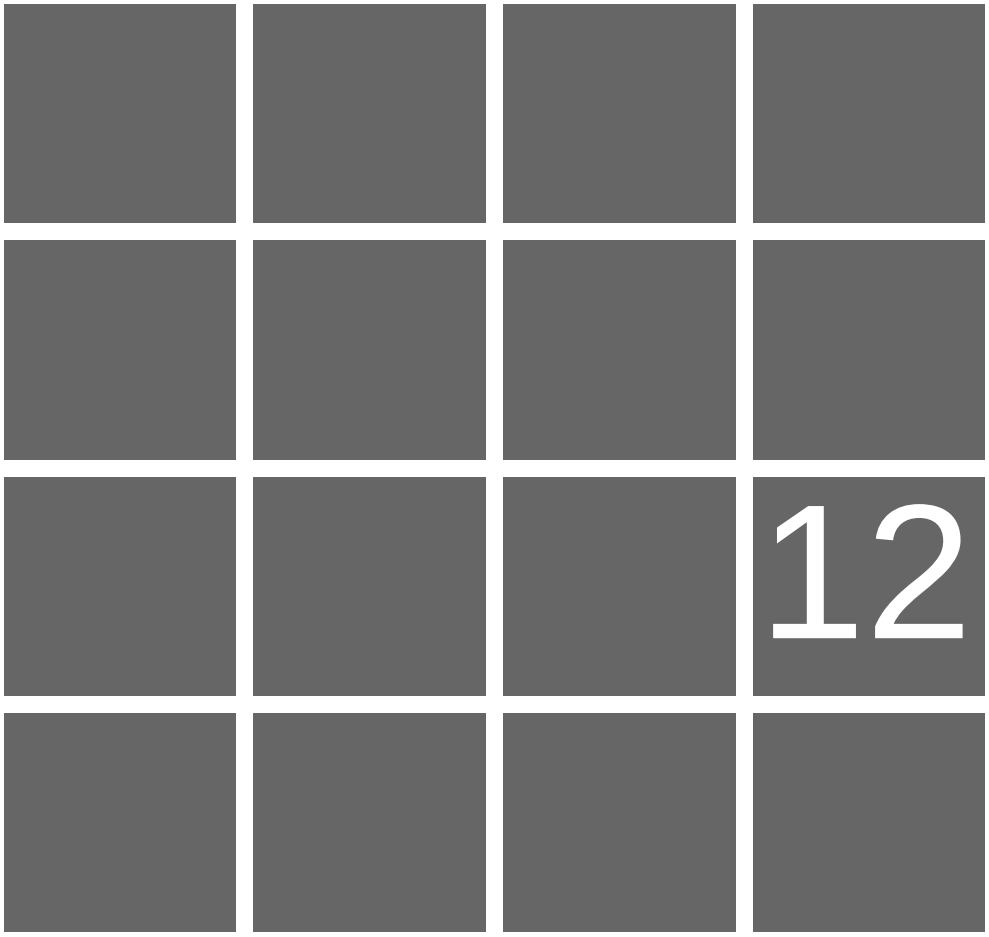
Le texte que vous consultez est une codification administrative des Règlements de l'UQAM. Leur version officielle est contenue dans les résolutions adoptées par le Conseil d'administration de l'UQAM.

La version des Règlements que vous consultez est celle qui était en vigueur en juillet 2018.

Règlement sur l'utilisation et la gestion des actifs informationnels

Règlement
numéro 12



Université du Québec à Montréal

TABLE DES MATIÈRES

RÈGLEMENT NO 12
RÈGLEMENT SUR L'UTILISATION ET LA GESTION DES ACTIFS INFORMATIONNELS

ARTICLE 1 - DÉFINITIONS

Dans ce règlement, à moins que le contexte ne s'y oppose, les expressions suivantes signifient ce qui suit :

a) « actif informationnel » : tout équipement relié ou non au réseau, logiciel, système, donnée ou information utilisés pour l'hébergement, le traitement, la diffusion et l'échange d'informations, qu'ils soient la propriété de l'UQAM ou qu'ils utilisent ou hébergent des actifs dont l'Université est propriétaire, fiduciaire ou dépositaire;

