Politique de sécurité de l'information

Approbation : Conseil d'administration

Entrée en vigueur : 24 février 2021

Responsable : Vice-rectorat à l'administration

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;*
- *Directive sur la sécurité de l'information gouvernementale*;
- *Politique relative à la gestion de crise de l'Université Laval*;
- *Règlement de sécurité de l'information sur l'utilisation des actifs informationnels.*

UNIVERSITÉ LAVAL

Table des matières

PRÉAMBULE

La Politique de sécurité de l'information de l'Université Laval (ci-après, la Politique) définit des principes et rôles et responsabilités pour protéger les membres de l'Université[1] (ci-après, les membres), ses infrastructures technologiques et son information comme actif stratégique. Elle indique les attentes de l'Université liées à la protection de l'information de l'Université eu égard aux membres qui conçoivent, développent ou utilisent des systèmes d'information. Cette politique respecte les normes et la législation applicable en matière de sécurité de l'information. Le succès de sa mise en œuvre dépend d'une prise en charge pragmatique de la sécurité de l'information. Le vécu récent de plusieurs organisations confrontées à des incidents de sécurité de l'information porte à poser un regard nouveau sur les pratiques de l'Université et à les moderniser pour en arriver à des actions concertées.

Cette politique se décline en deux axes indissociables :

- La protection de l'information incluant la propriété intellectuelle de l'Université;
- La promotion d'un comportement responsable face aux risques associés à l'information.

Le premier axe vise la mise en place d'une approche de conception sécurisée ainsi que l'application de modèles de sécurité fiables et modernes. Le second axe s'assure que les membres maîtrisent l'ensemble des règles et des pratiques favorisant des comportements adéquats, notamment en ce qui a trait à l'utilisation des ressources informationnelles.

Les membres qui conçoivent, développent ou utilisent des systèmes d'information partagent des responsabilités pour assurer la sécurité de l'information à l'Université. La sécurité de l'information est un écosystème complexe dans lequel chaque individu joue un rôle primordial. Elle doit être réellement intégrée à la culture universitaire. L'Université doit sensibiliser ses membres et ses partenaires dans l'adoption d'habitudes et de comportements sécuritaires.

[1] Appellation telle que définie dans les Statuts de l'Université Laval Mars 2019 – Livre II

1. OBJECTIFS

La Politique vise à faire de l'Université Laval une institution protégée, résiliente et proactive en matière de sécurité de l'information, qui offre des services numériques de qualité aux membres de sa communauté. Sa mise en œuvre se traduit notamment par une stratégie de prévention des risques qui se décline en mesures de protection adaptées et flexibles face aux enjeux liés à la sécurité de l'information. De plus, son but est d'influencer la culture, les pratiques et les connaissances des membres qui conçoivent, développent ou utilisent des actifs informationnels.

Spécifiquement, la Politique a comme objectifs :

- De préciser les rôles et les responsabilités des divers intervenants impliqués dans la sécurité de l'information de l'Université;
- De mobiliser l'ensemble des membres de l'Université autour de la sécurité de l'information;
- D'innover dans la prise en charge des risques de sécurité de l'information de manière proactive; et
- De favoriser et d'encourager les actions de sensibilisation qui visent à promouvoir l'adoption de comportements sécuritaires auprès des membres.

2. CHAMPS D'APPLICATION

La Politique vise l'ensemble des membres de l'Université (tels que définis par les Statuts de l'Université Laval), qui conçoivent, développent ou utilisent des actifs informationnels. Elle s'applique à l'ensemble des actifs informationnels de l'Université.

3. DÉFINITIONS [2]

3.1 Actif informationnel

Tout support de l'information permettant son traitement, sa transmission ou sa conservation aux fins d'utilisations prévues.

3.2 Cyberdéfense

Ensemble des moyens mis en place par une organisation pour défendre dans le cyberespace les systèmes d'information jugés d'importance vitale, qui contribuent à assurer la cybersécurité. Dans le présent document, la notion d'importance vitale fait référence à la valeur de l'information établie selon la confidentialité, l'intégrité et la disponibilité requises et tient compte notamment d'exigences légales, réglementaires et contractuelles.

[2] Reproduites avec permission à partir de la *Politique gouvernementale de* cybersécurité, Secrétariat du conseil de trésor, 2020, p. 2.

3.3 Cyberespace

Espace virtuel constitué par l'interconnexion mondiale des systèmes informatiques, des réseaux de télécommunication et des infrastructures de technologies de l'information, qui permet l'échange d'informations entre des utilisateurs individuels ou collectifs.

3.4 Cybersécurité

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

3.5 Incident de sécurité à portée institutionnelle

Conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée institutionnelle, nécessitant une intervention concertée au plan institutionnel.

