Politique
de sécurité de l'information

Approbation :	Conseil d'administration (Résolution CA-2012-239)
Modification :	Conseil d'administration (Résolution CA-2013-30)
Révision :	Bureau de sécurité de l'information
Entrée en vigueur :	28 novembre 2012

UNIVERSITÉ LAVAL

TABLE DES MATIÈRES

1 PRÉAMBULE

Afin de mener à bien sa mission, l'Université Laval produit, emmagasine, traite, communique et élimine de l'information sous plusieurs formes. Cette information possède une valeur légale, administrative, économique ou patrimoniale.

L'Université Laval reconnait que ces informations, essentielles à ses activités d'administration, d'enseignement et de recherche, doivent faire l'objet d'une évaluation, d'une utilisation appropriée et d'une protection adéquate, et ce, tout au long de leur cycle de vie. À cette fin, il convient de mettre en œuvre un ensemble cohérent de mesures de sécurité déterminé par une approche de gestion des risques de sécurité.

Ces mesures de sécurité se retrouvent dans différents documents, traitant de la sécurité de l'information, et l'ensemble de ces documents compose le « cadre régissant la sécurité de l'information », ci-après appelé le Cadre.

2 INTRODUCTION

2.1 Définitions et références

La définition des différents termes et abréviations utilisés dans cette politique et dans les autres documents composant le Cadre est consignée dans le Glossaire de sécurité de l'information de l'Université Laval.

Les documents de référence du Cadre sont tous accessibles sur le site web du Bureau de sécurité de l'information (BSI) à l'adresse suivante : http://www.bsi.ulaval.ca/sgc/cadre.

2.2 Objectifs

La Politique de sécurité de l'information, ci-après appelée la Politique, est avant tout la démonstration du soutien et de l'engagement de l'Université Laval vis-à-vis de la sécurité de l'information et de sa prise de position ferme et claire quant aux mesures de sécurité à appliquer pour protéger ses actifs informationnels. Elle a été élaborée conformément aux obligations légales et administratives et selon les meilleures pratiques. Elle énonce les principes directeurs, identifie les acteurs concernés, précise leurs rôles et responsabilités en lien avec les principes de gestion de la sécurité de l'information énoncés.

Les principaux objectifs de la présente Politique sont d'assurer :

- La conformité aux lois, politiques et règlements applicables;
- La disponibilité, l'intégrité et la confidentialité de l'information;
- La confidentialité des renseignements personnels des étudiants, des administrateurs, du personnel enseignant ou administratif de l'Université Laval et de ses partenaires d'affaires.

2.3 Champ d'application

La Politique s'applique aux actifs informationnels, utilisateurs et activités suivants :

2.3.1 Actifs informationnels

Les actifs informationnels visés sont ceux :

- Appartenant à l'Université et exploités par elle;
- Appartenant à l'Université, mais détenus par un partenaire, fournisseur ou autre intervenant;
- Appartenant à un partenaire, fournisseur ou autre intervenant et exploités par lui au profit de l'Université.

2.3.2 Utilisateurs

Les utilisateurs sont :

- Les étudiants, le personnel enseignant, les administrateurs ou le personnel administratif de l'Université Laval;
- Tout consultant, fournisseur, partenaire, organisme ou firme externe appelée à accéder ou à utiliser les actifs informationnels de l'Université Laval.

2.3.3 Activités

Les activités impliquant la cueillette, la consultation, la production, la transmission, la conservation et la destruction des actifs informationnels peu importe leur support, leur emplacement et le mode d'expression utilisés pour les rendre intelligibles, que ces activités soient conduites dans les locaux de l'Université ou dans un autre lieu.