b) « norme institutionnelle de sécurité informatique » : ensemble de spécifications en vigueur à l'UQAM, dont l'objectif consiste à recommander ou à prescrire les technologies, les procédures ou les paramètres devant être utilisés pour satisfaire aux exigences de sécurité informatique. Ces normes sont établies conformément aux responsabilités prévues dans la Politique de sécurité informatique;

c) « utilisatrice ou utilisateur » : les professeures et professeurs, les chargées et chargés de cours, les cadres, les employées et employés ainsi que les étudiantes et étudiants de l'Université, de même que toute personne utilisatrice des actifs informationnels ou services de l'Université.

ARTICLE 2 - SÉCURITÉ DE L'IDENTIFIANT ET DE L'AUTHENTIFIANT

Tout utilisatrice ou utilisateur est tenu de préserver la confidentialité de son mot de passe ou de ce qui en tient lieu et, dans le cas d'un authentifiant matériel (carte, jeton, etc.), d'en protéger l'accès et l'utilisation.

L'utilisatrice ou utilisateur est réputé imputable des activités entreprises par le biais de ses codes d'accès (identifiants) et authentifiants. Elle ou il ne doit alors pas en divulguer la teneur à une tierce partie sans ensuite le modifier rapidement de façon confidentielle. Elle ou il est également responsable de restreindre l'accès à des tierces parties aux ordinateurs et autres dispositifs d'accès authentifiés aux réseaux grâce à ses identifiants et authentifiants.

L'utilisatrice ou utilisateur doit s'assurer que l'authentifiant respecte minimalement les normes institutionnelles de sécurité informatique propres aux actifs informationnels qu'elle ou il utilise.

ARTICLE 3 - CONDITIONS D'UTILISATION DES ACTIFS INFORMATIONNELS (résolutions 2014-E-8897 et 2011-A-15037, 2016-E-9223 et 2011-A-15037)

L'utilisation des actifs informationnels est limitée à la réalisation de la mission prévue de ces actifs et au respect des droits et responsabilités des autres utilisatrices et utilisateurs.

Les utilisatrices ou utilisateurs sont tenus de se conformer au présent règlement, aux normes institutionnelles et à toutes les politiques, règles d'utilisation et codes d'éthique des Services du Vice-rectorat aux systèmes d'information.

À moins d'une autorisation par les responsables des actifs informationnels en cause ou d'une utilisation effectuée dans le cadre d'une activité académique légale, l'utilisatrice ou utilisateur ne doit pas poser ou tenter de poser l'un des gestes suivants :

- prise de connaissance, modification, destruction, déplacement ou divulgation non autorisés des actifs informationnels;
- lecture, modification ou destruction de tout message, texte, donnée ou logiciel sans l'autorisation de leur propriétaire ou de la ou du responsable des actifs informationnels concerné;
- décryptage ou décodage de codes ou de clés d'accès, de fichiers ou de mots de passe sans autorisation préalable des responsables de ces ressources;
- utilisation d'un actif informationnel abusive ou nuisible à son bon fonctionnement;
- contournement des mécanismes de protection des actifs informationnels ;
- non-respect de la réglementation des réseaux externes auxquels on a accès, ni de l'intégrité des systèmes informatiques ainsi accessibles;
- utilisation des actifs informationnels de l'Université à des fins commerciales non autorisées ou illicites;
- propagation de matériel utilisant un langage injurieux, malveillant, haineux ou discriminatoire, ainsi que de toute forme de harcèlement, de menace ou de diffamation;
- consultation et propagation de matériel pornographique;
- vol de ressources et utilisation malicieuse ou contraire aux lois et règles d'éthique en vigueur.

L'installation, le déplacement, la désinstallation ou l'utilisation d'un équipement de télécommunications personnel (par exemple : routeur, routeur sans-fil, équipement RF, etc.) sur le réseau de l'Université doit être approuvé par la directrice, le directeur des Services informatiques - Infrastructures et la directrice, le directeur des Services informatiques – Bureau de la sécurité et de la gouvernance.

