

POLITIQUE 2500-036

TITRE :	Politique de sécurité de l'information		
ADOPTION :	Conseil d'administration	Résolution :	CA-2016-09-26-19
ENTRÉE EN VIGUEUR :	2016-09-26		
MODIFICATION :	Conseil d'administration	Résolution :	CA-2025-03-24-11

TABLE DES MATIÈRES

PRÉAMBULE	2
1. CADRE LÉGAL ET ADMINISTRATIF	2
2. DÉFINITIONS	2
3. OBJECTIFS	4
4. CHAMP D'APPLICATION	4
5. PRINCIPES DIRECTEURS	4
5.1 Protéger les actifs informationnels en fonction de leur criticité et des risques encourus	5
5.2 Gérer efficacement les accès aux actifs informationnels critiques	5
5.3 Assurer le respect des réglementations et des normes applicables	5
5.4 Promouvoir la sécurité de l'information au sein de la communauté universitaire	5
5.5 Protéger les renseignements personnels	5
5.6 Permettre la continuité des activités	5
6. CADRE DE GOUVERNANCE ET DE GESTION	6
6.1 Les trois lignes de protection	6
6.2 Rôles et responsabilités	7
6.2.1 Les instances institutionnelles	7
6.2.2 Les comités	8
6.2.3 Les principaux intervenants	9
7. SANCTIONS	14
8. DIFFUSION ET MISE À JOUR DE LA POLITIQUE	14
9. ENTRÉE EN VIGUEUR	14

NOTE AU LECTEUR

Cette Politique est un cadre général en matière de sécurité de l'information. Il s'opérationnalise de multiples façons, par exemple : par un cadre normatif, de multiples normes, des procédures et des directives.

La Politique est complétée notamment par la *Directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels* (Directive 2600-063), les *Règles de gouvernance des renseignements personnels* (Politique 2500-051) et la *Directive relative à la protection des renseignements personnels* (Directive 2600-094).

PRÉAMBULE

L'Université de Sherbrooke reconnaît que l'information est une ressource stratégique essentielle à la réalisation de ses missions d'enseignement et de recherche ainsi qu'à la performance et à la pérennité de ses opérations. Cette information peut être sur papier ou support technologique.

Les trois vocations capitales de la sécurité de l'information sont de préserver adéquatement la confidentialité, garantir l'intégrité et assurer la disponibilité de l'information et des actifs informationnels de l'Université, et ce tout au long de leur cycle de vie.

Au regard des différentes menaces à la sécurité de l'information, il est incontournable de mettre en œuvre des mesures de protection et de prévention adaptées et proportionnelles aux risques et menaces anticipés en s'appuyant sur le cadre normatif applicable à l'Université de Sherbrooke, tout en réalisant de façon efficace sa mission.

1. CADRE LÉGAL ET ADMINISTRATIF

La *Politique de sécurité de l'information* s'inscrit notamment 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 c. G-1.03);
- La *Loi concernant le cadre juridique des technologies et l'information* (RLRQ c. C-1.1);
- La *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, (RLRQ c. A -2.1);
- La *Politique gouvernementale de cybersécurité* (mars 2020);
- La *Directive gouvernementale sur la sécurité de l'information* (décret 1514-2021 décembre 2021).

En novembre 2024, l'Université a adopté le *Cadre de référence en gouvernance informationnelle* (Directive 2600-102), afin de façon progressive, ajuster les politiques, directives et procédures existantes et de guider l'élaboration de celles à venir, permettant de répondre aux besoins de l'Université en matière de gouvernance informationnelle. Ainsi, la mise à jour de la *Politique de sécurité de l'information* s'appuie sur ce cadre de référence.

2. DÉFINITIONS

Actif informationnel

Une information, une banque d'informations, 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 l'Université 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.

Cadre normatif en sécurité de l'information

Ensemble des documents de référence définissant des politiques, directives, normes et procédures à respecter en sécurité de l'information.

Catégorisation

Le processus d'assignation d'une valeur à certaines caractéristiques d'une information, qualifiant le degré de sensibilité de cette information et, conséquemment, la protection à lui accorder en termes de disponibilité, d'intégrité et de confidentialité.

Communauté universitaire

Ensemble des étudiantes et étudiants, des membres du personnel, des professeures associées ou professeurs associés, des membres d'une instance décrite dans les Statuts de l'Université de Sherbrooke, ainsi que toute personne accueillie en vertu d'une convention de travail, d'études ou de stages.

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.

Détentrice ou détenteur d'actifs informationnels

Le membre du personnel cadre détenant la plus haute autorité au sein d'une unité académique 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.

Disponibilité

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

Incident de sécurité

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.

Informations

Des données qui ont été consignées dans un contexte de signification particulière, sur un support quelconque pour être conservé, traité ou communiqué comme étant un 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.

