UNIVERSITÉ DE SHERBROOKE

DIRECTIVE 2600-063

TITRE :	**Directive relative à l'utilisation, à la gestion et à la sécurité des actifs informationnels**		
ADOPTION :	Comité de direction de l'Université	Résolution :	CD-2016-09-20-22
ENTRÉE EN VIGUEUR :	Le 26 septembre 2016		
MODIFICATION :	Comité de direction de l'Université	Résolution :	

TABLE DES MATIÈRES

PRÉAMBULE

L'Université de Sherbrooke reconnaît l'importance de donner accès à ses actifs informationnels dont ses équipements et ses ressources informatiques et de télécommunication aux membres de la communauté universitaire qui participent à des activités d'enseignement, de recherche, de création, de gestion, de service à la collectivité et de vie étudiante découlant de la mission de l'Université. L'accès à ces ressources peut aussi être accordé à des personnes invitées par un membre de la communauté habilité à parrainer leurs demandes.

La présente directive vise à établir les conditions relatives à l'utilisation sécuritaire par les utilisatrices et utilisateurs de l'Université des équipements, des systèmes, des logiciels et du réseau de même que des données contenues ou véhiculées par eux. L'approche préconisée privilégie la responsabilisation personnelle et collective des membres de la communauté universitaire afin de protéger les actifs informationnels de l'Université et ceux utilisés sur une base sectorielle ou individuelle, d'assurer la qualité des services dispensés, de favoriser l'utilisation éthique de ces actifs et de sensibiliser chaque utilisatrice et utilisateur à la sécurité de l'information. La directive vise à concilier les besoins communs et individuels, étant entendu que la protection des actifs universitaires et collectifs a préséance sur les biens et comportements individuels. Enfin, la directive englobe la protection des actifs informationnels, la confidentialité des données (le cas échéant) et la continuité des services.

Cette directive définit des modalités opérationnelles découlant des principes directeurs de la *Politique de sécurité de l'information* (Politique 2500-036) devant guider toutes les personnes autorisées à utiliser les actifs informationnels de l'Université afin d'assurer la sécurité de l'information tout au long de son cycle de vie.

1. OBJECTIFS

Cette directive encadre l'utilisation, la gestion et la sécurité des actifs informationnels de l'Université de Sherbrooke. Elle établit les règles et les conditions applicables ainsi que les limites et les responsabilités qui en découlent dans le but d'en favoriser une utilisation responsable.

Ainsi, la directive poursuit les objectifs suivants :

- favoriser l'utilisation efficace, sécuritaire, légale et éthique des actifs informationnels;
- établir des mesures visant à assurer la disponibilité, l'intégrité et la confidentialité des actifs informationnels de l'Université;
- éviter que l'utilisation des actifs informationnels de l'Université ne soit l'instrument de perturbations internes ou externes;
- définir les droits et les obligations des utilisatrices et utilisateurs à l'égard de l'utilisation des actifs informationnels dans le respect des lois, des règlements et des politiques applicables;
- encadrer les mesures de protection et de contrôle des actifs informationnels de l'Université et du rétablissement de leur accès à la suite d'un incident;
- sensibiliser et faire participer activement les utilisatrices et utilisateurs à la protection des actifs informationnels de l'Université et aussi favoriser une utilisation responsable et éthique de ces actifs.

2. CADRE JURIDIQUE

La présente directive s'inscrit dans un cadre juridique régissant l'utilisation des technologies de l'information et l'accès à l'information, à savoir notamment :

- 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 concernant le cadre juridique des technologies de l'information* (L.R.Q., c. C-1.1);

- 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 *Directive sur la sécurité de l'information gouvernementale* (Décret 7-2014 du 15 janvier 2014);
- la *Loi sur le droit d'auteur* (L.C., 1985, c. C-42).

