Politique de sécurité de l'information

Approbation :	Conseil d'administration (Résolution CA-2021-27)
Entrée en vigueur :	28 février 2021
Modifications :	Conseil d'administration (Résolution CA-2025-62)
Entrée en vigueur :	16 avril 2025
Responsable :	Vice-rectorat aux infrastructures et à la transformation
Cadre juridique :	Loi concernant le cadre juridique des technologies de l'information (c. C-1.1) Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (C. A-2.1) Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement (chapitre G-1.03) Politique gouvernementale de cybersécurité (Québec, 2020) Directive sur la sécurité de l'information gouvernementale (Québec, 2021) Politique relative à la gestion de crise de l'Université Laval Règlement sur l'utilisation responsable des technologies de l'information

UNIVERSITÉ LAVAL

Table des matières

PRÉAMBULE

La sécurité de l'information constitue un fondement essentiel pour assurer la confidentialité, l'intégrité et la disponibilité de l'information au sein de l'Université Laval, tout en renforçant la confiance de la communauté universitaire et de ses partenaires envers l'institution.

Dans un contexte marqué par l'évolution constante des risques liés à la cybercriminalité, aux erreurs humaines et aux menaces technologiques, l'établissement d'un cadre clair, structuré et cohérent s'impose comme une condition essentielle pour assurer la protection et la gestion efficaces des actifs informationnels de l'Université.

Les actifs informationnels de l'Université, indispensables à son bon fonctionnement et à la réalisation de sa mission d'enseignement, de recherche et de service à la collectivité, doivent faire l'objet de mesures de protection adaptées afin d'en assurer la disponibilité, l'intégrité et la confidentialité.

La sécurité de l'information ne se limite pas aux technologies de l'information : elle englobe l'ensemble des processus, des pratiques organisationnelles et des comportements individuels visant à gérer les risques associés à l'information, qu'elle soit sous forme numérique, physique ou verbale. Elle repose sur l'engagement actif, conscient et responsable de l'ensemble des membres de la communauté universitaire — étudiantes et étudiants, professeures et professeurs, chercheuses et chercheurs, membres du personnel administratif et cadres — ainsi que sur le respect d'engagements contractuels clairs de la part des tiers contribuant à la mission de l'Université.

Dans cette optique, la présente politique établit un cadre structurant qui précise les principes directeurs, les rôles et les responsabilités essentiels à une gestion rigoureuse, cohérente et proactive de la sécurité de l'information. Elle constitue une référence commune pour l'ensemble des parties prenantes, afin de favoriser la création et le maintien d'un environnement informationnel sécuritaire, résilient et conforme aux exigences institutionnelles.

1. OBJECTIFS

La Politique de sécurité de l'information (la « Politique ») vise à faire de l'Université une organisation résiliente et protégée, en garantissant la confidentialité, l'intégrité et la disponibilité de ses actifs informationnels.
En ce sens, les objectifs principaux de cette Politique sont :

a) De protéger les actifs informationnels supportant la mission de l'Université
b) De préciser les rôles et responsabilités dans la gestion de la sécurité de l'information afin d'assurer une coordination cohérente et efficace des actions
c) De promouvoir une culture de sécurité et de confiance par la valorisation d'un engagement collectif et responsable en matière de sécurité de l'information
d) D'encourager l'innovation dans la gestion proactive des menaces et la résilience face aux incidents de sécurité
e) De garantir la conformité aux lois, règlements et bonnes pratiques relatifs à la protection de l'information

2. CHAMPS D'APPLICATION

La Politique vise l'ensemble des membres de l'Université qui gèrent, conçoivent, développent ou utilisent des actifs informationnels. Elle s'applique à l'ensemble des actifs informationnels de l'Université.

3. DÉFINITIONS

Actif informationnel

Tout support de l'information, matériel ou immatériel, permettant le traitement, la transmission ou la conservation d'informations dans le cadre de leur utilisation prévue, et ayant une valeur stratégique ou opérationnelle pour l'organisation.

Cybersécurité

Capacité, pour un système en réseau, de se protéger et de résister à des événements de sécurité de l'information et susceptibles de porter atteinte à la confidentialité, à l'intégrité et à la disponibilité de l'information qu'il contient.

Incident de sécurité de l'information

Événement avéré où une menace a exploité une vulnérabilité, causant un impact négatif sur la confidentialité, l'intégrité ou la disponibilité des informations. C'est la matérialisation d'un risque, pouvant entraîner des perturbations, des pertes ou des violations des actifs informationnels.