Renseignement personnel

Tout renseignement qui concerne une personne physique et qui permet, directement ou indirectement, de l'identifier. Le nom d'une personne, pris isolément, n'est pas un renseignement personnel. Cependant, lorsque ce nom est associé ou jumelé à un autre renseignement visant cette même personne, il devient alors un renseignement personnel. Un renseignement personnel est un actif informationnel.

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 de l'Université.

Sécurité de l'information

La protection de l'information et des systèmes d'information contre les risques de sécurité de l'information et les incidents afin de préserver leur disponibilité, leur intégrité et leur confidentialité.

Système d'information

L'ensemble organisé de moyens mis en place pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information en vue de répondre à un besoin déterminé, y incluant notamment les applications, progiciels, logiciels, technologies de l'information et les procédés utilisés pour accomplir ces fonctions.

Technologie de l'information

Tout logiciel ou matériel électronique et toute combinaison de ces éléments utilisés pour recueillir, emmagasiner, traiter, communiquer, protéger ou éliminer l'information sous toute forme (textuelle, symbolique, sonore ou visuelle).

Utilisatrice ou utilisateur

Toute personne qui, dans le cadre de ses fonctions, conserve l'information que l'Université détient dans l'accomplissement de sa mission, ainsi que les ressources qui la sous-tendent ou toute personne physique, appartenant ou non à la communauté universitaire, autorisée à accéder à une information appartenant à l'Université ou sous la responsabilité de l'Université au moyen de l'un de ses systèmes d'information.

3. OBJECTIFS

La Politique vise à faire de l'Université de Sherbrooke une organisation protégée et résiliente qui limite de manière proactive l'occurrence et les impacts, le cas échéant, d'une violation en matière de sécurité de l'information tout en prenant compte les besoins de la communauté à l'égard des données institutionnelles.

Les objectifs spécifiques sont :

1. Préciser les rôles et responsabilités des diverses instances et parties prenantes;
2. Établir et maintenir un programme de conformité de la sécurité de l'information au sein de l'Université;
3. Mettre en œuvre une stratégie afin d'assurer la continuité des activités au sein de l'Université;
4. Favoriser l'adoption de comportements sécuritaires par les membres de la communauté universitaire.

4. CHAMP D'APPLICATION

La Politique vise, sans exception, l'ensemble des membres de la communauté universitaire qui conçoivent, développent, hébergent ou utilisent des actifs informationnels.

Elle s'applique également à tout utilisateur externe (par exemple : consultant, partenaire ou fournisseur) autorisé à accéder, à exploiter ou à héberger de l'information et à utiliser les actifs informationnels de l'Université.

L'information et les actifs informationnels visés par la Politique sont ceux :

- Appartenant à l'Université et détenus par elle ou par un tiers;
- Utilisés et détenus par un tiers au bénéfice et au nom de l'Université;
- Conservés sur un support tangible ou intangible.

Les activités visées par la Politique sont la cueillette, la consultation, la production, la transmission, la conservation et la destruction de l'information et des actifs informationnels, peu importe leur support, leur emplacement, le moyen de communication, que ces activités soient conduites sur les campus de l'Université ou dans un autre lieu.

5. PRINCIPES DIRECTEURS

Les principes directeurs suivants guident les actions de l'Université en matière de sécurité de l'information.

5.1 Protéger les actifs informationnels en fonction de leur criticité et des risques encourus

L'Université adopte une approche stratégique de la sécurité de l'information en identifiant et en catégorisant ses actifs informationnels, en évaluant les risques et en mettant en place des mesures de protection et de mitigation appropriées pour préserver la sécurité des informations en fonction de leur criticité et des risques encourus.

L'Université protège ses actifs par une gestion efficace des événements de sécurité de l'information et le traitement adéquat des vulnérabilités identifiées.

5.2 Gérer efficacement les accès aux actifs informationnels critiques

L'Université met en place des processus et des mesures pour que seuls les individus dûment autorisés aient accès aux ressources informatiques et informationnelles strictement nécessaires à leurs fonctions et responsabilités, réduisant ainsi les risques de fuites de données, de violations de sécurité et de perturbations opérationnelles.

5.3 Assurer le respect des réglementations et des normes applicables

L'Université respecte les lois, les réglementations et les normes applicables par des moyens raisonnables tout en maintenant un niveau élevé de sécurité pour les informations sensibles. En outre, l'Université met en œuvre des outils d'audit et de vérification interne de sa conformité.

5.4 Promouvoir la sécurité de l'information au sein de la communauté universitaire

L'Université informe et mobilise les membres de la communauté sur les meilleures pratiques en matière de sécurité de l'information et les comportements à adopter pour protéger les actifs informationnels et les informations ainsi que sur les mesures pour éviter les risques. Ceci s'effectue notamment par leur participation à des activités de sensibilisation et de formation, renforçant leur compréhension et capacité reconnaître les risques, signaler les incidents et se conformer au cadre normatif en vigueur.