3. CHAMP D'APPLICATION ET PERSONNES VISÉES

En appui à la réalisation de la mission de l'Université, la directive porte sur l'utilisation des actifs informationnels appartenant à l'Université ou placés sous sa responsabilité que sont :

- le réseau informatique et de télécommunication de l'Université;
- les équipements informatiques et de télécommunication appartenant à l'Université;
- les équipements informatiques et de télécommunication qui n'appartiennent pas à l'Université mais qui sont en lien avec son réseau, incluant les appareils intelligents sans fil;
- les logiciels et les données qui résident ou qui transitent sur le réseau de l'Université et les équipements qui y sont associés;
- tous les documents numériques détenus ou hébergés par l'Université peu importe leur forme et quels que soient les supports sur lesquels ils sont fixés;
- tous les documents sur supports analogiques dont le papier, dans la mesure où l'une ou l'autre des modalités de la présente directive est applicable.

La présente directive vise toutes les utilisatrices et tous les utilisateurs des actifs informationnels de l'Université : les membres du personnel, les étudiantes et les étudiants (incluant les locataires des résidences étudiantes), les personnes œuvrant dans des organismes ou des entreprises associés à l'Université ainsi que les fournisseurs de l'Université qui accèdent aux actifs informationnels appartenant à l'Université ou sous la responsabilité de l'Université. Ainsi, tous les utilisateurs et utilisatrices sont tenus d'appliquer la directive et de participer activement à sa mise en œuvre.

La présente directive est applicable en complémentarité avec les règlements, les politiques et les autres directives de l'Université.

4. DÉFINITIONS

Aux fins de l'application de la présente directive, il est utile de relever les définitions suivantes :

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.

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.

Confidentialité : la propriété d'une information de n'être accessible qu'aux personnes ou entités désignées et de n'être divulguée qu'à celles-ci.

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.

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.

IS : l'acronyme désignant l'interface sécurisée du réseau des établissements de santé et de services sociaux.

Réseau : tout réseau de communication accessible par l'intermédiaire des équipements et des ressources informatiques et de télécommunication, contrôlé ou administré par l'Université. Lorsque l'utilisatrice ou l'utilisateur, de par ses activités professionnelles ou d'études, œuvre aussi au sein du réseau de la santé et des services sociaux, il s'agit également des équipements et des ressources informatiques et de télécommunication de l'IS de l'Estrie.

Responsable d'actifs informationnels : le membre du personnel 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 directive, 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.

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.

5. CONDITIONS D'UTILISATION DES ACTIFS INFORMATIONNELS

Au-delà des dispositions de la présente directive, l'Université s'attend à ce que la conduite de chaque utilisatrice ou utilisateur soit dictée par les règles usuelles de bienséance, de courtoisie et dans le respect des règlements, des politiques et des autres directives de l'Université ainsi que par les lois et les règlements gouvernementaux applicables. De plus, pour le personnel, l'Université s'attend à un comportement respectueux et loyal à son égard dans le cadre de l'exercice de son travail.

5.1. Utilisation responsable

Seuls les utilisateurs et utilisatrices dûment autorisés peuvent avoir accès aux actifs informationnels de l'Université, selon leurs fonctions et dans les limites de l'autorisation qui leur a été accordée. L'utilisation de ces actifs informationnels doit être faite de façon pertinente, raisonnable et efficace.

L'utilisatrice ou l'utilisateur doit utiliser les actifs informationnels avec circonspection. L'Université peut aviser la personne concernée que son usage des actifs informationnels est irrégulier et voir à ce que la situation soit corrigée.

5.2. Comportements interdits

L'utilisatrice ou l'utilisateur ne doit pas poser ou tenter de poser l'un des gestes suivants :

- prise de connaissance, modification, destruction, déplacement ou divulgation non autorisé des actifs informationnels;
- décryptage ou décodage sans autorisation de codes ou de clés d'accès ou de fichiers;
- utilisation abusive ou nuisible d'un actif informationnel;
- contournement des mécanismes de protection des actifs informationnels;
- usurpation ou tentative d'usurpation de l'identité d'une autre utilisatrice ou d'un autre utilisateur, ou de celle d'un tiers;
- non-respect de la règlementation des réseaux auxquels l'utilisatrice ou l'utilisateur a accès, qu'ils soient internes ou externes;
- utilisation d'actifs informationnels de l'Université à des fins commerciales non autorisées ou illicites;
- propagation de matériel utilisant un langage injurieux, irrespectueux, déloyal malveillant, haineux ou discriminatoire, ainsi que toute forme de harcèlement, de menace ou de diffamation;
- consultation, stockage, reproduction ou transmission de matériel pornographique;
- utilisation d'actifs informationnels à des fins autres que celles autorisées par l'Université ou par l'unité administrative de l'utilisatrice ou de l'utilisateur;
- utilisation d'actifs informationnels malveillante ou contraire aux lois en vigueur et aux règles d'éthique.

