UNIVERSITÉ DE SHERBROOKE

POLITIQUE 2500-036

TITRE :	**Politique de sécurité de l'information**		
ADOPTION :	Conseil d'administration	Résolution :	CA-2016-09-26-19
ENTRÉE EN VIGUEUR :	Le 26 septembre 2016		
MODIFICATION :	Conseil d'administration	Résolution :	

PRÉAMBULE

Dans l'accomplissement de sa mission, l'Université de Sherbrooke traite de l'information sous plusieurs formes et sur plusieurs supports à l'aide de différents systèmes d'information. Cette information détenue par l'Université afin de soutenir ses activités possède une valeur administrative, légale, financière ou patrimoniale et doit, par conséquent, faire l'objet d'une évaluation continue, d'une utilisation appropriée et d'une protection adéquate tout au long de son cycle de vie. À ces fins, la mise en œuvre d'un ensemble cohérent de mesures de sécurité, déterminé par une approche de gestion des risques, est nécessaire.

Dans ce contexte, l'entrée en vigueur de la *Loi sur la gouvernance des ressources informationnelles des organismes publics et des entreprises du gouvernement* (L.R.Q., c. G-1.03) et de la *Directive sur la sécurité de l'information gouvernementale* (une directive du Conseil du Trésor du Québec applicable à l'Université) crée des obligations aux établissements universitaires en leur qualité d'organismes publics. Ainsi, la *Directive sur la sécurité de l'information gouvernementale* oblige l'Université de Sherbrooke à adopter, à mettre en œuvre, à maintenir à jour et à assurer l'application d'une politique de sécurité de l'information – dont les principales modalités sont définies dans la directive gouvernementale – notamment en s'assurant de la mise en œuvre des processus formels de sécurité de l'information permettant, notamment, d'assurer la gestion des risques, la gestion de l'accès à l'information et la gestion des incidents.

1. OBJECTIF

La présente politique a pour objectif d'assurer la sécurité de l'information tout au long de son cycle de vie, et plus précisément :

- la disponibilité de l'information de façon à ce qu'elle soit accessible en temps voulu et de la manière requise aux personnes autorisées;
- l'intégrité de l'information de manière à ce que celle-ci ne soit pas détruite ni altérée d'aucune façon sans autorisation, et que le support de cette information lui procure la stabilité et la pérennité voulues;
- la confidentialité de l'information, en limitant la divulgation et l'utilisation de celle-ci aux seules personnes autorisées, notamment celle constituant des renseignements personnels.

La politique soutient la mise en œuvre du cadre de gestion en matière de sécurité de l'information et renforce le maintien de systèmes de contrôles internes offrant une assurance raisonnable de conformité à l'égard des lois, directives et pratiques gouvernementales en la matière.

2. 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* (L.R.Q., c. G-1.03);
- la *Loi concernant le cadre juridique des technologies et l'information* (L.R.Q., c. C-1.1);
- la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1);
- la *Loi sur les archives* (L.R.Q. c. A-21.1);
- la *Politique-cadre sur la gouvernance et la gestion des ressources informationnelles des organismes publics* (Décret no 261-2012 du 28 mars 2012);
- la *Directive sur la sécurité de l'information gouvernementale* (Décret 7-2014 du 15 janvier 2014);
- le *Cadre gouvernemental de gestion de la sécurité de l'information* (juin 2014);
- la *Loi sur le droit d'auteur* (L.C., 1985, c. C-42).

La *Politique de sécurité de l'information* est applicable en considérant les politiques, directives et règlements suivants de l'Université de Sherbrooke :

- le *Règlement des études* (2575-011);
- la *Politique de gestion intégrée des risques* (2500-031);
- la *Directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels* (2600-063)
- la *Directive sur la divulgation de renseignements confidentiels en vue d'assurer la protection des personnes* (2600-020);
- les *Règles de sécurité informatique* (2600-028).

3. CHAMP D'APPLICATION

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

- appartenant à l'Université et détenus par elle;
- appartenant à l'Université, mais détenus par un tiers;
- utilisés par un tiers et détenus par lui au bénéfice ou pour et au nom de l'Université;

quels qu'en soient les supports, incluant le papier.

Les utilisatrices et utilisateurs visés par la Politique sont :

- les personnes à l'emploi de l'Université;
- les étudiantes et étudiants de l'Université;
- toute entité externe autorisée à accéder, à exploiter ou à héberger l'information et les actifs informationnels de l'Université.