5.5 Protéger les renseignements personnels

L'Université est responsable des renseignements personnels qu'elle détient dans l'exercice de ses fonctions, que sa conservation soit assurée par l'Université ou par un tiers. À ce titre, elle prend les mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support.

Ce principe directeur est plus amplement défini par les *Règles de gouvernance à l'égard des renseignements personnels* (Politique 2500-051) et la *Directive relative à la protection des renseignements personnels* (Directive 2600-094).

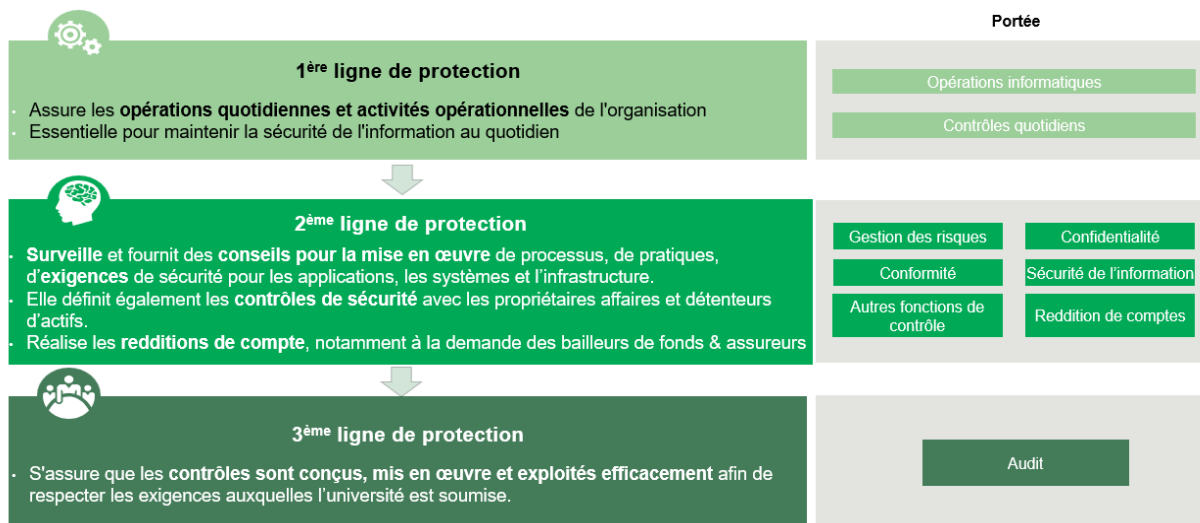
5.6 Assurer la continuité des activités

L'Université prend les mesures en vue de maintenir ses opérations essentielles, même en cas d'incidents, de sinistres ou de perturbations. Elle développe une résilience globale renforçant ainsi sa capacité à poursuivre sa mission et ses activités tout en préservant la sécurité de l'information et des actifs institutionnels.

6. CADRE DE GOUVERNANCE ET DE GESTION

La gouvernance en sécurité de l'information de l'Université de Sherbrooke s'inspire de la *Directive gouvernementale sur la sécurité de l'information* (2020) et du modèle de l'*Institute of Internal Auditors* (« IIA »)¹. La gouvernance et la gestion de la sécurité de l'information est un modèle fondé sur les trois lignes de protection selon groupes de fonctions impliqués dans la gestion efficace des risques liés à la sécurité de l'information.

6.1 Les trois lignes de protection



1^{ère} ligne de protection

Cette ligne assure la protection des actifs informationnels de l'Université par la mise en œuvre de mesures visant à réduire les risques, de toutes formes, d'atteinte à la disponibilité, la confidentialité ou l'intégrité de l'information, telles des vulnérabilités, des menaces ou des cyberattaques et par la mise en place d'actions préventives et correctives permettant de remédier aux lacunes des processus et des contrôles.

Cette première ligne met en œuvre toute action requise pour la prise en charge d'un événement de sécurité de l'information.

Elle est constituée principalement par le personnel du Service des technologies de l'information (STI) et des services informatiques facultaires (SIF). La personne responsable de la protection des renseignements personnels joue aussi un rôle clé au niveau de cette 1^{ère} ligne.

2^e ligne de protection

La 2^e ligne de protection s'assure de la mise en place d'actions visant à atteindre la conformité aux différentes normes en sécurité de l'information.

Elle participe au processus de gestion intégrée des risques institutionnels en effectuant l'analyse des risques liés à la sécurité de l'information notamment en soutenant les personnes détentrices d'actifs informationnels dans la détermination des niveaux de risque visés. Elle facilite et s'assure de la mise en place de dispositifs efficaces de mitigation des risques au sein des unités.