5.3. Sécurité de l'identifiant et du mot de passe associé

Les utilisatrices et utilisateurs prennent toutes les précautions nécessaires pour protéger l'intégrité et le caractère confidentiel, le cas échéant, des données utilisées. À ces fins, les codes d'accès, les mots de passe et les autorisations qui ont été octroyés ne doivent pas être partagés.

Toute utilisatrice ou utilisateur est tenu en tout temps de préserver la confidentialité du mot de passe associé à un identifiant qui lui a été attribué (ex. un code d'accès). Dans le cas d'un identifiant matériel (ex. : clé, carte magnétique, etc.), la personne concernée doit en protéger l'accès et l'utilisation.

L'utilisatrice ou l'utilisateur est responsable de l'exactitude de ses données d'identité qui doivent être valides et complètes en tout temps. En cas d'inexactitude, l'utilisatrice ou l'utilisateur doit les faire rectifier rapidement.

Une utilisatrice ou un utilisateur est réputé responsable des activités effectuées avec son identifiant et le mot de passe qui y est associé. La personne informée que le mot de passe qui protège cet identifiant a été compromis doit le changer dans les plus brefs délais et en aviser la section Sécurité informatique du Service des technologies de l'information.

Une utilisatrice ou un utilisateur ne peut atténuer, contourner ou modifier le contrôle d'accès et le fonctionnement d'un actif informationnel appartenant à l'Université ou sous la responsabilité de l'Université.

5.4. Utilisation des services de messagerie électronique

5.4.1. Identification

Pour tout message électronique diffusé sur le réseau de l'Université, l'utilisatrice ou l'utilisateur doit s'identifier à titre d'auteure ou d'auteur du message et préciser, s'il y a lieu, à quel titre elle s'exprime ou il s'exprime.

5.4.2. Comportements interdits

Il est strictement interdit à l'utilisatrice ou à l'utilisateur de transmettre du courrier électronique de façon anonyme, de falsifier son identification ou de s'identifier illégitimement au nom d'une autre personne ou encore d'envoyer des courriels non sollicités (pourriels).

5.4.3. Accès au courrier électronique pour les étudiantes et les étudiants

L'Université alloue une adresse de courrier électronique à chaque étudiante et à chaque étudiant admis à un programme d'études. L'étudiante ou l'étudiant reconnait que les différentes unités administratives de l'Université peuvent lui communiquer des informations à cette adresse durant ses études. L'étudiante ou l'étudiant a la responsabilité de consulter régulièrement sa boîte de courriels pour prendre connaissance des informations qui lui sont transmises. L'étudiante ou l'étudiant reconnaît également que les courriels reçus ou envoyés à cette adresse pourraient être conservés par un fournisseur externe de services en ligne choisi par l'Université et assujetti aux mêmes règles de confidentialité.

5.4.4. Accès au courrier électronique pour le personnel de l'Université et toute autre personne détenant une adresse USherbrooke.ca

L'Université alloue une adresse de courrier électronique à chaque membre du personnel (incluant le personnel retraité ainsi que les professeures et professeurs associés) et à certaines personnes dont les fonctions le requièrent. La personne concernée reconnait qu'elle a la responsabilité de consulter régulièrement sa boîte de courriels pour prendre connaissance des informations qui lui sont transmises. La personne reconnaît également que les courriels reçus ou envoyés à cette adresse pourraient être conservés par un fournisseur externe de services en ligne choisi par l'Université et assujetti aux mêmes règles de confidentialité. La personne reconnaît enfin que les courriels qu'elle envoie ou qu'elle reçoit avec un système de messagerie électronique de l'Université, dans le cadre de ses fonctions à l'Université, constituent des documents détenus par l'Université au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et qu'ils sont assujettis à cette loi de même qu'au *Calendrier de conservation des documents de l'Université de Sherbrooke*.