Cette approbation a pour but de mieux cerner les besoins de la requérante, du requérant, de l'informer des conséquences de l'utilisation d'équipement de télécommunications personnel et, au besoin, de lui proposer d'autres solutions dans le cas où l'utilisation d'un de ces équipements pourrait affecter la qualité du service du réseau de télécommunications institutionnel.

3.1 Utilisation des services de messagerie électronique

Une utilisatrice ou utilisateur est responsable de sa messagerie électronique, qui comprend une boîte vocale et une adresse de courriel.

3.1.1 Identification

Pour tout message électronique diffusé, l'utilisatrice ou utilisateur doit s'identifier en tant que signataire du message et préciser, s'il y a lieu, à quel titre elle ou il s'exprime.

3.1.2 Comportements interdits

L'utilisatrice ou utilisateur doit s'assurer que l'utilisation de sa messagerie électronique ou de toute autre messagerie à laquelle elle, il a accès à partir des actifs informationnels de l'Université (postes de travail, serveurs, téléphones, etc.) respecte le présent règlement. À cet effet, les comportements suivants sont interdits :

- utiliser, dans tout courriel diffusé ou dans tout message laissé dans une boîte vocale, un langage injurieux, malveillant, haineux ou discriminatoire, ainsi que toute forme de harcèlement, de menace ou de diffamation;
- capter, stocker, reproduire ou transmettre (au moyen du réseau de télécommunications vers une boîte vocale ou une adresse électronique) du matériel ou un message à caractère illégal;
- se servir de l'adresse de courriel ou de la messagerie électronique à des fins commerciales (annonces publicitaires, pourriels, etc.) ou illicites, ou en faciliter l'utilisation à ces fins;
- avoir recours à un ou des subterfuges ou à d'autres moyens pour transmettre du courriel ou des messages vocaux de façon anonyme ou au nom d'une autre personne.

3.1.3 Accès au courriel pour les étudiantes, lesétudiants

L'Université fournit une adresse de courriel à chaque étudiante, chaque étudiant. Elle, il reconnaît que les différentes unités de l'Université pourront lui communiquer des informations à cette adresse de courriel durant ses études.

À cet effet, l'étudiante, l'étudiant doit consulter régulièrement le contenu de sa boîte de messages.

3.1.4 Accès au courriel pour le personnel de l'Université

L'Université fournit une adresse de courriel à chaque employée, employé qui, si elle, il utilise un poste de travail informatisé, doit consulter régulièrement le contenu de sa boîte de messages pour prendre connaissance des informations qui lui seront transmises par les différentes unités de l'Université.

3.2 Utilisation personnelle (résolutions 2014-E-8897 et 2011-A-15037, 2016-E-9223 et 2011-A-15037)

Les utilisatrices ou utilisateurs peuvent faire un usage raisonnable de certains actifs informationnels à des fins personnelles, par exemple, pour le traitement de renseignements qui leur sont personnels et qui ont un caractère confidentiel, à la condition que cet usage soit conforme aux dispositions de ce règlement.

Dans certains cas, l'utilisation des actifs informationnels à des fins personnelles, par exemple, l'utilisation du réseau et des ordinateurs publics pour l'échange de fichiers ou le clavardage, peut faire l'objet de restrictions ou d'interdictions par l'unité concernée.

Le droit à l'utilisation personnelle n'a pas pour effet d'empêcher l'accès à un actif informationnel par une personne autorisée, autre que son utilisatrice ou utilisateur principal, lorsque cet accès est requis par la nécessité du service et qu'il est autorisé par la supérieure immédiate, le supérieur immédiat de l'utilisatrice ou utilisateur principal et de la directrice, le directeur des Services informatiques – Bureau de la sécurité et de la gouvernance. L'utilisation par une personne autorisée de l'ordinateur d'une employée, d'un employé en cas d'absence ou de maladie en est un exemple. Cet accès doit respecter le principe de moindre accès et n'être octroyé qu'en cas de nécessité du service.

Dans tous les cas où un tel accès est nécessaire, la supérieure hiérarchique, le supérieur hiérarchique et la directrice, le directeur des Services informatiques – Bureau de la sécurité et de la gouvernance doivent prendre les moyens raisonnables pour aviser préalablement l'utilisatrice ou utilisateur principal de l'actif informationnel. Dans tous les cas, l'utilisatrice ou utilisateur principal doit être avisé à posteriori des accès autorisés, du motif de leur autorisation et de la durée de l'accès par une tierce partie.