Menace de sécurité de l'information

Événement ou acteur potentiel capable de compromettre la confidentialité, l'intégrité ou la disponibilité des informations ou des systèmes.

Mesure de sécurité de l'information

Action, dispositif ou ensemble de procédures mises en place pour protéger les actifs informationnels contre les menaces et les vulnérabilités visant à garantir la confidentialité, l'intégrité et la disponibilité des informations en minimisant le risque d'incidents de sécurité. Elles peuvent inclure des contrôles physiques, techniques et administratifs tels que le chiffrement des données, les pares-feux, les politiques de gestion des accès, la formation des utilisateurs et les plans de réponse aux incidents.

Risque de sécurité de l'information

Probabilité qu'une menace exploite une vulnérabilité pour entraîner un incident, compromettant ainsi la confidentialité, l'intégrité ou la disponibilité des informations. Il peut conduire à un impact négatif sur les actifs informationnels.

Système d'information

Système constitué d'actifs informationnels et des procédures permettant d'acquérir, de conserver, de traiter et de diffuser les éléments d'information pertinents au fonctionnement de l'Université.

Vulnérabilité

Faiblesse ou une faille dans un système d'information ou un processus qui peut être exploitée pour compromettre la confidentialité, l'intégrité ou la disponibilité des informations.

4. PRINCIPES DIRECTEURS RELATIFS À LA SÉCURITÉ DE L'INFORMATION

Les pratiques de l'Université en matière sécurité de l'information reposent sur les principes directeurs ci-dessous.

4.1 Inventorier et classer les actifs informationnels selon leur criticité et les risques associés

a) Les actifs informationnels sont inventoriés et leurs responsables ont été identifiés.

b) Un profil de sécurité des actifs informationnels est attribué en fonction de la confidentialité, de l'intégrité et de la disponibilité des informations qu'ils contiennent en conformité avec les exigences légales, réglementaires ou contractuelles

c) Un registre de risques de sécurité de l'information est défini et est révisée au besoin, mais au minimum à chaque trimestre.

4.2 Adapter la protection des actifs informationnels aux risques identifiés

Les actifs informationnels sont protégés par des mesures de sécurité de l'information déterminées en fonction du niveau de criticité attribué et basées sur des cadres de référence reconnus, notamment ceux de l'ISO et du NIST[1]. Ces référentiels permettent d'assurer une gestion efficace de la protection des actifs informationnels.

4.3 Intégrer la sécurité tout au long du cycle de vie des systèmes d'information

La sécurité de l'information doit être considérée tout au long du cycle de vie d'un système d'information, notamment des évaluations de sécurité, des tests de sécurité et la conception et l'implémentation de mesures de sécurité, incluant lors de sa fin de vie.

[1] NIST Cybersecurity Framework

4.4 Harmoniser l'application des mesures de sécurité de l'information sur tous les actifs informationnels

Des mesures de sécurité de l'information sont appliquées sur tous les actifs informationnels de l'Université, et ce, peu importe leur localisation physique. Ces mesures permettent :

a) D'identifier et de gérer les actifs informationnels
b) De protéger les actifs informationnels d'éventuels risques
c) De détecter les menaces, vulnérabilités et incidents de sécurité de l'information
d) D'intervenir en cas d'incidents de sécurité de l'information
e) De rétablir l'actif informationnel à un état fonctionnel et sécuritaire

4.5 Promouvoir l'adoption de comportements sécuritaires

L'Université sensibilise et mise sur le développement de la vigilance et du jugement critique de ses membres afin d'éveiller leur vigilance vis-à-vis les risques auxquels ils font face, notamment par leur participation à des formations en matière de sécurité de l'information.

4.6 Renforcer la collaboration et la concertation

a) Les membres qui conçoivent et mettent en œuvre des actifs informationnels ou des systèmes d'information partagent et mettent en commun leurs connaissances, outils et expertises dans la mise en place de saines pratiques en sécurité de l'information.
b) L'Université collabore et participe aux initiatives interuniversitaires, ministérielles et gouvernementales en matière de sécurité de l'information.

4.7 Assurer un équilibre entre innovation en recherche et exigences de sécurité au sein de l'Université

Moteur d'innovation et d'exploration des limites du savoir, la recherche universitaire aborde des enjeux sociétaux et des risques liés aux avancées scientifiques, ce qui exige des mesures de sécurité de l'information adaptées, lesquelles sont ajustées en fonction des spécificités et de la sensibilité de chaque activité de recherche, assurant la protection de l'Université, tout en maintenant un équilibre entre progrès et sécurité.