¹ [Institute of Internal Auditors](#)

Elle communique aux membres de la communauté universitaire des informations relatives aux risques relatifs à la sécurité de l'information ainsi que les mesures et pratiques à adopter afin de mitiger ces risques.

La 2^e ligne est notamment assurée par le membre du comité de direction de l'Université de qui relève la gouvernance de la sécurité de l'information, en collaboration avec la vice-rectrice adjointe ou le vice-recteur adjoint à la sécurité de l'information occupant le rôle de chef de la sécurité de l'information organisationnelle (CSIO).

3^e ligne de protection

La 3^e ligne assure l'évaluation systématique et indépendante des processus de gestion des risques, de contrôle et de gouvernance. Elle donne une assurance objective sur la suffisance et l'efficacité de la gouvernance en sécurité de l'information et de la gestion des risques au sein de l'Université, incluant les contrôles maintenus par les parties externes.

Pour permettre de conserver son indépendance, cette ligne est assumée par le Bureau de l'audit interne.

6.2 Rôles et responsabilités

6.2.1 Les instances institutionnelles

6.2.1.1 Conseil d'administration

Le conseil d'administration adopte la *Politique de sécurité de l'information* (Politique 2500-036). Le conseil est régulièrement informé des actions de l'Université en matière de sécurité de l'information notamment par le suivi de la gestion intégrée des risques et l'adoption du Plan directeur en ressources informationnelles et ses financements associés.

6.2.1.2 Comité de gouvernance des ressources informationnelles

Le comité de gouvernance des ressources informationnelles du conseil d'administration a le mandat d'examiner les règlements, les politiques, les orientations, les stratégies et les pratiques générales de l'Université ayant une incidence sur la gestion des ressources informationnelles et de formuler des recommandations au conseil d'administration.

Le comité reçoit et examine périodiquement des rapports d'audits et de conformité eu égard au cadre normatif afférent à la sécurité de l'information et des systèmes d'information applicables à l'Université ainsi qu'aux plans d'action pour corriger les écarts.

Dans le cadre du processus institutionnel de la gestion intégrée des risques, le comité suit l'évolution des risques institutionnels en matière de sécurité de l'information et de technologies informationnelles ainsi que les mesures de mitigation prioritaires.

6.2.1.3 Comité des finances et d'audit

Le comité des finances et d'audit du conseil d'administration a le mandat d'étudier le plan directeur en ressources informationnelles et les financements associés tels que proposés par la direction de l'Université, soumettre à celle-ci les suggestions qu'il juge appropriées et soumettre au conseil d'administration ses recommandations à ces égards.

Il valide l'application par l'Université d'un processus institutionnel évolutif, efficace et permanent de l'identification et de la gestion des risques, y compris les risques ESG, et examine biennuellement le plan d'action en découlant. Il confie cette responsabilité au comité de gouvernance des ressources informationnelles eu égard aux risques liés à la sécurité de l'information et aux technologies informationnelles.

6.2.1.4 Comité de planification

Selon l'article 39 des *Statuts de l'Université de Sherbrooke*, le comité de planification constitue un lieu privilégié pour discuter de tout défi relatif au développement de la mission universitaire dévolue aux facultés. Ce comité est complémentaire au comité stratégique de sécurité de l'information afin de recueillir et de prendre en compte les appréciations et les recommandations des doyennes et des doyens en regard des initiatives en sécurité de l'information.

6.2.1.5 Comité de direction de l'Université

Le comité de direction obtient l'assurance raisonnable que l'Université agit en conformité du cadre législatif et réglementaire applicable. Il s'assure que le cadre normatif est respecté et mis à jour périodiquement ainsi que des mesures de contrôle adéquates sont en place.

Il reçoit les bilans de sécurité de l'information. Il adopte des directives et des procédures afin de préciser ou de soutenir l'application de la *Politique de sécurité de l'information* (Politique 2500-036). Il alloue les ressources financières, humaines et technologiques en matière de sécurité de l'information en se souciant d'améliorer la performance de l'Université.

Il suit l'évolution des risques institutionnels et met en place des contrôles utiles.

6.2.2 Les comités

6.2.2.1 Comité stratégique de sécurité de l'information

Le comité stratégique de sécurité de l'information analyse et prend les décisions appropriées eu égard :

- Aux faits saillants sur les enjeux institutionnels et les recommandations issus du Comité tactique en sécurité de l'information;
- Aux tableaux de bord de gestion stratégique en sécurité de l'information;
- Aux mesures de mitigation recommandées concernant les risques en sécurité de l'information identifiés par le comité tactique en sécurité de l'information, ainsi qu'à l'avancement des travaux à risque reliés aux mesures de mitigations retenues;
- À la réalisation du plan stratégique.

Ce comité consulte les instances institutionnelles appropriées en vue de l'exercice optimal de son mandat.