3.6 Ressource informationnelle

Ressource utilisée par une organisation dans le cadre de ses activités de traitement de l'information pour mener à bien sa mission, pour la prise de décision, ou encore pour la résolution de problèmes.

3.7 Risque de sécurité à portée institutionnelle

Le risque de sécurité à portée institutionnelle est un risque d'atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information institutionnelle, qui peut avoir des conséquences sur la prestation de 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 qui les concernent et au respect de leur vie privée, sur l'image de l'Université ou sur la prestation de services des partenaires de l'Université.

3.8 Système d'information

Système constitué de ressources informationnelles et des procédures permettant d'acquérir, de stocker, de traiter et de diffuser les éléments d'information pertinents au fonctionnement d'une organisation.

4. PRINCIPES

4.1 Identification et catégorisation des actifs informationnels

i. Les actifs informationnels sont connus et leurs responsables ont été identifiés.

ii. Un niveau de criticité des actifs informationnels est attribué en fonction de la confidentialité, de l'intégrité et de la disponibilité des informations qu'ils contiennent. Les exigences légales, réglementaires ou contractuelles sont également prises en compte.

4.2 Protection des actifs informationnels en fonction des risques encourus

i. Les actifs informationnels sont protégés par des mesures de protection déterminées en fonction du niveau de criticité attribué.

ii. En matière de sécurité de l'information, l'Université se base sur des cadres de référence reconnus, notamment ceux de l'ISO et du NIST[3]. Ces référentiels permettent d'assurer une gestion efficace de la protection des actifs informationnels.

4.3 Conception et utilisation sécurisées 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). La sécurité de l'information est aussi prise en compte lors de la fin de vie des systèmes d'information.

4.4 Uniformatisation de l'application des mesures de protection

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 des événements affectant la sécurité de l'information;

d) D'intervenir en cas d'événements affectant la sécurité de l'information; et

e) De rétablir l'actif informationnel à un état adéquat.

4.5 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 des risques auxquels ils font face. Ceci s'effectue notamment par leur participation à des formations en matière de sécurité de l'information.

4.6 Collaboration et concertation face aux risques en sécurité de l'information

i. Les facultés, directions, services, centres et instituts de recherche de l'Université mettent en commun leurs connaissances, outils et expertises dans la mise en place de saines pratiques en sécurité de l'information.

[3] NIST Cybersecurity Framework

ii. Les facultés, directions, services, centres et instituts de recherche participent au Réseau de cyberdéfense de l'Université. Ce réseau a un pôle d'expertise représenté par des spécialistes de cybersécurité de la Direction des technologies de l'information.

iii. L'Université collabore et participe aux initiatives interuniversitaires, ministérielles et gouvernementales en matière de sécurité de l'information.

5. RÔLES ET RESPONSABILITÉS

5.1 Conseil d'administration

Le Conseil d'administration de l'Université adopte la Politique suivant la recommandation du Comité des ressources immobilières et informationnelles. Il est le responsable de la sécurité de l'information à l'Université Laval. Cette responsabilité peut être déléguée.

5.2 Comité des ressources immobilières et informationnelles

Le Comité des ressources immobilières et informationnelles (CRII) recommande l'approbation de la Politique auprès du Conseil d'administration (CA).

Suivant la recommandation de la dirigeante ou du dirigeant de l'information, le CRII approuve 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 Dirigeante ou dirigeant de l'information

La dirigeante ou le dirigeant de l'information, sous l'autorité de la vice-rectrice ou du vice-recteur à l'administration :

- Conçoit et met à jour la Politique;
- S'assure de la mise en œuvre de la Politique;
- Effectue une reddition de comptes auprès du CRII;
- S'assure du respect des lois et des principes généraux de sécurité de l'information déterminés par la Politique;
- Veille à ce que des responsables soient identifiés pour la gestion des actifs informationnels de l'Université;
- Identifie et fait le suivi des risques de sécurité à portée institutionnelle; et
- S'assure de faire une reddition de comptes au Comité des ressources immobilières et informationnelles concernant l'état de protection de l'Université, des risques en sécurité de l'information ainsi que des événements de sécurité de l'information ayant eu lieu.