5. RÔLES ET RESPONSABILITÉS

5.1 Conseil d'administration

Adopte la Politique suivant la recommandation du Comité des ressources immobilières et informationnelles. Certaines fonctions ou responsabilités peuvent être déléguées, conformément aux mécanismes de gouvernance en vigueur, sans que cela ne diminue cette responsabilité.

5.2 Comité des ressources immobilières et informationnelles

Recommande l'approbation de la Politique en sécurité de l'information (SI) au Conseil d'administration (CA), examine les éléments du cadre normatif en SI, exerce un rôle de surveillance et de suivi à l'égard de la gouvernance et de la gestion de la SI et soutient le CA à l'égard de la gestion des risques en SI. Suivant la recommandation de la dirigeante ou du dirigeant de l'information, le CRII peut approuver les modifications mineures à apporter à la Politique pour l'adapter à de nouvelles circonstances, notamment lors d'un changement à la législation.

5.3 Vice-rectrice ou vice-recteur aux infrastructures et à la transformation

Responsable exécutif de l'ensemble des fonctions liées à la cybersécurité, en encadrant les grandes orientations, les mécanismes de gouvernance et la capacité organisationnelle à protéger les actifs informationnels.

5.4 Comité de la sécurité de l'information

Sous la responsabilité de la vice-rectrice ou du vice-recteur aux infrastructures et à la transformation, instance de concertation en matière de sécurité de l'information, au niveau stratégique, au sein de l'Université. Le comité formule des recommandations sur le cadre normatif, le registre des risques, les plans stratégiques, les initiatives et les bilans de sécurité de l'information de l'Université ainsi que toute proposition d'action en matière de sécurité de l'information.

5.5 Dirigeante ou dirigeant de l'information

Sous l'autorité de la vice-rectrice ou du vice-recteur aux infrastructures et à la transformation assure la gestion stratégique et opérationnelle des services et initiatives en sécurité de l'information.

5.6 Officière ou officier de la sécurité de l'information

Sous l'autorité de la dirigeante ou du dirigeant de l'information, l'officière ou l'officier de la sécurité de l'information représente l'autorité exécutive en matière de sécurité de l'information :

- définit et met en œuvre la stratégie de sécurité de l'information, en l'alignant sur les normes et exigences réglementaires applicables
- assure le développement et le suivi de la maturité organisationnelle en sécurité de l'information
- prend des décisions immédiates en cas d'incident majeur et coordonne les interventions avec les unités concernées, internes ou externes
- valide la conformité aux lois, règlements et obligations contractuelles en vigueur
- supervise la gestion des risques et exige la mise en œuvre des mesures correctives nécessaires
- ordonne la mise en place immédiate de mesures de sécurité lorsqu'une situation le justifie
- veille à l'élaboration, à la mise à jour et au maintien d'un plan intégré de reprise informatique

Cette personne agit à titre de cheffe ou chef de la sécurité de l'information organisationnelle tel que défini par la Directive gouvernementale de la sécurité de l'information du gouvernement du Québec

5.7 Responsables de la sécurité de l'information

Sous l'autorité fonctionnelle de l'officière ou de l'officier de la sécurité de l'information :

- planifient, définissent, conçoivent et intègrent la sécurité de l'information dans tous les actifs informationnels de leur secteur d'activité respectif afin de maintenir et améliorer la performance et la conformité de l'organisation en matière de sécurité de l'information
- veillent à ce qu'un profil de sécurité de l'information soit attribué adéquatement aux actifs informationnels de leur secteur d'activités
- veillent à ce que des mesures respectant le profil de sécurité de l'information des actifs informationnels soient mises en place dans leur secteur d'activité
- participent à la définition de la stratégie de cyberdéfense de l'Université
- effectuent une reddition de comptes à l'officière ou à l'officier de la sécurité de l'information sur la mise en œuvre du plan de traitement des risques et sur les risques de leur secteur d'activité en matière de sécurité de l'information
- collaborent à la gestion des incidents en matière de sécurité de l'information associés à leur secteur d'activité

5.8 Centre de cyberdéfense

Sous l'autorité de l'officière ou de l'officier de la sécurité de l'information :