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.

4. PRINCIPES DIRECTEURS

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

a) s'assurer de bien connaître l'information à protéger et en identifier les responsables;
b) s'appuyer sur les normes internationales pertinentes afin de favoriser le déploiement des meilleures pratiques et de recourir à des barèmes de comparaison avec des organismes ou établissements similaires;
c) identifier les mesures de sécurité de l'information en fonction de son degré de sensibilité et des risques et menaces pouvant affecter sa disponibilité, son intégrité et sa confidentialité, étant entendu que ces mesures doivent couvrir la protection de l'information, la détection de tout usage abusif ou inapproprié de l'information, l'éradication des menaces et le recouvrement des activités de l'Université possiblement compromises;
d) déployer des mesures de sécurité adéquates et cohérentes permettant d'atténuer les risques et de les maintenir à un niveau acceptable;
e) protéger rigoureusement les renseignements personnels ainsi que toute autre information confidentielle;
f) rendre accessibles à la communauté universitaire des modalités et des outils favorisant la sécurité de l'information;
g) informer la communauté universitaire des risques et des menaces pouvant affecter l'information afin que ses membres puissent reconnaître les incidents et les risques potentiels et comprendre leurs rôles et responsabilités en matière de sécurité de l'information en développant les habiletés et les compétences appropriées;

h) se prémunir contre les interruptions de service en disposant de plans de continuité et de relève permettant d'assurer la remise en opération des services jugés essentiels en cas d'incident majeur de sécurité de l'information;
i) effectuer des vérifications de l'existence et de l'efficacité des mesures de sécurité de l'information;
j) effectuer des vérifications ciblées ou encore des enquêtes lorsque des activités ayant une incidence sur la sécurité de l'information contreviennent ou semblent contrevenir aux lois, règlements, politiques, conventions ou ententes applicables, étant entendu que ces interventions doivent être encadrées par un processus rigoureux et impartial et menées par des personnes dûment autorisées;
k) promouvoir des bonnes pratiques de protection des actifs informationnels, notamment par l'élaboration et la diffusion d'activités de sensibilisation et de perfectionnement du personnel de l'Université.

5. CADRE DE GESTION

L'efficacité des mesures de sécurité de l'information exige l'attribution claire de rôles et de responsabilités aux différents intervenants et intervenantes de l'Université par la mise en place d'un cadre de gestion de la sécurité permettant notamment une reddition de comptes adéquate.

Les pratiques et les solutions retenues en matière de sécurité de l'information doivent être réévaluées périodiquement afin de tenir compte des changements juridiques, organisationnels, technologiques, physiques et environnementaux, ainsi que de l'évolution des menaces et des risques.

La Politique de sécurité de l'information de l'Université s'articule autour de trois axes fondamentaux de gestion, soit la gestion des accès, la gestion des risques et la gestion des incidents.

5.1. Gestion des accès

La sécurité de l'information est assurée par des mesures d'encadrement et un contrôle adéquat de l'accès, de la divulgation et de l'utilisation de l'information par les personnes autorisées afin d'en protéger la confidentialité et l'intégrité, en portant une attention particulière à l'information confidentielle et aux renseignements personnels.

L'efficacité des mesures de sécurité de l'information repose sur l'attribution de responsabilités et une imputabilité des utilisatrices et utilisateurs, à tous les niveaux de l'Université.

5.2. Gestion des risques

Une catégorisation à jour soutient l'analyse de risques en permettant de connaître la valeur de l'information à protéger.

L'analyse de risques guide également l'acquisition, le développement et l'exploitation des systèmes d'information, en spécifiant les mesures de sécurité à mettre en œuvre pour leur déploiement dans l'environnement de l'Université. La gestion des risques reliés à la sécurité de l'information s'inscrit dans le processus global de gestion des risques de l'Université. Les risques à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Le niveau de protection de l'information est établi en fonction :

- de la nature de l'information et de son importance;
- des probabilités d'occurrence d'accident, d'erreur et de malveillance auxquels elle est exposée;
- des conséquences de la matérialisation de ces risques.