Le comité est composé des personnes suivantes :

- Le membre du comité de direction de l'Université de qui relève la gouvernance de la sécurité de l'information qui préside;
- Le membre du comité de direction de l'Université de qui relève le Service des technologies de l'information;
- La secrétaire générale ou le secrétaire général;
- La cheffe ou le chef de la sécurité de l'information organisationnel;
- Le vice-rectorat adjoint à la transformation numérique (vue d'ensemble sur l'architecture d'entreprise et le Bureau de projet);
- La direction générale du Service des technologies de l'information.

Des personnes sont invitées selon leur expertise ou leurs responsabilités institutionnelles.

6.2.2.2 Comité tactique de sécurité de l'information

Le comité tactique de sécurité de l'information est notamment chargé d'examiner et de formuler des recommandations concernant les politiques, les directives, les plans d'action, les bilans de l'Université ainsi que l'état d'avancement des travaux, initiatives, projets liés à la sécurité de l'information.

Le mandat de ce comité tactique consiste également à :

- Analyser et formuler des recommandations sur les principes généraux, les orientations, les axes stratégiques de sécurité de l'information;
- Recevoir les résultats de l'analyse des risques en sécurité de l'information, identifier les mesures de mitigation et estimer l'impact attendu des mesures sur le degré de mitigation du risque selon des paramètres reconnus;
- Analyser et formuler des recommandations concernant les événements ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'Université, qui ne sont pas traités en vertu de la *Directive relative à la gestion des situations d'exception* (Directive 2600-097);
- Suivre la mise en œuvre des plans d'action à l'aide d'indicateurs d'avancement qui permettent de mesurer le déploiement des projets de sécurité, qui ne sont pas suivis par les comités directeurs des projets;
- Analyser périodiquement les indicateurs issus des tableaux de bord utiles visant à suivre l'efficacité des mesures mises en place et la détection des menaces et vulnérabilités;
- Identifier les travaux visant une optimisation et une synergie entre les trois lignes de prévention;
- Coordonner les activités liées à la sécurité de l'information;
- S'assurer de la tenue des activités de sensibilisation et de formation pour les membres de la communauté universitaire;
- Assurer tout autre mandat confié par les membres du comité de direction de l'Université de qui relève le STI, la sécurité de l'information ou la transformation numérique.

Ce comité formule ses recommandations au comité stratégique de sécurité de l'information ou aux vice-recteurs concernés.

Le comité est composé des personnes suivantes :

- La cheffe ou le chef de la sécurité de l'information organisationnelle qui préside;
- Les conseillères ou les conseillers en sécurité de l'information;
- Les coordonnatrices et les coordonnateurs organisationnels des mesures de sécurité de l'information;
- La direction de la sécurité et gestion des identités et des accès du Service des technologies de l'information;
- Deux directrices ou directeurs de services informatiques facultaires.

Des personnes sont invitées selon leur expertise ou leurs responsabilités institutionnelles.

6.2.3 Les principaux intervenants

6.2.3.1 Dirigeante de l'organisme ou dirigeant de l'organisme public (DO)

La personne dirigeante d'organisme public est la première responsable de la sécurité de l'information. À ce titre, la rectrice ou le recteur veille au respect du cadre gouvernemental de gestion de la sécurité de l'information et s'acquitte de ses obligations telles qu'elles sont édictées dans la *Directive gouvernementale sur la sécurité de l'information* (2021).

Elle ou il désigne la cheffe de la sécurité de l'information organisationnelle ou le chef de la sécurité de l'information organisationnelle (CSIO) et la personne responsable de la protection des renseignements personnels, et leur attribue les responsabilités définies par les lois.

À l'Université de Sherbrooke, certaines fonctions sont déléguées par la rectrice ou le recteur à un membre du comité de direction de l'Université dans le but d'assurer la gestion et l'administration efficaces de la sécurité de l'information au sein de l'Université. À cet effet, elle ou il s'assure des éléments suivants:

- Respect des lois, des orientations et des règles de sécurité de l'information gouvernementales qui s'appliquent à l'Université;

- Mise en œuvre des processus de sécurité de l'information permettant, notamment, de veiller à la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents;
- Mise en place d'un programme de formation et de sensibilisation du personnel en matière de sécurité de l'information.

6.2.3.2 Le membre du comité de direction de l'Université de qui relève la gouvernance de la sécurité de l'information

Par délégation de la dirigeante ou du dirigeant d'organisme, ce membre du comité de direction est chargé d'approuver, de coordonner et de mettre en œuvre les mesures de sécurité de l'information, visant à assurer la protection de l'Université contre les menaces et les risques en sécurité de l'information, et ce dans le respect des mandats des instances. À cet effet, elle ou il :

- Veille à l'application de la *Politique de sécurité de l'information* (Politique 2500-036), ainsi que toutes les directives en découlant;
- Représente l'Université en matière de sécurité de l'information ou désigne une ou des personnes pour agir en cette qualité;
- Fait adopter les orientations stratégiques, les évaluations de risques, les bilans de sécurité, les redditions de compte en matière de sécurité de l'information par les instances appropriées;
- Autorise une dérogation à l'une ou l'autre des dispositions d'une directive ou d'une procédure institutionnelle ayant une incidence directe ou indirecte sur la sécurité de l'information et qui serait incompatible avec une activité ou un projet directement relié à la mission de l'Université;
- Autorise une enquête lorsqu'une contravention réelle ou apparente aux documents officiels en sécurité de l'information est signalée;
- Tient à jour le registre des dérogations et le registre des cas de contraventions.