Un membre du personnel enseignant de même qu'une étudiante ou un étudiant peut utiliser son adresse @USherbrooke.ca à des fins professionnelles lorsqu'elle agit ou lorsqu'il agit en qualité d'intervenante ou d'intervenant auprès d'un établissement de santé ou de services sociaux. La personne reconnaît que les courriels qu'elle envoie ou qu'elle reçoit avec le système de messagerie électronique de l'Université en cette qualité constituent des documents détenus par cet établissement du réseau de la santé et des services sociaux au sens de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et qu'ils sont assujettis à cette loi de même qu'au *Calendrier de conservation des documents* de cet établissement.

5.5. Utilisation à des fins personnelles

L'utilisatrice ou l'utilisateur peut occasionnellement faire usage de certains actifs informationnels à des fins personnelles, par exemple pour le traitement d'informations privées et qui ont un caractère confidentiel, à la condition que cet usage soit conforme aux dispositions de la présente directive et aux lois en vigueur. Le cas échéant, la personne doit suivre les modalités d'accès et d'utilisation spécifiées par l'Université et respecter notamment les conditions suivantes :

- pour les membres du personnel, l'utilisation doit être faite en dehors des heures de travail, notamment durant les pauses ou les repas; de manière à ne pas nuire à la réalisation de leur tâche,

- pour les membres du personnel et aussi les étudiantes et les étudiants, l'utilisation ne doit pas impliquer, sans autorisation, l'installation, l'exécution ou le téléchargement sur le poste de travail appartenant à l'Université d'applications pour lesquelles l'utilisatrice ou l'utilisateur ne détient pas les licences appropriées. L'autorisation, le cas échéant, ne sera émise qu'à la condition que de telles applications ne perturbent pas le fonctionnement normal des autres actifs informationnels de l'Université et n'entraînent pas de coûts supplémentaires pour l'Université. Les personnes pouvant fournir de telles autorisations sont les personnes qui ont la responsabilité immédiate de la gestion, de l'exploitation et de la sécurité des actifs informationnels mentionnées à l'article 6.2 de la présente directive.

Pour les membres du personnel, l'utilisation à des fins personnelles inclut notamment l'utilisation des réseaux sociaux (Facebook, Twitter, etc.) à des fins non requises dans le cadre des fonctions de l'utilisatrice ou de l'utilisateur. L'utilisation d'appareils à des fins personnelles durant les heures de travail (téléphones intelligents, tablettes, etc.) doit être faite avec discernement et de manière responsable pour des besoins ne pouvant être comblés en dehors des heures de travail.

Pour toute utilisatrice ou tout utilisateur, l'utilisation à des fins personnelles ne peut, sans exception, permettre l'usage pour des activités commerciales, de publicité ou de sollicitation.

Malgré ce qui précède, l'Université pourrait limiter ou interdire l'usage de ses actifs informationnels à des fins personnelles.

5.6. Protection des données personnelles

L'utilisatrice ou l'utilisateur est responsable de la protection de ses données personnelles, sous réserve de l'obligation générale de l'Université de protection des réseaux et des équipements technologiques qu'elle rend disponibles à ses utilisatrices et utilisateurs.

Dans certaines circonstances particulières, notamment en cas d'absence temporaire ou prolongée d'un membre de la communauté universitaire, ou encore lorsqu'il est nécessaire de remplacer un poste de travail ou de le réparer, la confidentialité des données personnelles de la personne concernée peut ne pas être totalement assurée. Chaque fois que les circonstances le permettent, la personne concernée est avisée afin de lui donner l'occasion de préserver ces informations. Lorsqu'un tel accès par un tiers est nécessaire, la supérieure ou le supérieur hiérarchique et la directrice générale ou le directeur général du Service des technologies de l'information doivent prendre les moyens raisonnables à leur disposition afin de limiter l'accès du tiers aux données personnelles en tenant compte des circonstances.

5.7. Protection des ordinateurs et autres dispositifs d'accès

L'utilisatrice ou l'utilisateur doit veiller à la sécurité des actifs informationnels mis à sa disposition ou placés sous sa responsabilité. Lorsqu'il lui semble que la sécurité de ces actifs est compromise ou pourrait être compromise, l'utilisatrice ou l'utilisateur doit le signaler à la section Sécurité informatique du Service des technologies de l'information.