5.3. Gestion des incidents

L'Université déploie des mesures de sécurité de l'information afin d'assurer la continuité de ses services. À cet égard, elle met en place les mesures nécessaires afin de :

- limiter l'occurrence des incidents en matière de sécurité de l'information;
- gérer adéquatement ces incidents pour en minimiser les conséquences et rétablir les activités ou les opérations.

Les incidents de sécurité de l'information à portée gouvernementale sont déclarés conformément à la *Directive sur la sécurité de l'information gouvernementale*.

Dans la gestion des incidents, l'Université peut exercer ses pouvoirs et ses prérogatives eu égard à toute utilisation inappropriée de l'information qu'elle détient ou de ses systèmes d'information, notamment en matière de relations de travail et d'enquêtes ou encore de conformité au *Règlement des études*.

6. RÔLES ET RESPONSABILITÉS

La présente politique attribue la gestion de la sécurité de l'information à l'Université à des instances, à des comités et à des personnes en raison des fonctions particulières qu'elles exercent.

6.1. Conseil d'administration

Le conseil d'administration adopte la *Politique de sécurité de l'information* ainsi que toute modification à celle-ci. Le conseil est régulièrement informé des actions de l'Université en matière de sécurité de l'information.

6.2. Comité de gouvernance des ressources informationnelles du conseil d'administration

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.

Ainsi, le comité de gouvernance des ressources informationnelles du conseil d'administration évalue, examine ou vérifie notamment :

- l'application, la validité et l'efficacité du cadre de gestion, des plans d'action et des moyens technologiques élaborés et mis en œuvre en matière de sécurité de l'information;
- le respect du cadre de gestion afférent à la sécurité de l'information et des systèmes d'information.

Le comité veille à la gestion des risques inhérents aux ressources informationnelles en s'assurant que ceux-ci sont considérés à l'intérieur du processus institutionnel de la gestion intégrée des risques.

6.3. Comité de direction de l'Université

Le comité de direction de l'Université adopte des mesures visant à favoriser l'application de la présente politique et des obligations légales de l'Université en matière de sécurité de l'information. Ainsi, il adopte les orientations stratégiques, les plans d'action et les bilans de

sécurité de l'information. Il peut également adopter des directives et des procédures afin de préciser ou de soutenir l'application de la présente politique.

6.4. Secrétaire générale ou secrétaire général

La secrétaire générale ou le secrétaire général veille à l'application de la présente politique. Cette personne :

- 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 plans d'action, les bilans de sécurité, les redditions de comptes en matière de sécurité de l'information;
- autorise exceptionnellement une dérogation à l'une ou l'autre des dispositions de la présente politique, 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 à la présente politique est signalée;
- tient à jour le registre des dérogations et le registre des cas de contravention à la présente politique.

En outre, en sa qualité de responsable de l'accès aux documents et de la protection des renseignements personnels, la secrétaire générale ou le secrétaire général agit comme personne-ressource pour toute question ou problématique relative à la sécurité des renseignements personnels détenus par l'Université. Sa fonction lui permet de prescrire des mesures de protection des renseignements personnels à l'égard des documents, de vérifier l'application de telles mesures et d'exiger que des correctifs soient apportés, le cas échéant.

6.5. Comité de sécurité de l'information

Sous la responsabilité de la secrétaire générale ou du secrétaire général, le comité de sécurité de l'information est la principale instance de concertation en matière de sécurité de l'information, au niveau stratégique, au sein de l'Université. Ce comité est notamment chargé de formuler des recommandations sur :

- le cadre de gestion, les plans d'action et les bilans de sécurité de l'information de l'Université ainsi que toute proposition d'action en matière de sécurité de l'information;
- les événements significatifs ayant mis ou qui auraient pu mettre en péril la sécurité de l'information de l'Université.

Le mandat spécifique est établi par le comité de direction de l'Université, après avoir obtenu l'avis du comité de gouvernance des ressources informationnelles du conseil d'administration.

Le comité de sécurité de l'information, présidé par la secrétaire générale ou le secrétaire général, est composé des personnes suivantes :

- l'officière ou l'officier de sécurité de l'information;
- la directrice générale ou le directeur général du Service des technologies de l'information;
- la directrice générale ou le directeur général du Service des communications;
- la registraire ou le registraire;
- la directrice générale ou le directeur général du Service des ressources humaines;
- la doyenne ou le doyen de chaque faculté ou un cadre de la faculté qu'elle ou qu'il désigne;
- une membre ou un membre du corps enseignant expert en gestion de l'information;

- une membre ou un membre du corps enseignant expert en sécurité des technologies de l'information.