3 CADRE LÉGAL ET ADMINISTRATIF

La Politique s'inscrit, entre autres, dans le contexte législatif de :

- Charte des droits et libertés de la personne du Québec (L.R.Q., c. C-12);
- Code civil du Québec (L.Q., 1991, c. 64);
- Loi concernant le cadre juridique des technologies de l'information (L.R.Q., c. C-1.1);
- Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (L.R.Q., c. A-2.1);
- Loi sur les archives (L.R.Q. c. A-21.1);
- Loi sur le droit d'auteur (L.R. 1985, c. C-42);
- Code criminel (L.R.C., 1985, ch. C-46).

4 PRINCIPES DIRECTEURS

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

SEC-P1 S’appuyer sur la famille des normes internationales ISO-27000 qui proposent les meilleures pratiques en cette matière et fournissent à l’Université Laval des barèmes de comparaison avec des organisations similaires.

SEC-P2 S’assurer de bien connaître les actifs informationnels à protéger ainsi que leur degré de sensibilité et en identifier les responsables.

SEC-P3 Identifier les mesures de sécurité de l’information en fonction du degré de sensibilité des actifs informationnels et des risques et menaces pouvant affecter leur disponibilité, leur intégrité ou leur confidentialité. Ces mesures doivent couvrir la protection des actifs, la détection de tout usage abusif ou inapproprié, l’éradication des menaces et le recouvrement des activités de l’Université possiblement compromises.

SEC-P4 Voir à ce que le niveau de mesures de sécurité à déployer permette d’atténuer les risques et de les maintenir à un niveau acceptable. Les mesures à déployer doivent également tenir compte du niveau de maturité de l’organisation et être cohérentes dans leur application.

SEC-P5 Protéger rigoureusement les renseignements personnels et s’assurer que les unités qui constituent des fichiers informatisés permanents contenant ce type de données déclarent leur existence au Bureau du secrétaire général, selon les modalités établies.

SEC-P6 Protéger également toute autre information confidentielle, tant dans sa conservation, son utilisation que sa destruction afin que cette dernière respecte les normes d'archivage prescrites par le Bureau du secrétaire général.

SEC-P7 Documenter clairement les attentes en fournissant à la communauté universitaire, un Cadre régissant la sécurité de l’information évolutif qui décrive l’ensemble des mesures, normes, processus, procédures ou guides traitant de ce sujet.

SEC-P8 Faire connaître à la communauté universitaire, les risques et les menaces affectant les actifs informationnels afin que chacun comprenne les attentes de l’Université en cette matière, puisse reconnaître les incidents et les risques potentiels et développe des habilités et des compétences appropriées. Veiller également à ce que les intervenants comprennent leur rôle et responsabilités en matière de sécurité de l’information.

SEC-P9 Être à même d’effectuer des vérifications de l’existence et de l’efficacité des mesures de sécurité entourant les actifs informationnels, afin de s’assurer du respect des exigences énoncées dans le Cadre régissant la sécurité de l’information.

SEC-P10 Être à même d’effectuer des vérifications ciblées ou encore des enquêtes informatiques lorsque des activités contreviennent aux législations, aux politiques, aux règlements, aux conventions et aux ententes de l’Université Laval. Ce type d’interventions doit cependant être encadré par un processus rigoureux impliquant des personnes dûment habilitées à les réaliser.

SEC-P11 Se prémunir contre les interruptions de service prolongées en disposant d’un plan de continuité permettant d'assurer la remise en opération des services jugées essentiels en cas de sinistre majeur.

5 RÔLES ET RESPONSABILITÉS

5.1 Le Conseil d'administration

Le Conseil d'administration a les responsabilités suivantes :

- Adopte la Politique et le Règlement;

5.2 Le Comité exécutif

- Le Comité exécutif approuve les directives et les processus faisant partie du Cadre.

5.3 Le Vice-recteur exécutif

Le Vice-recteur exécutif et au développement a les responsabilités suivantes :

- Adresser les recommandations nécessaires au Comité exécutif concernant le Cadre;
- Recommander le programme de sécurité de l'information au Comité exécutif;
- Veiller à l'exécution de la Politique;
- Veiller à la mise en œuvre des directives et des règlements;
- Approuver les demandes de dérogation à la Politique, à une directive ou à un règlement;
- Entériner l'identification des responsables d'actif informationnel à la suite de leur recommandation du Comité de sécurité de l'information.