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

La personne responsable de l'accès à l'information et de la protection des renseignements personnels veille au respect de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (RLRQ c. A -2.1).

Relativement à la sécurité de l'information, cette personne contribue à assurer la cohérence et l'harmonisation des interventions entre la sécurité de l'information, l'accès aux documents et la protection des renseignements personnels.

6.2.3.4 Cheffe de la sécurité de l'information organisationnelle ou chef de la sécurité de l'information organisationnelle (CSIO)

La personne occupant les fonctions de CSIO est un membre du personnel cadre qui assume le rôle de responsable de la sécurité de l'information au sens du *Cadre gouvernemental de gestion de la sécurité de l'information*. Cette personne soutient le membre du comité de direction de l'Université de qui relève la gouvernance de la sécurité de l'information en contribuant notamment à la mise en place des processus de sécurité de l'information et des mesures d'atténuation des risques. À cet égard, elle :

- Coordonne les analyses de risques de sécurité de l'information, identifie les menaces et les situations de vulnérabilité afin de mettre en œuvre les solutions appropriés;
- Élabore, propose et met à jour le programme de sécurité de l'information de l'Université incluant ses objectifs et rend compte de son implantation;
- Voit à la mise à jour du cadre normatif de sécurité de l'information;
- Formule des recommandations concernant les besoins, les priorités, les orientations, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information;

- Soutient les unités concernées afin que les ententes de service et les contrats conclus avec les prestataires de services, les partenaires et les mandataires comportent des clauses concernant les exigences de sécurité de l'information;
- Assure la coordination et la cohérence des actions menées au sein de l'Université en matière de sécurité de l'information, notamment en conseillant les détentrices ou les détenteurs d'actifs informationnels dans les unités;
- Produit les bilans et les redditions de compte en matière de sécurité de l'information;
- S'assure de la déclaration, par l'Université, des risques et des incidents de sécurité de l'information à portée gouvernementale;
- Mets en place le programme de sensibilisation et de formation;
- Procède aux enquêtes de contravention présumée sur du membre du comité de direction de l'Université de qui relève la gouvernance de la sécurité de l'information;
- Assure les veilles normatives, juridiques, gouvernementales et technologiques;
- S'assure de la mise en place d'un processus de gestion des incidents, des menaces et des vulnérabilités (GMVI) conformément au processus ministériel de GMVI.

6.2.3.5 Direction générale du Service des technologies de l'information (STI)

La direction générale du STI ainsi que les différents secteurs du STI contribuent à la sécurité de l'information des actifs placés sous sa responsabilité et, de concert avec la ou le CSIO, ils conseillent la direction de l'Université, les facultés, les instituts et les services en matière de sécurité, tout en s'assurant que ces actions sont alignées avec l'architecture d'entreprise et les orientations stratégiques de l'Université.

En étroite collaboration avec la ou le CSIO, la direction générale agit à titre de personne de référence pour la gestion de la sécurité de l'information à l'Université.

Plus spécifiquement, l'équipe du secteur de la sécurité informatique et gestion des identités et des accès supervise les activités opérationnelles rattachées à la sécurité de l'information de façon à assurer la disponibilité, l'intégrité et la confidentialité des données sous la responsabilité du service. De plus, elle coordonne les activités rattachées à la gestion des identités et des accès de façon à assurer que les personnes, objets, programmes et services soient identifiés et détiennent les accès minimaux requis. Cette équipe collabore étroitement avec la ou le CSIO.

L'équipe de l'infrastructure technologique collabore étroitement la ou le CSIO dans la planification et le suivi du Plan triennal d'investissement et des plans annuels en découlant.

L'ensemble des responsabilités du STI à l'égard de la sécurité de l'information sont décrites au Plan d'organisation du STI, tel qu'adopté par le comité de direction.

6.2.3.6 Direction générale du Service de la mobilité, de la sécurité et de la prévention (SMSP)

La direction générale du SMSP met en place les mesures de protection physique des locaux et de sécurisation de leurs accès, notamment lorsqu'ils abritent des systèmes et des installations technologiques stratégiques ou essentielles ou des supports de l'information confidentielle.