À l'exclusion des membres d'office, les membres du comité de sécurité de l'information sont nommés par le comité de direction de l'Université pour un mandat de trois ans renouvelable.

La secrétaire générale ou le secrétaire général peut inviter, de façon permanente ou ponctuelle, toute personne à participer au comité en fonction des besoins établis ou d'expertises spécifiques.

6.6. Comité de coordination du plan de mesures d'urgence (CCPMU)

Le comité de coordination du plan de mesures d'urgence (CCPMU) est chargé de la gestion opérationnelle des incidents critiques de sécurité de l'information. Le mandat et la composition de ce comité sont définis dans le Plan d'organisation du Service des immeubles de l'Université.

6.7. Officière ou officier de sécurité de l'information (OSI)

L'officière ou l'officier de sécurité de l'information est un membre du personnel cadre, nommé par le conseil d'administration, relevant directement de la secrétaire générale ou du secrétaire général et qui assume le rôle de responsable de la sécurité de l'information (RSI) au sens du *Cadre gouvernemental de gestion de la sécurité de l'information*. Cette personne soutient la secrétaire générale ou le secrétaire général en contribuant notamment à la mise en place des processus de sécurité de l'information et à la mise en œuvre des mesures d'atténuation des risques. À cet égard, l'officière ou l'officier :

- élabore et propose le programme de sécurité de l'information de l'Université dont ses objectifs et, périodiquement, rend compte de son implantation à la secrétaire générale ou au secrétaire général, participe à son évaluation et procède à sa mise à jour;
- formule des recommandations concernant les besoins, les priorités, les orientations, les plans d'action, les directives, les procédures, les initiatives et les bonnes pratiques en matière de sécurité de l'information et la mise à jour de la présente politique;
- 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 responsables d'actifs informationnels dans les unités;
- produit les plans d'action, les bilans et les redditions de comptes de l'Université en matière de sécurité de l'information;
- propose des dispositions visant le respect des exigences en matière de sécurité de l'information à intégrer dans les ententes de service et les contrats;
- s'assure de la déclaration, par l'Université, des risques et des incidents de sécurité de l'information à portée gouvernementale;
- collabore à l'élaboration du contenu du plan de communication et du programme de sensibilisation et de formation en matière de sécurité de l'information et veille à leur déploiement;
- procède aux enquêtes de contraventions sérieusement présumées à la présente politique sur autorisation de la secrétaire générale ou du secrétaire général;
- assure des veilles normative, juridique, gouvernementale et technologique afin de suivre l'évolution des normes, des lois et règlements, des pratiques gouvernementales et des progrès technologiques en matière de sécurité de l'information.

6.8. Service des technologies de l'information (STI)

En matière de sécurité de l'information, le Service des technologies de l'information, en collaboration avec les ressources facultaires dédiées aux technologies de l'information :

- s'assure de la prise en charge des exigences de sécurité de l'information dans l'exploitation des systèmes d'information de même que lors de la réalisation de projets de développement ou d'acquisition de systèmes d'information dans lesquels il intervient;
- participe activement à l'analyse de risques, à l'évaluation des besoins et des mesures à mettre en œuvre, et à l'anticipation de toute menace en matière de sécurité des systèmes d'information faisant appel aux technologies de l'information;
- élabore et met en place le programme de sensibilisation et d'information du personnel de l'Université en matière de sécurité de l'information;
- applique des mesures de réaction appropriées à toute menace ou à tout incident de sécurité de l'information notamment l'interruption ou la révocation temporaire, lorsque les circonstances l'exigent, des services d'un système d'information faisant appel aux technologies de l'information afin d'assurer la sécurité de l'information en cause;
- participe à l'exécution des enquêtes relatives à des contraventions réelles ou apparentes à la présente politique autorisées par la secrétaire générale ou le secrétaire général.

6.9. Service des immeubles

La Division de la sécurité et de la prévention du Service des immeubles participe, avec l'officière ou l'officier de sécurité de l'information, à l'identification des mesures de sécurité physique permettant de protéger adéquatement les actifs informationnels de l'Université.

Le Service des immeubles 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 de gestion de l'information ou des supports de l'information confidentielle.