3.3 Protection des ordinateurs et autres dispositifs d'accès

L'utilisatrice ou utilisateur doit assurer la sécurité des ordinateurs et autres dispositifs d'accès aux actifs informationnels qu'elle, qu'il utilise ou dont elle, il est responsable.

Tout utilisatrice ou utilisateur des actifs informationnels de l'Université doit s'assurer que le dispositif d'accès qu'elle, qu'il utilise, ou dont elle, il est responsable, est protégé contre les virus et autres logiciels pernicieux. Ce même dispositif doit également être protégé contre les failles corrigibles de sécurité des systèmes ou des applications utilisées, dans le respect des normes institutionnelles établies pour ces systèmes.

Tout utilisatrice ou utilisateur ou responsable des dispositifs d'accès qui sont sous la responsabilité de l'Université doit garantir la protection physique de ces équipements en mettant en place des mesures appropriées.

3.4 Droits de propriété intellectuelle

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

La reproduction de logiciels, de progiciels ou de didacticiels n'est autorisée qu'à des fins de copies de sécurité ou selon les normes institutionnelles de la licence d'utilisation la régissant. Il est strictement interdit aux utilisatrices ou utilisateurs de :

- reproduire ou utiliser toute reproduction illicite d'un logiciel, d'un fichier électronique ou de la documentation qui y est jointe;
- participer directement ou indirectement à la reproduction illicite d'un logiciel ou d'un fichier électronique;

- consulter, modifier ou détruire un logiciel ou une banque de données sans l'autorisation de la détentrice, du détenteur des droits;
- utiliser les actifs informationnels afin de commettre ou de tenter de commettre une infraction aux lois, en particulier les lois régissant la propriété intellectuelle.

ARTICLE 4- GESTION, EXPLOITATION ET PROTECTION DES ACTIFS INFORMATIONNELS (résolutions 2014-E-8897 et 2011-A-15037, 2016-E-9223 et 2011-A-15037)

4.1 Responsabilité

La responsabilité de chacun des actifs informationnels est formellement attribuée à une, un « responsable » dont l'identité et la portée des responsabilités en matière de protection de ces actifs sont communiquées à la directrice, au directeur des Services informatiques – Bureau de la sécurité et de la gouvernance.

4.2 Normes institutionnelles de sécurité informatique

Des normes institutionnelles de sécurité informatique définissent les orientations et les exigences pratiques et concrètes qui doivent être respectées par les utilisatrices ou utilisateurs et les responsables de systèmes.

Ces normes institutionnelles sont élaborées dans le cadre d'un processus de collaboration et de consultation entre les responsables de systèmes, les utilisatrices ou utilisateurs et la directrice, le directeur des Services informatiques – Bureau de la sécurité et de la gouvernance.

Les normes énonçant les grandes orientations de sécurité informatique peuvent être émises sans nécessiter d'approbation formelle. Les normes de nature prescriptive doivent être approuvées par les représentantes, les représentants des gestionnaires et des utilisatrices ou utilisateurs des actifs informationnels concernés.

4.3 Gestion des droits d'accès

Tout actif informationnel contenant des renseignements confidentiels ou à accès restreint doit être protégé, au minimum, par un mécanisme d'identification et d'authentification de l'utilisatrice ou utilisateur. 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.

L'octroi des droits d'accès doit être effectué par le biais d'une procédure établie par la, le responsable de systèmes ou la directrice, le directeur des Services informatiques – Bureau de la sécurité et de la gouvernance, et faire l'objet d'une autorisation formelle par la, le responsable identifié. Cette procédure doit notamment respecter le principe de moindre accès, qui consiste à limiter l'accès au minimum de personnes requis par la nécessité du service et à ne rendre accessibles que les seules données pertinentes à l'exercice de leur fonction et non l'ensemble des données.