5.4 Le Vice-recteur adjoint aux systèmes d'information

Le Vice-recteur adjoint aux systèmes d'information agit en tant que dirigeant principal de l'information à l'Université Laval. À ce titre, il a les responsabilités suivantes :

- Adresser les recommandations nécessaires au Vice-recteur exécutif et au développement concernant le Cadre;
- Recommander le programme de sécurité de l'information au Vice-recteur exécutif et au développement;
- Prendre action, de façon diligente, lorsque des décisions sont requises à la suite d'une situation inattendue liée à la sécurité de l'information et qui exige un redressement rapide.

5.5 Le Comité de sécurité de l'information

Sous la responsabilité du Vice-recteur adjoint aux systèmes d'information, le Comité de sécurité de l'information assure le leadership dans la protection des actifs informationnels de l'Université Laval. Ce comité a pour rôle d'entériner les recommandations institutionnelles en matière de sécurité de l'information provenant du Bureau de sécurité de l'information.

Ses principales responsabilités sont :

- Établir les objectifs du programme de sécurité de l'information de l'Université Laval, examiner son rendement et son efficacité et émettre les recommandations appropriées Vice-recteur adjoint aux systèmes d'information;
- Examiner, prioriser et recommander au Vice-recteur adjoint aux systèmes d'information les orientations, initiatives ainsi que les projets de sécurité de l'information;
- Analyser les documents du Cadre et, s'il y a lieu, recommander au Vice-recteur adjoint aux systèmes d'information les ajustements requis;
- Réviser toutes demandes de dérogation à la Politique, à une directive ou à un règlement du Cadre qui lui seraient soumises.

5.6 Le Bureau de sécurité de l'information

Le Bureau de sécurité de l'information a pour mandat d'assurer la sécurité de l'information de l'ensemble des unités d'enseignement, de recherche et d'administration de l'Université Laval.

À cette fin, le Bureau de sécurité de l'information doit :

- Élaborer et présenter des recommandations au comité de sécurité de l'information en vue de la mise à jour de la Politique de sécurité de l'information et des autres documents du Cadre et coordonner leur mise en œuvre;
- Procéder à des vérifications de conformité de la Politique et des autres documents du Cadre;
- Approuver les bonnes pratiques, normes, procédures, standards ainsi que le Glossaire de sécurité de l'information;
- Élaborer et proposer au comité de sécurité de l'information, un programme de sécurité de l'information, prenant en compte les besoins des unités, les objectifs et les risques de sécurité;
- Rendre compte au Vice-recteur exécutif et au développement et au Comité de sécurité de l'information, de la situation de l'Université Laval en matière de sécurité de l'information et de l'avancement du programme de sécurité de l'information;
- Maintenir et divulguer la liste des responsables d'actif informationnel;
- Identifier, avec la participation des responsables de la sécurité de l'information, des responsables d'actif informationnel et des détenteurs d'actif informationnel, les besoins de sécurité ainsi que les mesures de sécurité adéquates à mettre en place;
- Partager la vision de l'Université Laval en matière de sécurité de l'information avec l'ensemble de la communauté universitaire et ses partenaires pour en favoriser l'adhésion;
- Guider et soutenir les unités et les autres intervenants dans les activités liées à la sécurité de l'information;

- Assurer le suivi de la mise en œuvre de toute recommandation découlant d'une vérification externe ou interne touchant la sécurité de l'information;
- D'informer le Vice-rectorat aux ressources humaines de tout manquement de la part d'un employé aux dispositions du Cadre, y compris la présente Politique;
- S'assurer de la désignation d'un gestionnaire responsable de la sécurité de l'information par unité en tout temps.