6.10. Service des ressources humaines

En matière de sécurité de l'information, le Service des ressources humaines informe et obtient de tout nouvel employé de l'Université son engagement au respect de la présente politique.

6.11. Responsables d'actifs informationnels

Le responsable d'actifs informationnels est le membre du personnel cadre détenant la plus haute autorité au sein de 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. Le responsable d'actifs informationnels peut déléguer la totalité ou une partie de sa responsabilité à un autre membre du personnel cadre de l'unité.

Les responsables d'actifs informationnels :

- informent le personnel relevant de leur autorité et les tiers avec lesquels l'unité transige de la Politique de sécurité de l'information et des dispositions du cadre de gestion afin de le sensibiliser à la nécessité de s'y conformer;
- collaborent activement à la catégorisation de l'information de l'unité sous sa responsabilité et à l'analyse de risques;
- voient à la protection de l'information et des systèmes d'information sous sa responsabilité en veillant à que ceux-ci soient utilisés par le personnel relevant de son autorité en conformité avec la *Politique de sécurité de l'information* et de tout autre élément du cadre de gestion;

- s’assurent 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 consultant, fournisseur, partenaire, invité, organisme ou firme externe s’engage à respecter la Politique et tout autre élément du cadre de gestion;
- rapportent au Service des technologies de l’information toute menace ou tout incident afférant à la sécurité de l’information;
- collaborent 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;
- rapportent à la secrétaire générale ou au secrétaire général tout problème lié à l’application de la présente politique dont toute contravention réelle ou apparente d’un membre du personnel à l’égard de l’application de cette politique.

6.12. Utilisatrices et utilisateurs

La responsabilité de la sécurité de l’information de l’Université incombe à tous les utilisateurs et utilisatrices des actifs informationnels de l’Université.

Toute utilisatrice et tout utilisateur qui accède à une information, la consulte ou la traite est responsable de l’utilisation qu’il en fait et doit procéder de manière à protéger cette information.

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

- se conformer à la présente politique et à toute autre directive de l’Université en matière de sécurité de l’information et d’utilisation des actifs informationnels;
- utiliser les droits d’accès qui lui sont attribués et autorisés, l’information et les systèmes d’information mis à sa disposition uniquement dans le cadre de ses fonctions et aux fins auxquelles ils sont destinés;
- participer à la catégorisation de l’information de son unité;
- respecter les mesures de sécurité mises en place, ne pas les contourner ni modifier leur configuration ou les désactiver;
- signaler au responsable des actifs informationnels de son unité tout incident susceptible de constituer une contravention à la présente politique ou de constituer une menace à la sécurité de l’information de l’Université;
- collaborer à toute intervention visant à identifier ou à mitiger une menace à la sécurité de l’information 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 dont la présente Politique.

En outre, lorsque l’utilisatrice ou l’utilisateur de l’Université, par ses activités professionnelles ou d’études, partage des actifs informationnels, des dispositifs de technologies de l’information ou des systèmes d’information avec ceux d’un établissement du réseau de la santé et des services sociaux, cette personne doit :

- se conformer à la politique de l’établissement du réseau de la santé et des services sociaux en matière de sécurité de l’information et d’utilisation des actifs informationnels;
- signaler à la personne responsable des actifs informationnels de son unité tout incident susceptible de constituer une contravention à la politique de sécurité de l’établissement du réseau de la santé et des services sociaux ou de constituer une menace à la sécurité de l’information détenue par cet établissement.

Aussi, toute utilisatrice ou utilisateur de l’Université doit 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. SENSIBILISATION ET INFORMATION

La sécurité de l'information repose notamment sur la régulation des conduites et la responsabilisation individuelle. À cet égard, les membres de la communauté universitaire doivent être sensibilisés :

- à la sécurité de l'information et des systèmes d'information de l'Université;
- aux conséquences d'une atteinte à la sécurité;
- à leur rôle et à leurs responsabilités en la matière.

À ces fins, des activités de sensibilisation et de formation sont offertes périodiquement et des documents explicatifs sont rendus disponibles sur le site Internet de l'Université.

8. SANCTIONS

En cas de contravention à la présente politique, l'utilisatrice ou l'utilisateur engage sa responsabilité personnelle; il en est de même pour la personne qui, par négligence ou par omission, fait en sorte que l'information n'est pas protégée adéquatement.

Tout membre de la communauté universitaire 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 et du Règlement des études).