4.4 Protection des actifs informationnels

Les responsables des actifs informationnels doivent effectuer une évaluation des risques inhérents aux actifs dont elles, ils ont la charge. Pour ce faire, elles, ils peuvent être assistés par la directrice, le le directeur des Services informatiques – Bureau de la sécurité et de la gouvernance afin de cerner adéquatement les besoins de sécurité en matière de confidentialité, d'intégrité et de disponibilité de l'actif.

Les responsables de systèmes sont également responsables de s'assurer de la mise en œuvre des moyens nécessaires pour combler les besoins de sécurité informatique.

ARTICLE 5 - GESTION DES PROBLÈMES ET DES INCIDENTS DE SÉCURITÉ INFORMATIQUE ET SANCTIONS
(résolutions 2005-A-12811, 2008-A-13724, 2016-E-9223 et 2011-A-15037)

5.1 Contrôle et vérification
(résolutions 2010-A-14543, 2013-A-15988, 2014-E-8897 et 2011-A-15037, 2015-A-16761, 2018-A-17787 et 2011-A-15037)

Dans le cadre des activités de contrôle et de vérification, l'Université et ses représentantes, ses représentants ont l'obligation de respecter la dignité, la liberté d'expression, la liberté de pensée et la vie privée des membres de la communauté.

Les responsables de systèmes, la supérieure immédiate, le supérieur immédiat, les Services informatiques – Bureau de la sécurité et de la gouvernance sont autorisés à mandater une représentante, un représentant et à procéder à toutes les vérifications d'usage estimées nécessaires pour s'assurer du respect des dispositions de ce règlement ainsi que des politiques, normes institutionnelles, directives, règles d'utilisation, ententes et protocoles pertinents de l'Université ou des lois et règlements provinciaux ou fédéraux.

Une vérification nominative des renseignements personnels et privés d'une utilisatrice ou utilisateur ou de son utilisation des actifs informationnels ne peut être effectuée sans le consentement de cette personne, à moins que la supérieure immédiate, le supérieur immédiat, les responsables de systèmes, les Services informatiques – Bureau de la sécurité et de la gouvernance n'aient des motifs valables de croire que cette dernière contrevient à l'une ou l'autre des dispositions mentionnées au paragraphe précédent.

De plus, cette vérification ne peut être entamée qu'après avoir obtenu l'autorisation de la vice-rectrice, du vice-recteur à la Vie académique dans le cas des personnels enseignants ou de la vice-rectrice, du vice-recteur au Développement humain et organisationnel dans le cas des personnels non enseignants et de la vice-rectrice, du vice-recteur aux Systèmes d'information ou, en cas d'absence desdits vice-rectrices ou vice-recteurs, de la rectrice, du recteur.

L'utilisation de la technologie dans les activités de contrôle et de vérification ne peut pas permettre que soient surveillés, sans motifs valables, les faits et gestes des utilisatrices ou utilisateurs ou le contenu de leurs communications.

Cette restriction ne s'applique cependant pas aux activités de journalisation automatique par des logiciels, lesquels sont nécessaires pour assurer la pérennité des services à la communauté. C'est alors la consultation et l'interprétation de données nominatives qui ne peuvent être faites sans motif valable, conformément au processus de vérification décrit ci-dessous.

Dans le cas d'une vérification qui impliquerait l'accès à des données privées et confidentielles, que ces données soient l'objet ou non de la vérification, l'Université doit veiller à éviter toute surveillance ou contrôle abusifs. L'Université ne peut vérifier que lorsqu'elle possède des motifs valables de croire qu'une utilisatrice ou utilisateur manque à ses obligations ou abuse des outils qui lui sont fournis.

Dans l'éventualité où une vérification nominative des informations personnelles et privées d'une utilisatrice ou utilisateur ou de son utilisation des actifs informationnels a été effectuée et que l'ensemble du

processus de vérification et des activités qui en découlent est complété, l'utilisatrice ou utilisateur doit être informé de la vérification qui a eu lieu et des renseignements qui ont été consultés dans ce cadre.

5.2 Communication des incidents
(résolutions 2014-E-8897 et 2011-A-15037)

Les utilisatrices ou utilisateurs qui constatent un incident de sécurité informatique doivent prendre les actions appropriées, selon la nature de l'incident, pour corriger la situation et limiter les probabilités qu'il se répète. Si elles le désirent, ces personnes peuvent également aviser la directrice, le directeur des Services informatiques – Bureau de la sécurité et de la gouvernance de l'incident, et ce, même si elles considèrent que la situation est résolue.