L'utilisatrice ou l'utilisateur des actifs informationnels de l'Université doit veiller à ce que le dispositif d'accès utilisé ou placé sous sa responsabilité soit employé de façon adéquate afin d'assurer son intégrité (par exemple : protection contre les virus et autres logiciels malveillants, utilisation par les personnes autorisées seulement).

L'utilisatrice ou l'utilisateur ou la personne responsable des dispositifs d'accès de l'Université doit garantir la protection physique de ces équipements en mettant en place des mesures appropriées, avec le soutien du Service des technologies de l'information.

5.8. Droits de propriété intellectuelle

En tout temps, l'utilisatrice ou l'utilisateur doit respecter les droits de propriété intellectuelle notamment les droits d'auteur des tiers et les ententes contractuelles avec les fournisseuses et fournisseurs de contenu alimentant les bibliothèques virtuelles.

Les reproductions de logiciels, de progiciels ou de didacticiels ne sont autorisées qu'à des fins de copies de sécurité ou selon les licences d'utilisation les régissant.

Il est strictement interdit à l'utilisatrice ou l'utilisateur :

- de reproduire la documentation associée à un logiciel sans l'autorisation écrite du titulaire du droit d'auteur;
- d'utiliser toute reproduction illicite d'un logiciel ou d'un fichier électronique;
- de participer directement ou indirectement à la reproduction illicite d'un logiciel ou d'un fichier électronique;
- de commettre ou de tenter de commettre toute autre action contrevenant aux droits de propriété intellectuelle.

6. GESTION, EXPLOITATION ET PROTECTION DES ACTIFS INFORMATIONNELS

6.1. Responsabilité générale

La responsabilité générale de la gestion des actifs informationnels relève du Secrétariat général de l'Université notamment en ce qui concerne les règlements, les politiques, les directives et les orientations institutionnelles.

6.2. Responsabilités opérationnelles

La responsabilité immédiate de la gestion, de l'exploitation et de la sécurité des actifs informationnels revient à la direction des facultés, des centres universitaires de formation, des instituts de recherche et des services qui peuvent toutefois désigner des responsables opérationnels dans leurs unités respectives à la condition d'en informer la direction générale du Service des technologies de l'information.

Au plan opérationnel, la personne responsable d'actifs informationnels doit s'assurer de la réalisation des activités suivantes concernant les actifs informationnels relevant de l'unité :

- l'identification, la localisation et la classification des actifs;
- l'évaluation et la révision périodique de la sensibilité des actifs en termes de disponibilité, d'intégrité et de confidentialité;
- la sensibilisation à la sécurité auprès de ses utilisatrices et utilisateurs;
- la vérification de conformité des mesures de protection mises en place pour protéger les actifs informationnels.

Cette personne peut être assistée par le Service des bibliothèques et archives et par le Service des technologies de l'information.

6.3. Directives et procédures institutionnelles complémentaires de sécurité des actifs informationnels

Dans le but d'assurer la disponibilité, l'intégrité et la confidentialité des actifs informationnels de l'Université, le comité de direction de l'Université peut adopter des directives ou des procédures institutionnelles complémentaires à la présente directive. Le cas échéant, celles-ci définissent

les orientations et les exigences pratiques qui doivent être respectées par les utilisatrices et utilisateurs ainsi que par les responsables d'actifs informationnels.

6.4. Gestion des droits d'accès

Tout actif informationnel contenant des renseignements personnels, confidentiels ou à accès restreint doit être protégé minimalement par un mécanisme d'identification et d'authentification de l'utilisatrice ou de l'utilisateur dans un environnement sécurisé. Ce mécanisme doit également permettre de limiter la divulgation, le traitement et la mise à la disposition des données et des systèmes aux seules personnes ou entités autorisées, selon les modalités établies. Il doit s'agir d'un mécanisme institutionnel approuvé, sous réserve d'une dérogation prévue à l'article 9 de la présente directive.

L'octroi des droits d'accès doit être consenti selon les modalités établies par la personne responsable des actifs informationnels visés. Ces modalités doivent s'inspirer du principe du moindre accès tout en tenant compte de l'efficience opérationnelle. Ce principe consiste à limiter l'accès au minimum de personnes requises par la nécessité du service et à ne rendre accessibles que les seules données pertinentes à l'exercice de leur fonction et non à l'ensemble des données.

