui nécessite une intervention.
[4] Office québécois de la langue française.

Actifs visés : Cette politique s'applique à l'ensemble des actifs informationnels dont l'Université doit assurer la sécurité, peu importe leur forme, leur support ou leur emplacement. Ces actifs informationnels peuvent être détenus 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.

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 reconnait 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* (RLRQ, chapitre A-2.1), les renseignements personnels ainsi que tout renseignement que la loi permet de garder confidentiel en lien avec les activités de l'Université, autant académiques, de recherche qu'administratives.

5.3 Classification des données

L'Université s'appuie sur le modèle gouvernemental de classification des données numériques pour encadrer le processus de classification des données.

Ce dernier offre une méthodologie structurée permettant d'identifier et d'évaluer la sensibilité en fonction des préjudices potentiels liés à une atteinte à la confidentialité, l'intégrité ou la disponibilité, et d'attribuer un profil de classification; ce profil détermine les mesures de sécurité appropriées à mettre en place.

La classification des données doit faire l'objet d'une revue périodique pour s'assurer que les mesures de protection appliquées restent appropriées.

5.4 Sensibilisation et formation

L'Université s'engage à sensibiliser et à former ses utilisateurs et utilisatrices 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.

5.5 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[5] qui les aide 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 et intervenantes et comités de l'Université en considération des principes fondamentaux suivants : la gestion des accès, la gestion des risques et la gestion des menaces, des vulnérabilités et 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 habilitations des utilisateurs et utilisatrices aux systèmes d'information organisationnels ou à 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 utilisatrices et utilisateurs.

6.1.2 Gestion des risques

La gestion des risques en sécurité de l'information consiste à mettre 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[6].

6.1.3 Gestion des menaces, vulnérabilités et incidents (GMVI)

La gestion des menaces, vulnérabilités et incidents est constituée de l'ensemble des 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 menaces, vulnérabilités et incidents concernent les éléments suivants : prévention, détection, réaction, rétablissement et suivis.

6.2 Rôles et responsabilités

Conseil d'administration

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

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

Comités du conseil d'administration

- Exercent les rôles et responsabilités prévus au règlement *Régie interne* de l'Université[7] sur recommandation, le cas échéant, du comité compétent.

Comité de sécurité de l'information

- S'assure d'établir et de maintenir les règles de gouvernance en matière de sécurité informationnelle et formule les recommandations associées;
- Est composé des personnes suivantes :
  - ✓ Chef ou cheffe de la sécurité de l'information organisationnelle (CSIO);
  - ✓ Deux coordonnatrices ou coordonnateurs organisationnels des mesures de sécurité de l'information (COMSI);
  - ✓ Directeur ou directrice du Service des technologies de l'information;
  - ✓ Secrétaire général ou secrétaire générale et directeur ou directrice de la gouvernance numérique;
  - ✓ Directeur ou directrice de la Direction des services administratifs et à la communauté (DSAC);
  - ✓ Responsable des archives (archiviste);
  - ✓ Une professeure ou un professeur;
  - ✓ Toute personne invitée, au besoin, à participer aux échanges du comité à titre de personne-ressource;
- Détermine son mode de fonctionnement, voit à se nommer un ou une responsable de comité et se rencontre périodiquement.

Comité de gestion de crise

- Intervient notamment lorsque les tentatives de rétablissement des activités n'ont pas apporté les résultats escomptés ou qu'aucune mesure palliative n'a pu assurer la continuité ou la reprise rapide des services.

Les responsabilités spécifiques du comité ainsi que les processus d'activation, de coordination et de communication sont définis au Plan de gestion de crise de l'Université.

Chef ou cheffe de la sécurité de l'information organisationnelle (CSIO)

- Assume la responsabilité de la prise en charge globale de la sécurité de l'information au sein de l'Université;
- Travaille en étroite collaboration avec les répondants en matière de sécurité de l'information pour assurer la prise en charge des exigences de sécurité de l'information;
- Agit comme porte-parole du dirigeant principal de l'information (DPI) auprès de l'Université, à laquelle il communique les orientations et les priorités d'intervention gouvernementales en matière de sécurité de l'information;
- Assure la coordination et la cohérence des actions, dont les principales portent sur l'adoption d'une politique et d'un cadre de gestion de la sécurité de l'information ainsi que sur la mise en œuvre de processus officiels de gestion des risques, de gestion de l'accès à l'information et de gestion des menaces, vulnérabilités et incidents de sécurité de l'information;
- Conseille la haute direction en matière de sécurité de l'information;
- Définit et met en œuvre les orientations internes de sécurité de l'information;
- Soutient les unités administratives et les propriétaires d'actifs informationnels dans la prise en charge des exigences de sécurité de l'information;

[7] Régie interne (2025-TU-CA-132- 1183).