5.7 Le responsable d'actif informationnel

Le rôle du responsable d'actif informationnel est de gérer du point de vue décisionnel et fonctionnel l'actif informationnel sous sa responsabilité de manière à ce qu'elle réponde aux besoins de sécurité identifiés.

Ses principales responsabilités sont :

- Contribuer à l'identification, la localisation et le marquage de l'actif informationnel;
- Évaluer et réviser périodiquement la sensibilité de l'actif informationnel en termes de disponibilité, intégrité, confidentialité et de sa valeur;
- Désigner et réviser périodiquement les détenteurs de l'actif informationnel;
- Identifier les mesures de sécurité à mettre en place et s'assurer de leur bonne application;
- Rendre compte de l'état de la sécurité de l'actif informationnel au gestionnaire responsable de la sécurité de son unité;
- S'assurer de la réalisation des activités suivantes concernant l'actif informationnel :
    - L'analyse et l'évaluation des risques de sécurité;
    - La sensibilisation à la sécurité auprès de ses utilisateurs;
    - La vérification de conformité quant aux mesures mises en place pour le protéger;
    - La gestion d'un incident de sécurité.

5.8 Le détenteur d'actif informationnel

Le rôle du détenteur d'actif informationnel est de gérer du point de vue opérationnel l'actif informationnel sous sa responsabilité de manière à ce qu'elle réponde aux besoins de sécurité identifiés par le responsable de l'actif informationnel.

Ses principales responsabilités sont :

- Localiser et marquer les actifs informationnels;
- Appuyer le responsable de l'actif informationnel dans l'évaluation de la sensibilité de la disponibilité, intégrité et confidentialité de l'actif informationnel;
- Protéger adéquatement l'actif informationnel par la mise en place, le maintien et la mise à jour des mesures de sécurité identifiées;

- Rendre compte de l'état de la sécurité de l'actif au gestionnaire responsable de la sécurité de son unité et au responsable de l'actif informationnel;
- Réaliser ou appuyer le responsable de l'actif informationnel dans les activités suivantes concernant l'actif informationnel :
    - L'analyse et l'évaluation des risques de sécurité;
    - La sensibilisation à la sécurité auprès de ses utilisateurs;
    - La vérification de conformité quant aux mesures mises en place pour protéger l'actif;
    - La gestion d'un incident de sécurité.

5.9 Le Service de sécurité et de prévention

En matière de sécurité de l'information, le Service de sécurité et de prévention participe, en collaboration avec le Bureau de sécurité de l'information, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels de l'Université Laval.

5.10 Le Vice-rectorat aux ressources humaines

À l'égard de la sécurité de l'information, leurs responsabilités sont :

- D'informer tout nouveau membre du personnel de sa responsabilité quant au respect de la présente Politique;
- De décider de la pertinence de toute requête d'enquête informatique à l'égard d'un membre du personnel de l'Université Laval et, s'il y a lieu, en autoriser la tenue.

5.11 L'enquêteur

L'enquêteur du Service de sécurité et de prévention est la seule personne ayant l'autorité requise afin de procéder à une enquête à l'Université Laval. L'enquêteur du Service de sécurité et de prévention est un « constable spécial » assermenté par un juge de la cour du Québec et ayant réussi un contrôle de sécurité élevée effectué par le ministère de la Sécurité publique du Québec. L'enquêteur travaille en conformité avec le « Code de déontologie des policiers du Québec ». À ce titre, il détient tous les pouvoirs pour procéder à l'ensemble des enquêtes les plus complexes incluant les enquêtes informatiques au sein de l'Université Laval. Toutes les enquêtes sont sous la responsabilité du directeur-adjoint du Service de sécurité et de prévention, lui aussi « constable spécial ».

Dans le cadre des enquêtes informatiques, l'enquêteur est chargé d'investiguer sur les activités impliquant les actifs informationnels de l'Université Laval et qui seraient en contravention avec la législation, les politiques, règlements, conventions et ententes de l'Université Laval.