Si les utilisatrices ou utilisateurs jugent qu'elles, qu'ils ne disposent pas des moyens nécessaires pour poser personnellement les actions correctives appropriées à un incident ou que l'incident est de nature à avoir des répercussions sur le reste de la communauté, elles, ils doivent le signaler à la directrice, au directeur des Services informatiques – Bureau de la sécurité et de la gouvernance.

Les utilisatrices ou utilisateurs doivent également collaborer, dans la limite où cette collaboration ne leur portera pas un préjudice personnel, avec les services concernés dans le cadre des exercices d'évaluation de la sécurité informatique et des investigations lors d'incidents de sécurité informatique.

5.3 Mesures d'urgence
(résolutions 2014-E-8897 et 2011-A-15037)

Afin de préserver l'intégrité des services des actifs informationnels, les Services informatiques – Bureau de la sécurité et de la gouvernance peuvent, après avoir pris les moyens raisonnables pour aviser les responsables ou les utilisatrices ou utilisateurs des actifs informationnels, poser les actions suivantes ou exiger qu'elles soient posées :

- interrompre ou révoquer temporairement les services offerts à certains utilisatrices ou utilisateurs afin de protéger le reste de la communauté;
- intervenir sur un actif informationnel suspecté de contrevenir à l'une ou l'autre des dispositions prévues dans ce règlement;
- appliquer les différentes fonctions de diagnostic sur les actifs informationnels;
- prendre les mesures urgentes requises afin de circonscrire la situation.

5.4 Sanctions
(résolutions 2013-A-15988, 2014-E-8897 et 2011-A-15037, 2015-A-16761, 2015-A-16988, 2018-A-17787 et 2011-A-15037)

L'utilisatrice ou utilisateur qui pose des actions qui constituent un incident de sécurité informatique est présumé être de bonne foi jusqu'à preuve du contraire.

Dans le cas où des incidents de sécurité informatique résulteraient d'agissements volontaires et malicieux d'une utilisatrice ou utilisateur ou d'une utilisation personnelle abusive, l'Université peut appliquer des sanctions en transmettant l'incident aux instances suivantes :

5.4.1 Dans les cas d'étudiantes, d'étudiants, les Services informatiques – Bureau de la sécurité et de la gouvernance peuvent, selon la gravité de l'incident, mettre en place des mesures provisoires de sécurité spécifiques à ce type d'utilisatrice ou utilisateur. Si des mesures disciplinaires ou de suspension sont requises, le cas est soumis soit au Comité de discipline ou au Comité d'intervention selon la juridiction de ces comités et est traité conformément aux dispositions prévues par le Règlement no 2 de régie interne.

5.4.2 Les cas de membres du personnel sont référés à la supérieure immédiate, au supérieur immédiat qui prend les mesures requises en concertation avec le Vice-rectorat à la vie académique dans le cas des personnels enseignants ou avec le Vice-rectorat au Développement humain et organisationnel dans le cas des personnels non enseignants. Lorsque la nature du cas comporte des éléments pouvant laisser croire que la sécurité des actifs informationnels pourrait être compromise, les Services informatiques – Bureau de la sécurité et de la gouvernance doivent en discuter avec le Vice-rectorat aux systèmes d'information afin que les actions envisagées assurent la sécurité des actifs informationnels de l'Université dans le respect des droits des membres du personnel.

5.4.3 Tous les cas de personnes autres que des étudiantes, étudiants ou des employées, employés présentant des comportements pouvant porter atteinte à la sécurité informatique sont pris en charge par les Services informatiques – Bureau de la sécurité et de la gouvernance selon les procédures de gestion établies.