- Reçoit les plaintes et coordonne toute enquête relative à la sécurité de l'information.

Coordonnatrice organisationnelle ou coordonnateur organisationnel des mesures en sécurité informationnelle (COMSI)

- Intervient dans la mise en œuvre des mesures de sécurité et apporte le soutien nécessaire au CSIO de l'Université, notamment en matière de la gestion des incidents et des risques en sécurité de l'information;
- Représente l'Université auprès du réseau d'alerte gouvernemental;
- Est responsable de l'application du processus de gestion des menaces, vulnérabilités et incidents (GMVI) au sein de l'Université, en soutien au CSIO;
- Produit les plans d'action et les bilans de l'Université en matière de sécurité de l'information;
- Collabore auprès du CSIO à l'élaboration des divers éléments stratégiques et tactiques en sécurité de l'information :
  - ✓ Maintient le registre des événements et des incidents liés à la sécurité de l'information;
  - ✓ Participe et effectue des analyses de risques en sécurité de l'information;
  - ✓ Gère le processus de gestion, de déclaration des incidents et de résolution de problème, et contribue à sa mise en place;
  - ✓ Contribue au processus formel de gestion des droits d'accès à l'information.

Secrétariat général et Direction de la gouvernance numérique

- S'assure de la classification et de la catégorisation de l'information et applique les mesures de gestion de l'information adéquates;
- S'assure du maintien du registre des incidents de confidentialité;
- S'assure de la vérification interne et de la gestion documentaire;
- Participe à la mise en œuvre des activités permettant la réduction des risques de sécurité de l'information;
- Participe au programme de formation et de sensibilisation en matière de saine gestion de l'information;
- S'assure du respect des politiques, règlements, procédures et pratiques internes;
- S'assure de l'application des plans d'urgence et de continuité des activités pour les systèmes informatiques et le maintien des ressources informationnelles de l'organisation.

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;
- S'assure de la continuité des services en mettant en place les moyens appropriés afin de répondre à toutes vulnérabilités, menaces ou tous incidents, 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/QC, 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.

Responsable de l'accès à l'information et de la protection des renseignements personnels

- Veille à assurer le respect et la mise en œuvre des règles et des obligations de l'Université en matière de protection des renseignements personnels;
- Participe notamment à la prévention et à la gestion des incidents de confidentialité, à établir un processus de traitement des plaintes concernant la protection des renseignements personnels conformément à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ, chapitre A-2.1);
- Conseille les unités administratives relativement à toute question relative aux renseignements personnels sous leur garde.

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

- Informe les nouveaux membres du personnel de cette politique, des directives 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 du personnel 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 et utilisatrices;
- 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 utilisatrices et utilisateurs en matière de sécurité dans l'utilisation des actifs informationnels de l'Université.

Propriétaire d'actifs informationnels

- S'assure de la gestion de la sécurité des actifs informationnels sous sa responsabilité en réalisant les mesures de sécurité nécessaires et en veillant à ce qu'elles soient connues et respectées par les utilisateurs et utilisatrices;
- S'assure de classifier et d'évaluer les niveaux de disponibilité, d'intégrité et de confidentialité des actifs informationnels sous sa responsabilité ;
- S'assure de la révision des accès aux actifs informationnels des membres du personnel sous sa responsabilité;
- S'assure de l'application des mesures de 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 classification des actifs informationnels sous sa responsabilité.

Utilisateur, utilisatrice

- Prend connaissance de la politique, des directives et des 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 habilitations 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 auxquels il ou elle a accès dans le cadre de ses fonctions et respecte les mesures de sécurité mises en place;
- Signale à son ou sa gestionnaire, à la coordonnatrice organisationnelle ou au coordonnateur organisationnel des mesures en sécurité informationnel (COMSI) toute situation ou tout incident susceptible de compromettre la sécurité d'un actif informationnel.

7. Sanctions

Lorsqu'un utilisateur ou une utilisatrice contrevient à la politique ou aux directives de l'Université, il ou elle 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 portent à croire qu'une infraction à toute loi ou tout règlement en vigueur a été commise.

8. Contrôle

L'Université se réserve le droit de procéder à des contrôles réguliers pour vérifier la bonne application de la présente politique.

9. Dispositions finales

- La politique entre en vigueur à la date de son adoption par le conseil d'administration;
- La politique remplace la Politique sur la sécurité des systèmes d'information de l'Université (2026-TU-CA-138-1254) adoptée par le conseil d'administration le 21 avril 2026.

Table des matières