5.4 Officière ou officier de la sécurité de l'information

L'officière ou l'officier de la sécurité de l'information apporte son soutien à la dirigeante ou au dirigeant de l'information sur le plan stratégique et tactique, notamment dans la définition

et l'exécution d'un plan de traitement des risques se déclinant en mesures de protection. L'officière ou l'officier de la sécurité de l'information :

- S'assure de définir une stratégie de protection en matière de sécurité de l'information permettant de protéger l'Université en fonction des principes de sécurité de l'information définis par la Politique;
- Veille à ce qu'un niveau de criticité soit attribué adéquatement par les responsables de la sécurité de l'information et les responsables d'actifs informationnels;
- Veille à ce que des mesures respectant le niveau de criticité des actifs informationnels soient mises en place;
- S'assure du bon fonctionnement du Réseau de cyberdéfense et coordonne les actions du Réseau en cas d'incident de sécurité à portée institutionnelle;
- Définit le cahier des directives en matière de gestion des incidents de sécurité informationnelle;
- S'assure que les pratiques de sécurité de l'information qui ont cours à l'Université sont suivies par l'ensemble des membres et unités de l'Université et qu'elles favorisent la protection de l'infrastructure technologique et de l'information de l'Université;
- S'assure de la cohésion et de la cohérence des interventions des responsables de la sécurité de l'information de l'Université auprès des facultés, directions, services, centres et insituts de recherche de l'Université;
- Établit une stratégie de développement des compétences en matière de cybersécurité; et
- Effectue une reddition de comptes à la dirigeante ou au dirigeant de l'information sur la mise en œuvre du plan de traitement des risques, les événements rapportés par le Centre de cyberdéfense et les risques liés à la sécurité de l'information.

5.5 Responsable de la sécurité de l'information

La ou le responsable de la sécurité de l'information veille à la protection des actifs informationnels d'un des secteurs d'activité de l'Université. La ou le responsable de la sécurité de l'information :

- Planifie, définit, conçoit et intègre la sécurité de l'information dans tous les actifs informationnels de son secteur d'activité pour maintenir et améliorer la performance et la conformité de l'organisation en matière de sécurité de l'information;
- Veille à ce qu'un niveau de criticité soit attribué adéquatement avec la collaboration des responsables des actifs informationnels de son secteur d'activités;
- Veille à ce que des mesures respectant le niveau de criticité des actifs informationnels soient mises en place dans son secteur d'activité;
- Participe à la définition de la stratégie de cyberdéfense de l'Université;
- Est un membre obligatoire et contribue au Réseau de cyberdéfense de l'Université;
- Effectue 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 son secteur d'activité en matière de sécurité de l'information; et

- Gère les incidents en matière de sécurité de l'information associés à son secteur d'activité.

5.6 Centre de cyberdéfense

Le Centre de cyberdéfense de l'Université Laval est responsable de surveiller et de répondre aux événements de cybersécurité dans un objectif d'assurer la cyberdéfense des actifs informationnels numériques de l'Université. Ce centre, en tant que pôle d'expertise du Réseau de cyberdéfense :

- Reçoit, évalue et traite les signalements d'événements de cybersécurité;
- Rend compte, en temps opportun, des signalements d'événements de cybersécurité au responsable de la sécurité de l'information du secteur correspondant ou répondant du Réseau de cyberdéfense;
- 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; et
- 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.

5.7 Réseau de cyberdéfense

Le Réseau de cyberdéfense constitue une plateforme de partage d'informations, de collaboration et de concertation entre les répondants en cybersécurité désignés par les facultés, directions, services, centres et instituts de recherche et des spécialistes en cybersécurité de la Direction des technologies de l'information. Plus particulièrement, ce Réseau 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.

5.8 Les facultés, directions, services, centres et instituts de recherche de l'Université Laval

Les facultés, directions, services, centres et instituts de recherche qui conçoivent, développent ou supportent des systèmes d'information :

- Nomment une répondante ou un répondant en cybersécurité pour les représenter auprès du Réseau de cyberdéfense;
- S'assurent de considérer la sécurité de l'information à toutes les étapes du cycle de vie d'un actif informationnel, notamment en impliquant les responsables de la sécurité d'information de leur secteur; et
- Contribuent à la stratégie de protection en matière de sécurité de l'information de l'Université en mettant en place les moyens ciblés par le Réseau de cyberdéfense.

5.9 Service de sécurité et de prévention

Le Service de sécurité et de prévention de l'Université Laval est responsable de la protection des personnes, des infrastructures et des biens. Plus précisément, il prend en charge les

enquêtes découlant d'incidents de sécurité de l'information impliquant des membres lors de plaintes ou de signalements.

5.10 Vice-rectrice ou vice-recteur à l'équité, la diversité et l'inclusion et aux ressources humaines

La vice-rectrice ou le vice-recteur à l'équité, la diversité et l'inclusion et aux ressources humaines:

- Contribue à la sensibilisation des membres du personnel en matière de sécurité de l'information;
- Collabore avec l'officière ou l'officier de la sécurité de l'information pour concevoir des contenus de sensibilisation destinés aux membres du personnel; et

5.11 Membres

La membre ou le membre :

- Respecte le Règlement de sécurité de l'information sur l'utilisation des actifs informationnels; 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 Politique sera révisée au besoin, 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 – Représentation de la structure organisationnelle de la sécurité de l'information