Cette personne est responsable de la gestion des situations d'exception. Ainsi, elle coordonne le comité tactique de la gestion des incidents de sécurité de l'information. La ou le CSIO participe au comité stratégique des situations d'exception lors d'événements de sécurité de l'information.

6.2.3.7 Direction générale du Service des bibliothèques et archives

La direction générale du Service des bibliothèques et archives s'assure de la mise à jour de la *Politique relative à la gestion intégrée des documents administratifs et des archives institutionnelles* (Politique 2500-050) qui prescrit l'utilisation d'outils de gestion documentaire tels que le plan de classification, le calendrier de conservation ainsi que le logiciel institutionnel de gestion intégrée de documents. Les principes de cette Politique permettent aux membres du personnel d'organiser leurs documents, quel

que soit leur support (physique ou numérique), leur nature (administrative, financière, légale, historique), qu'ils soient créés ou reçus par un membre du personnel de l'Université, et ce, tout au long de leur cycle de vie et ce, considérant que ces documents peuvent comporter des renseignements personnels ou des renseignements anonymisés.

Ce Service développe des outils technologiques facilitant la découverte de l'information et de la documentation sous tous les formats.

6.2.3.8 Direction générale du Service des ressources humaines

En matière de sécurité de l'information, la direction générale du Service des ressources humaines informe tout nouvel employé de la *Politique de sécurité de l'information* (Politique 2500-036).

6.2.3.9 Auditrice ou auditeur interne

L'auditrice ou l'auditeur interne fournit une assurance indépendante et objective sur la suffisance et l'efficacité de la gouvernance, des processus de gestion des risques et des mécanismes de contrôle interne, de l'efficacité et de l'efficacité des opérations, de la protection des actifs informationnels et de la fiabilité et l'intégrité de leur processus de divulgation.

6.2.3.10 Détentrice ou détenteur (ou propriétaire) d'actif informationnel

En collaboration avec les équipes expertes en sécurité informatique et en sécurité de l'information, la détentrice ou le détenteur, soit le propriétaire, d'actif informationnel :

- Informe son personnel et les tiers avec lesquels l'unité transige, des dispositions de la présente Politique afin de le sensibiliser à la nécessité de s'y conformer;
- Catégorise les actifs informationnels relevant de sa responsabilité en termes de disponibilité, intégrité et confidentialité;
- Identifie les risques de sécurité d'information dans ses processus, effectue la gestion et le suivi des risques résiduels et faire rapport au CSIO des risques significatifs non mitigés;
- Réalise, avec le soutien du conseiller sécurité de l'information, le bilan d'impact sur l'activité et le plan de continuité des opérations des actifs informationnels sous sa responsabilité;
- Veille à la protection de l'information et des systèmes d'information sous sa responsabilité;
- S'assure 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 sa responsabilité et voit à ce que tout fournisseur, partenaire, invité, organisme ou firme externe s'engage à respecter la Politique;
- Rapporte au STI toute menace ou tout incident afférant à la sécurité de l'information des actifs informationnels dont il a la responsabilité;
- Collabore 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;
- Rapporte au CSIO tout problème lié à l'application du cadre normatif dont toute contravention réelle ou apparente d'un membre du personnel à l'égard de l'application du cadre normatif;
- Autorise les accès à ses actifs ou leurs retraits.

6.2.3.11 Conseillère organisationnelle ou conseiller organisationnel des mesures de sécurité de l'information (COMSI)

La ou le COMSI, sous l'autorité de la direction du STI, participe activement au réseau d'alerte gouvernemental et collabore étroitement avec la ou le CSIO. Elle ou il a notamment responsabilités suivantes :

- Contribuer à la mise en place du processus de gestion des incidents de sécurité de l'information;
- Tenir à jour le registre des incidents ayant pu mettre en péril la sécurité de l'information, de documenter ces incidents et d'en tenir informé la personne CSIO;

- Contribuer aux analyses de risques de sécurité de l'information, aux audits et aux évaluations de conformité afin d'identifier les menaces et les situations de vulnérabilité et de mettre en œuvre les solutions appropriées;
- Élaborer et tenir à jour les guides portant sur la sécurité opérationnelle des systèmes et des réseaux de télécommunications et maintenir une veille continue sur les risques, les menaces et les vulnérabilités;
- Assurer la coordination de l'équipe de réponse aux incidents de sécurité de l'information et mettre en œuvre les stratégies appropriées.