Lorsqu'une utilisatrice ou un utilisateur perd la qualité en vertu de laquelle un droit d'accès à un actif informationnel de l'Université lui a été accordé, cette personne perd sans délai ce droit d'accès.

6.5. Vérification

La secrétaire générale ou le secrétaire général est responsable de la surveillance et du respect des conditions d'utilisation des actifs informationnels. Dans les limites des lois, des conventions collectives, des protocoles et des règlements établissant les conditions de travail, cette personne peut procéder aux vérifications ou contrôles d'usage requis afin de veiller au respect des dispositions de la présente directive ou encore des lois, des règlements, des politiques, des autres directives et de toute autre disposition similaire applicable. La secrétaire générale ou le secrétaire général peut désigner une autre personne pour procéder en son nom.

Une vérification des informations personnelles et privées d'une utilisatrice ou d'un utilisateur ou de son utilisation des actifs informationnels ne peut être effectuée sans le consentement de cette personne à moins que la secrétaire générale ou le secrétaire général ait des motifs raisonnables de croire que cette personne a contrevenu ou contrevient aux lois, aux règlements, aux politiques ou aux directives applicables. Lorsqu'une contravention est présumée, la secrétaire générale ou le secrétaire général peut effectuer la vérification sans le consentement de la personne concernée. La secrétaire générale ou le secrétaire général maintient un registre des vérifications effectuées dans le cadre de contraventions présumées. Si une contravention est présumée de la part de la secrétaire générale ou du secrétaire général, le vice-recteur responsable des technologies de l'information peut effectuer la vérification sans le consentement de la personne concernée.

6.6. Vie privée et surveillance des actifs informationnels

L'Université effectue la surveillance et le contrôle de ses équipements et de ses ressources informatiques et de télécommunication par différents moyens technologiques (équipements et logiciels). Cette surveillance a pour but de favoriser la pérennité et le bon fonctionnement de ses équipements et ressources informatiques ainsi que le respect de la présente directive.

Les données collectées pourront servir lors de vérifications effectuées conformément aux dispositions de la présente directive. Dans le cas des utilisatrices et utilisateurs de l'Université qui, de par leurs activités professionnelles ou d'études, œuvrent également au sein d'un établissement du réseau de la santé et des services sociaux, les données collectées pourront servir lors de vérifications effectuées à la demande de la personne responsable de la sécurité de l'information de cet établissement. La consultation et l'interprétation de données privées et confidentielles à partir de ces activités peuvent être faites pour des motifs valables.

L'utilisation d'actifs informationnels de l'Université constitue de la part de l'utilisatrice ou de l'utilisateur une reconnaissance et une acceptation qu'elle est sujette à la surveillance et au contrôle de l'Université relativement à cette utilisation, à cette surveillance et à ce contrôle, sous réserve de l'article 6.5 de la présente directive.

7. GESTION DES PROBLÈMES ET DES INCIDENTS DE SÉCURITÉ DES ACTIFS INFORMATIONNELS

7.1. Communication des incidents

L'utilisatrice ou l'utilisateur qui pose une action donnant lieu à un incident de sécurité informatique est présumé être de bonne foi jusqu'à preuve du contraire.

Tout incident de sécurité qui risque de porter atteinte à la disponibilité, à l'intégrité ou à la confidentialité de l'information détenue par l'Université doit être signalé à la section Sécurité informatique du Service des technologies de l'information.

L'utilisatrice ou l'utilisateur qui constate un incident de sécurité informatique doit prendre les actions appropriées selon la nature de l'incident pour en limiter les impacts en attendant les interventions recommandées par la section sécurité du Service des technologies de l'information. Si un service de proximité existe dans son unité administrative, l'utilisatrice ou l'utilisateur est tenu de s'en prévaloir.

L'utilisatrice ou l'utilisateur doit collaborer avec les responsables d'actifs informationnels dans le cadre d'exercices d'évaluation de la sécurité informatique et des investigations lors d'incident de sécurité.