- responsable de surveiller et de répondre aux événements de cybersécurité dans un objectif d'assurer la cyberdéfense des actifs informationnels numériques de l'Université
- reçoit, évalue et traite les signalements d'événements de cybersécurité

- communique et supporte les responsables de la sécurité de l'information ou les personnes répondantes du Réseau de cyberdéfense concernant les signalements d'événements de cybersécurité ou des incidents de cybersécurité
- collabore avec les équipes de sécurité opérationnelle gouvernementales
- exécute, dans le cas d'un incident de cybersécurité, les actions énoncées par le cahier des directives en matière de gestion des incidents de sécurité informationnelle
- effectue une reddition de comptes à l'officière ou à l'officier de la sécurité de l'information sur les événements et incidents en cybersécurité

5.9 Réseau de cyberdéfense

Le Réseau de cyberdéfense regroupe des personnes répondantes en sécurité de l'information désignés par les faculté, directions, services, centres et instituts de recherche et les personnes spécialistes en sécurité de l'information que sont les membres du Centre de cyberdéfense et les responsables de la sécurité de l'information. Ce réseau assure un partage d'informations, une coordination efficace et une concertation continue pour protéger l'Université contre les menaces en cybersécurité. Il participe et contribue à la coordination des actions de conception et de déploiement de la stratégie de cyberdéfense de l'Université, ainsi qu'au traitement des incidents de cybersécurité à portée institutionnelle sous la coordination de l'officière ou de l'officier de la sécurité de l'information.

5.10 Cheffe ou chef de la protection des renseignements personnels

Responsable de la protection des renseignements personnels à l'Université, cette personne :

- travaille en étroite collaboration avec l'officière ou l'officier de la sécurité de l'information afin de s'assurer que des mesures de sécurité de l'information adéquates sont mises en place concernant les renseignements personnels
- s'impliqué dans le traitement des incidents de sécurité de l'information lorsque ceux-ci contiennent des renseignements personnels

5.11 Gestionnaires

Personnes administratrice ou administrateur, une directrice ou un directeur ainsi que tout personnel cadre dont l'unité administrative est responsable d'un actif informationnel ou d'un système d'information. Ces personnes sont responsables de :

- mettre en œuvre des capacités opérationnelles en fonction des directives et normes de sécurité de l'information de l'Université
- d'inventorier les actifs informationnels et systèmes d'information sous leur responsabilité
- mettre en œuvre des mesures de sécurité de l'information définies par l'Université
- collaborer avec l'officière ou l'officier de la sécurité de l'information lors du traitement des vulnérabilités ou des incidents de sécurité de l'information

5.12 Membres

Respecte la Politique de sécurité de l'information et participe aux formations proposées par l'Université afin d'adopter des comportements sécuritaires face aux risques de sécurité de l'information.

6. RÉVISION DE LA POLITIQUE

La présente politique est sous la responsabilité du Vice-rectorat aux infrastructures et à la transformation. Elle est révisée au besoin, mais au minimum tous les trois ans à compter de sa date d'adoption.

7. DISPOSITION FINALE

La Politique entre en vigueur lors de son adoption par le Conseil d'administration.

ANNEXE 1 – COMITÉ DE SÉCURITÉ DE L'INFORMATION

Mandat

Le Comité de sécurité de l'information est l'instance de concertation en matière de sécurité de l'information de l'Université. Plus particulièrement, il :

- Examine et formule des recommandations concernant les orientations, les politiques, les directives, les cadres de gestion, les plans d'action et les bilans de l'Université, ainsi que toute proposition d'action ou d'état d'avancement de projets en sécurité de l'information
- S'assure de la prise en charge des risques identifiés au registre de risques de sécurité de l'information, des situations vulnérables ou de menaces, ou des incidents de sécurité de l'information identifiés
- Analyse et formule des recommandations concernant incidents de sécurité de l'information ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'Université

Composition

Les membres du comité de sécurité de l'information de l'Université sont :

- La dirigeante ou le dirigeant de l'information
- L'officière ou l'officier de la sécurité de l'information
- La directrice ou le directeur de la Direction des technologies de l'information
- Une personne experte en sécurité de l'information provenant des membres de l'Université, si possiblement, provenant du corps professoral
- La directrice ou le directeur du Service de sécurité et de prévention
- Une personne désignée par la Vice-rectrice ou vice-recteur à la recherche, à la création et à l'innovation
- La dirigeante ou le dirigeant de la gouvernance des données
- Cheffe ou chef de la protection des renseignements personnels