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, conventions ou ententes, les conséquences suivantes, en fonction de la nature, de la gravité et des répercussions du geste ou de l'omission :

- 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.

9. DIFFUSION ET MISE À JOUR DE LA POLITIQUE

La secrétaire générale ou le secrétaire général est responsable de la diffusion et de la mise à jour de la présente politique.

10. ENTRÉE EN VIGUEUR

La présente politique entre en vigueur à la date de son adoption par le conseil d'administration.

GLOSSAIRE

Actif informationnel : une information, une banque d'information, 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.

Autorisation : l'attribution par l'Université à une personne ou à un groupe de personnes d'un droit d'accès, complet ou restreint, à une information ou à un système d'information.

Cadre de gestion : l'ensemble de consignes que sont les politiques, les règlements, les directives, les procédures, les bonnes pratiques reconnues qui encadrent les activités d'un établissement tel que l'Université de Sherbrooke.

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 : l'ensemble des personnes à l'emploi de l'Université et des étudiantes et étudiants de l'Université.

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.

Cycle de vie de l'information : l'ensemble des étapes que franchit une information, de sa création en passant par son enregistrement, son transfert, sa consultation, son traitement et sa transmission, jusqu'à sa conservation permanente ou sa destruction, en conformité avec le calendrier de conservation de l'Université de Sherbrooke.

Détentrice ou détenteur : une personne qui a effectivement la garde d'une partie ou de la totalité d'un actif informationnel ou de plusieurs actifs informationnels de l'Université.

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

Imputabilité : le principe selon lequel une violation ou une tentative de violation d'un système informatique est attribuée à la seule entité qui en est responsable.

Incident : 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.

Incident de sécurité de l'information à portée gouvernementale : la conséquence observable de la concrétisation d'un risque de sécurité de l'information à portée gouvernementale, nécessitant une intervention concertée au plan gouvernemental.

Information : un renseignement consigné sur un support quelconque pour être conservé, traité ou communiqué comme 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.

Mesure de sécurité de l'information : un moyen concret assurant partiellement ou totalement la protection d'information de l'Université contre un ou plusieurs risques (panne majeure du réseau informatique ou des serveurs institutionnels, acte involontaire, acte malveillant tel que l'intrusion dans un système informatique, etc.) et dont la mise en œuvre vise à amoindrir la probabilité de survenance de ces risques ou à réduire les pertes qui en résultent.

Plan de continuité : l'ensemble des mesures de planification établies et appliquées en vue de rétablir la disponibilité de l'information indispensable à la réalisation d'une activité de l'Université.

Plan de relève : le plan de reprise hors site mis en œuvre lorsque la détérioration ou la destructions d'actifs informationnels consécutive à un incident exige le transfert de l'exploitation dans un autre lieu, et qui décrit les procédures visant à assurer, dans des conditions de continuité adaptées aux critères de survie de l'Université, la mise à la disposition rapide et ordonnée des moyens de secours ainsi que la reprise éventuelle de l'exploitation normale après réfection ou remplacement des actifs détruits ou endommagés.

Registre d'autorité : le répertoire, le recueil ou le fichier dans lequel sont notamment consignés les désignations effectuées et les délégations consenties aux fins de la gestion de la sécurité de l'information ainsi que les responsabilités qui y sont rattachées.

Registre d'incident : un recueil dans lequel sont consignés la nature d'un incident de sécurité de l'information, l'impact, les mesures prises pour le rétablissement à la normale et le suivi.

Renseignement confidentiel : un renseignement dont l'accès est assorti d'une ou de plusieurs restrictions dont celles prévues à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* que sont les incidences sur les relations intergouvernementales, les négociations entre organismes publics, l'économie, l'administration de la justice et de la sécurité publique, les décisions administratives ou politiques et la vérification.

Renseignement personnel : une information concernant une personne physique et qui permet de l'identifier. Un renseignement personnel qui a un caractère public en vertu d'une loi n'est pas considéré un renseignement personnel aux fins de la présente politique.

Responsable 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.

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 et les incidents.

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).

Unité : l'un ou l'autre des facultés, écoles, départements, services administratifs, ainsi que l'une ou l'autre des unités de recherche de l'Université.

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. Les membres du personnel de l'Université ainsi que les étudiantes et étudiants sont les premiers utilisateurs et utilisatrices de l'information de l'Université.