7.2. Mesures d'urgence

Lorsque la nature du cas comporte des éléments qui laissent croire que la sécurité des actifs informationnels pourrait être compromise, la directrice générale ou le directeur général du Service des technologies de l'information doit s'assurer que les mesures nécessaires sont mises en place afin de garantir la protection des actifs informationnels.

Afin de préserver l'intégrité des services offerts et des actifs informationnels, la directrice générale ou le directeur général du Service des technologies de l'information peut, après avoir pris les moyens raisonnables pour aviser les responsables ou les utilisatrices et les utilisateurs d'actifs informationnels, poser les actions suivantes ou exiger que ces actions soient posées :

- interrompre ou révoquer temporairement les services offerts à certains utilisateurs ou utilisatrices afin de protéger les autres membres de la communauté universitaire et la communauté des utilisatrices et utilisateurs externes;
- intervenir sur un actif informationnel utilisé ou présumément utilisé en contravention à l'une ou l'autre des dispositions prévues dans cette directive;
- appliquer les différentes fonctions de diagnostic sur les actifs informationnels;
- prendre les mesures urgentes requises afin de circonscrire la situation.

8. SANCTIONS

Dans le cas où un incident résulterait d'agissements volontaires ou d'une utilisation personnelle abusive, l'Université peut appliquer des sanctions en référant l'incident aux instances concernées.

Dans le cas d'une étudiante ou d'un étudiant, la directrice générale ou le directeur général du Service des technologies de l'information peut, selon la gravité de la situation, appliquer des mesures provisoires et soumettre la plainte de délit au processus disciplinaire prévu au *Règlement des études*.

Dans le cas d'un membre du personnel, la plainte est référée à la supérieure immédiate ou au supérieur immédiat qui doit en informer la directrice générale ou le directeur général du Service des ressources humaines et prendre les mesures requises en concertation avec cette dernière ou ce dernier.

Tous les autres cas impliquant des utilisatrices ou des utilisateurs qui contreviennent aux lois, règlements, politiques et directives en vigueur, et qui ne sont pas des étudiantes ou des étudiants de l'Université ni des membres de son personnel, sont pris en charge par la directrice générale ou le directeur général du Service des technologies de l'information et traités selon les procédures de gestion établies.

L'utilisatrice ou l'utilisateur qui contrevient aux dispositions de cette directive peut, en plus des pénalités ou des sanctions prévues par les lois, les règlements, les directives, les conventions collectives, les protocoles ou les règlements établissant les conditions de travail, être l'objet de l'une ou plusieurs des mesures administratives suivantes :

- l'annulation de ses privilèges d'accès aux actifs informationnels;
- la facturation des services rendus et des frais encourus par l'Université pour rétablir le service, le cas échéant;
- l'obligation de rembourser à l'Université toute somme que celle-ci a été appelée à défrayer à titre de dommage, de pénalités ou autre à la suite de l'incident, le cas échéant.

9. DÉROGATION

Lorsqu'une disposition de la présente directive est incompatible avec des activités ou un projet directement relié à la mission de l'Université, l'utilisatrice ou l'utilisateur peut demander par écrit une dérogation à la secrétaire générale ou au secrétaire général.

Après analyse des motifs appuyant la demande de dérogation, la secrétaire générale ou le secrétaire général rend sa décision, étant entendu que cette personne peut déléguer à la directrice générale ou au directeur général du Service des technologies de l'information l'analyse et la décision relatives à des dérogations de nature purement techniques ou strictement opérationnelles.

La secrétaire générale ou le secrétaire général maintient un registre des dérogations accordées et informe le comité de sécurité de l'information des dérogations significatives qui ont été autorisées.

10. RESPONSABILITÉ DE LA DIRECTIVE

La secrétaire générale ou le secrétaire général assume la responsabilité générale de la diffusion, de l'application et de la mise à jour de la présente directive.

Il appartient cependant à la doyenne ou au doyen de chaque faculté, à la directrice ou au directeur de chaque centre universitaire de formation ou d'institut ainsi qu'à la directrice générale ou au directeur général de chaque service de voir à ce que la présente directive soit respectée dans les lieux et lors du déroulement des activités relevant de son autorité.

11. ENTRÉE EN VIGUEUR

La présente directive entre en vigueur à la date fixée par le comité de direction de l'Université.