5.12 Le gestionnaire responsable de la sécurité de l'information (GRS)

Le rôle du gestionnaire responsable de la sécurité de l'information est de s'assurer que la sécurité de l'information soit prise en compte dans son unité et que cette dernière respecte la présente Politique et les autres documents du Cadre.

Ses principales responsabilités sont :

- Assister le Bureau de sécurité de l'information dans la proposition d'orientations et de priorités d'intervention en matière de sécurité de l'information;
- Rendre les ressources physiques, humaines et financières disponibles afin de :
    - Participer aux projets institutionnels de sécurité;
    - Mettre en œuvre les mesures de sécurité obligatoires ou recommandées par le Bureau de sécurité de l'information;
    - Réaliser les activités opérationnelles de sécurité de son unité;
    - Avoir un plan de relève, à jour et validé, pour chaque service jugée essentielle ou prioritaire par l'Université Laval.
- Participer à la définition, à la mise en œuvre et au respect des processus visant à favoriser la sécurité de l'information à l'Université;
- S'assurer que tous les utilisateurs sous sa responsabilité sont sensibilisés aux mesures de sécurité de l'information entourant l'usage des actifs informationnels de l'Université Laval.
- Fournir un état de situation périodique au directeur du Bureau de sécurité de l'information, pour son unité;
- Informer le Bureau de sécurité de l'information de tout incident de sécurité et de toute situation pouvant influencer les risques liés à la sécurité de l'information, pour son unité et participer également à l'élaboration de la stratégie de mitigation les concernant;
- Rendre compte au Bureau de sécurité de l'information de la situation de son unité en matière de sécurité de l'information;
- S'assurer d'un transfert de toute information pertinente à son éventuel remplaçant pour ce rôle.

Pour l'assister, le gestionnaire responsable de la sécurité de l'information peut nommer un ou plusieurs répondant(s) de la sécurité de l'information (RS), pour son unité, qui réalisera les activités opérationnelles de sécurité qui lui sont confiées.

5.13 Le supérieur immédiat

Les principales responsabilités du supérieur immédiat en matière de sécurité de l'information, pour tous les membres du personnel sous sa responsabilité, sont :

- De les informer et les sensibiliser à leur rôle concernant la protection des actifs informationnels de l'Université Laval et à leurs responsabilités à cet égard;

- De leur communiquer les documents du Cadre en vigueur;
- De répondre de leur utilisation des actifs informationnels sous sa responsabilité.

5.14 L'utilisateur

La responsabilité de la protection des actifs informationnels de l'Université Laval incombe à tous les utilisateurs. Chacun d'eux est responsable de respecter la Politique ainsi que tous les autres documents du Cadre.

À cette fin, l'utilisateur doit notamment :

- Prendre connaissance et adhérer à la présente Politique;
- S'engager à utiliser les actifs informationnels de manière à respecter le Règlement de sécurité de l'information sur l'utilisation des actifs informationnels.

6 DISPOSITIONS FINALES

6.1 Sanctions

Toute contravention à la présente Politique peut entrainer, en plus des mesures prévues aux législations, règlements, politiques, conventions ou ententes, les conséquences suivantes, en fonction de la nature, de la gravité et des répercussions du geste ou de l'omission:

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

6.2 Dérogation

Aucune dérogation à la présente Politique n'est permise sans autorisation écrite du vice-recteur exécutif et au développement.

6.3 Mise en œuvre, suivi et révision

Le Bureau de sécurité de l’information est responsable de la coordination, de la mise en œuvre et de la mise à jour de la présente Politique qui doivent être réalisées tous les trois ans ou lors de changements significatifs qui pourraient l’affecter.

6.4 Adoption et date d’entrée en vigueur

La présente Politique est adoptée et entre en vigueur à la date de son adoption par le Conseil d’administration de l’Université Laval.