6.2.3.12 Conseillère en sécurité de l'information ou conseiller en sécurité de l'information

Sous l'autorité du CSIO, la personne conseillère en sécurité de l'information apporte son soutien au CSIO lors de la mise en œuvre des mesures d'atténuation des risques et à la mise en place des projets et processus de sécurité de l'information en fournissant, en autres, une expertise technique. Elle ou il a notamment les responsabilités suivantes:

- Mettre en œuvre les plans d'action en matière de sécurité de l'information en collaboration et dans le respect des responsabilités des différentes parties prenantes;
- Réaliser les analyses de risque, identifier les vulnérabilités et recommander des mesures d'atténuation, de concert avec les services et facultés;
- Soutenir les audits internes et externes de sécurité, voir à la rédaction des réponses et à la mise en œuvre des recommandations d'audits de concert avec les services et facultés;
- Apporter les réponses nécessaires à la communauté concernant les questions liées à la sécurité de l'information;
- Assurer la réalisation des travaux liés à la catégorisation et au bilan d'impact sur les activités des actifs avec les détenteurs d'actifs;
- Contribuer au plan de continuité des opérations en collaboration avec les différentes unités.

6.2.3.13 Responsable des services informatiques facultaires (Responsable des SIF)

Le responsable des SIF est un membre du personnel cadre de la faculté qui est responsable de la gestion, de la protection et de la disponibilité des systèmes informatiques qui relève de son périmètre.

Cette personne collabore étroitement avec l'équipe de sécurité informatique du STI pour mettre en œuvre des stratégies de sécurité efficaces et assurer que les systèmes informatiques de la faculté sont conformes aux normes de sécurité.

Plus spécifiquement, elle ou il :

- De concert avec le détenteur d'actif, révise périodiquement les différents droits d'accès accordés aux actifs utilisés par les membres de sa faculté et est garant de toute modification ou suppression de droits le cas échéant;
- S'assure de l'application des mesures de sécurité édictées dans le cadre normatif auprès du personnel de son unité ainsi que l'adoption des bonnes pratiques par le personnel;
- Informe, dans les meilleurs délais le CSIO, les écarts identifiés aux exigences de sécurité sur leur périmètre local;
- Agit en tant que relai du CSIO sur leur périmètre local
- Propose des ajustements en considérant les spécificités de son unité, met en œuvre des mesures de sécurité appropriées, et réagit promptement en cas d'incident de sécurité.

6.2.3.14 Utilisatrice ou utilisateur

La responsabilité de la sécurité de l'information à l'Université est l'affaire de toutes les personnes utilisatrices des actifs informationnels de l'Université. Toute personne qui accède, produit ou transforme une information, la consulte ou la traite doit procéder de manière à protéger cette information.

À cette fin, l'utilisatrice ou l'utilisateur doit :

- Se conformer au cadre normatif de l'Université en matière de sécurité de l'information et d'utilisation des actifs informationnels;
- N'utiliser que l'information, les systèmes d'information et les droits d'accès mis à leur disposition dans le cadre de leurs fonctions et aux fins auxquelles ils sont destinés;
- Respecter les mesures de sécurité mises en place, ne pas les contourner ni ne modifier leur configuration ou les désactiver;
- Signaler tout incident susceptible de constituer une menace à la sécurité de l'information de l'Université;
- Collaborer promptement à toute intervention visant à identifier ou à mitiger une menace ou un incident de sécurité de l'information;
- Renouveler périodiquement son engagement à respecter les consignes de l'Université en matière de sécurité de l'information;
- Se conformer aux politiques et directives en vigueur dans un organisme ou une entreprise avec lequel elle est ou il est en relation dans le cadre de ses activités professionnelles ou d'études, lorsqu'elle ou lorsqu'il y partage des actifs informationnels, des dispositifs de technologies de l'information ou des systèmes d'information.

7. SANCTIONS

Tout utilisateur ou utilisatrice 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 ou des règles disciplinaires internes applicables, dont celles des conventions collectives de travail ou des politiques, règlements et directives appropriées.

De même, toute contravention par un fournisseur, un partenaire, un invité, un consultant ou un organisme externe l'expose aux sanctions prévues au contrat le liant à l'Université ou en vertu des dispositions de la législation applicable en la matière.

Toute contravention à la présente Politique peut entraîner, en plus des mesures prévues aux lois, règlements, politiques, directives, conventions ou ententes, les conséquences suivantes, en fonction de la nature, de la gravité et des répercussions du geste:

- L'annulation des privilèges d'accès aux actifs informationnels de l'Université (l'annulation peut être effectuée sans préavis selon la nature et la gravité de la contravention);
- L'obligation de remboursement à l'Université de toute somme que cette dernière serait dans l'obligation de défrayer à la suite d'une utilisation non autorisée, frauduleuse, ou illicite de ses services ou de ses actifs informationnels.

La *Directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels* (Directive 2600-063) décrit davantage le processus menant aux sanctions.

8. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

Le membre du comité de direction de qui relève la gouvernance de la sécurité de l'information est responsable de la diffusion et de la mise à jour de la présente Politique.

9. ENTRÉE EN VIGUEUR

La présente Politique est entrée en vigueur le 26 septembre 2016. Les dernières modifications ont été approuvées par le conseil d'administration le 24 mars 2025.