Les Services du Vice-rectorat aux systèmes d'information sont habilités, sur recommandation des instances disciplinaires, à prendre les dispositions suivantes :

- modification des modalités d'utilisation spécifiques à l'utilisatrice ou utilisateur et exigence d'engagement de sa part à respecter la nouvelle convention d'utilisation;
- annulation du droit d'accès ou surveillance des activités liées aux codes d'accès de l'utilisatrice ou utilisateur;
- interdiction par les responsables de systèmes d'utiliser en totalité ou en partie leurs services, y compris l'accès aux laboratoires de micro-informatique ou aux postes publics des bibliothèques;
- facturation par les Services du Vice-rectorat aux systèmes d'information des services rendus pour rétablir le service;
- réclamation du remboursement de toute somme que l'Université serait appelée à payer à titre de dommages ou de pénalité à la suite de l'incident.

ARTICLE 6 - PROCESSUS DE DÉROGATION

6.1 Demande
(résolutions 2014-E-8897 et 2011-A-15037, 2016-E-9223 et 2011-A-15037)

Compte tenu que la mission de l'Université est d'assurer la formation, de rendre accessibles les connaissances et de répondre aux besoins de la collectivité, l'Université prévoit que certaines initiatives de sa communauté puissent nécessiter un assouplissement de la politique de sécurité informatique, des règlements ou des normes institutionnelles y afférents.

La demande de dérogation doit être formulée par écrit auprès de la directrice ou du directeur des Services informatiques – Bureau de la sécurité et de la gouvernance, qui sera responsable de coordonner la consultation auprès des intervenantes, intervenants concernés.

6.2 Approbation des dérogations
(résolutions 2005-A-12811, 2013-A-15988, 2014-E-8897 et 2011-A-15037, 2015-A-16761, 2018-A-17787 et 2011-A-15037)

L'approbation des dérogations aux dispositions de la politique de sécurité informatique, des règlements ou des normes institutionnelles y afférents est la responsabilité de la directrice, du directeur des Services informatiques – Bureau de la sécurité et de la gouvernance. Cette approbation sera donnée à la suite de l'étude du dossier par les différents intervenantes et intervenants concernés.

Dans l'éventualité d'un désaccord entre la requérante, le requérant et la directrice, le directeur des Services informatiques – Bureau de la sécurité et de la gouvernance quant à la décision rendue, la requérante, le requérant peut présenter une demande de révision de la décision auprès d'un sous-comité du comité des utilisateurs de l'informatique et des télécommunications, qui pourra, s'il le juge approprié, consulter les intervenantes, intervenants concernés (Services du Vice-rectorat aux systèmes d'information, requérante, requérant, ombudsman, Services du Vice-rectorat à la vie académique dans le cas des personnels enseignants ou Services du Vice-rectorat au développement humain et organisationnel dans le cas des personnels non enseignants etc.).

ARTICLE 7 - RESPONSABILITÉ DE L'UNIVERSITÉ

L'Université est responsable de fournir les ressources nécessaires aux membres de la communauté afin qu'elles, qu'ils puissent assumer leurs responsabilités quant à la sécurité informatique, et ce, dans un cadre de saine gestion des risques pour l'établissement. Cependant, l'Université ne pourra pas être tenue responsable des pertes, dommages, manques à gagner ou inconvénients qui pourraient être causés à une personne ou à une entité à l'occasion ou en conséquence de l'utilisation des actifs informationnels de l'Université ou advenant le cas où elle devrait, pour quelque cause que ce soit, diminuer ses services, ou les interrompre, quelle que soit la durée de telles diminutions ou interruptions.

AMENDEMENTS

Résolutions	Articles
90-A-7239	Règlement complet (en vigueur le 24 avril 1990)
91-A-7583	Féminisation
92-A-8539	2.3, 2.4, 2.5, nouvel article 3, art. 4, 5.2, 5.3
91-A-7583	Féminisation
2005-A-12774	Refonte
2005-A-21811	5.1, 5.4.2, 6.2
2008-A-13724	5.1
2010-A-14543	5.1
2013-A-15988	5.1, 5.4, 6.2
2014-E-8897 et 2011-A-15037	3, 3.2, 4, 5.1, 5.2, 5.3, 5.4, 6.1, 6.2
2015-A-16761	5.1, 5.4, 6.2
2015-A-16988	5.4
2016-E-9223 et 2011-A-15037	3, 3.2, 4, 5, 6
2018-A-17787 et 2011-A-15037	5.1, 5.4, 6.2