UQÀM | Université du Québec à Montréal

Politique no 47
Politique sur la sécurité informatique

Responsable : Vice-rectorat aux systèmes d'information

Cette politique s'adresse à toute la communauté de l'UQAM

Le texte que vous consultez est une codification administrative des Politiques de l'UQAM. Leur version officielle est contenue dans les résolutions adoptées par le Conseil d'administration. La version que vous consultez est celle qui est en vigueur en avril 2020.

Adoptée le 14 juin 2005 : résolution 2005-A-12774
AMENDEMENTS
2011-A-15037
2011-A-15038
2015-A-16761
2018-A-17787
2018-A-17867
2019-A-18146
2019-E-9641
2020-A-18441

TABLE DES MATIÈRES

Préambule

La sécurité informatique en milieu universitaire : contexte et enjeux

Les réseaux et les ordinateurs des universités hébergent et transmettent des informations aussi variées que :

- des informations liées aux activités de recherche, de création et d'enseignement assujetties à la propriété intellectuelle;
- des renseignements personnels sur les étudiantes, étudiants et les membres du personnel;
- des informations de gestion essentielles aux opérations quotidiennes normales des établissements.

Des équipements informatiques universitaires vulnérables ont fréquemment été utilisés afin d'enclencher des attaques informatiques importantes contre d'autres organisations, en plus d'affecter la prestation des services technologiques à l'intérieur même des universités. Le maintien d'un niveau approprié de sécurité pour les actifs informationnels des universités est donc devenu un besoin crucial non seulement pour leur propre bénéfice, mais également pour celui de la collectivité.

Dans ce contexte, les universités doivent appliquer des mesures de sécurité informatique, sans pour autant compromettre le respect des valeurs fondamentales nécessaires au développement du savoir, soit :

- le civisme et l'esprit communautaire;
- la liberté académique;
- la vie privée et la confidentialité;
- l'équité, la diversité et l'accessibilité;
- l'éthique, l'intégrité et la responsabilisation.

Il est donc important que les organismes dont la mission est centrée sur le développement de la société du savoir établissent des principes de sécurité informatique qui leur sont propres en fonction de leur unicité.

La sécurité informatique à l'Université

La présente politique sur la sécurité informatique permet à l'Université de réaffirmer clairement l'intérêt qu'elle porte à cette question et d'énoncer ses objectifs en la matière.

Par cette politique, l'Université fait appel à la responsabilisation personnelle et collective des membres de la communauté universitaire. Chaque membre et chaque unité organisationnelle doivent faire preuve dans l'exécution de leurs tâches d'un réel sens des responsabilités en matière de sécurité informatique, en vue de la protection de la qualité des services informatiques offerts à la communauté, de l'utilisation éthique des actifs informationnels, de l'éducation et de la sensibilisation relatives à la sécurité informatique.

Cette politique s'inscrit dans une perspective de prévention et s'appuie sur la nécessaire collaboration entre les membres de la communauté qui utilisent et gèrent les actifs informationnels de l'Université.

Conséquemment, la politique précise les droits et obligations du personnel, des étudiantes, étudiants, des invitées, invités et de l'Université dans ce domaine et détermine les responsabilités quant à sa mise en œuvre.

1. Cadre juridique

Le cadre juridique de la présente politique est constitué d'une part, par les lois canadiennes et québécoises en vigueur et, d'autre part, par les politiques, règlements et protocoles internes et externes à l'Université, de même que par les principes qui régissent la liberté académique et l'autonomie universitaire ainsi que par les conventions collectives en vigueur à l'Université.

À cet effet, toute utilisatrice, tout utilisateur, tel que défini à la section 5, qui est appelé à utiliser, à gérer, à exploiter ou à traiter les actifs informationnels de l'Université doit respecter la réglementation propre à l'Université, qui comprend :

- le Règlement no 12 sur l'utilisation et la gestion des actifs informationnels;
- le Règlement no 14 relatif à l'emprunt d'équipement informatique et de télécommunications;
- le Règlement no 10 sur la protection des personnes et des biens;

- le Règlement no 15 sur la confidentialité des dossiers nominatifs;
- la Politique no 26 sur l'administration des données institutionnelles;
- la Politique no 36 sur la reconnaissance et la protection de la propriété intellectuelle;
- les conventions collectives et protocoles de travail en vigueur à l'Université.

2. Énoncé de principes

La sécurité informatique peut être vue comme :

- une démarche : elle se définit alors comme la poursuite active des objectifs de confidentialité, d'intégrité et de disponibilité de manière à ce que les actifs informationnels soient utilisables dans des conditions adéquates;
- un objectif : elle se définit alors comme un objectif qui vise à maintenir les conditions adéquates pour que les actifs informationnels soient utilisables, dans le respect des exigences de confidentialité, d'intégrité et de disponibilité;
- un résultat : elle se définit alors comme l'état des actifs informationnels qui sont utilisables dans des conditions adéquates, dans le respect des exigences de confidentialité, d'intégrité et de disponibilité.

La sécurité informatique se rapporte aux actifs informationnels qui sont l'ensemble des données et des équipements nécessaires à l'évolution de l'information tout au long de son cycle de vie, de son acquisition ou de sa création à sa destruction.

La sécurité informatique est une responsabilité institutionnelle et personnelle de sorte que l'atteinte de ces objectifs repose sur la reconnaissance et la mise en œuvre d'un ensemble de droits et responsabilités individuelles qui respectent les principes directeurs suivants :

- le respect des droits des utilisatrices, utilisateurs tels qu'ils sont définis dans la présente politique;
- le respect de l'autonomie du personnel d'enseignement et de recherche dans la gestion des informations créées par le biais des activités d'enseignement de recherche et de création;
- l'amélioration constante des mécanismes administratifs, préventifs et d'intervention pour permettre de poser les actions requises dans les situations mettant en péril la sécurité des actifs informationnels;
- la fiabilité, la qualité et le bon fonctionnement des services qui permettent à l'Université de réaliser sa mission et ses objectifs, dans le respect des droits et libertés des personnes, de la liberté académique, ainsi que des lois et règlements;
- la recherche et la mise en œuvre de moyens afin de protéger le travail des personnes en permettant une utilisation des actifs informationnels dans des conditions optimales;
- la résolution des problèmes de sécurité informatique par une approche « proactive » et préventive plutôt que par une approche réactive;
- la sensibilisation des membres de la communauté, en mettant les moyens nécessaires à leur disposition, à l'importance d'assumer les responsabilités préconisées par la Politique sur la sécurité informatique, et ce, considérant qu'ils sont les principaux artisans de la mise en application efficace d'une telle politique à l'Université.

3. Objectifs

La Politique sur la sécurité informatique vise à atteindre les objectifs suivants dans le respect de la liberté académique, de la vie privée et de la confidentialité des renseignements des membres de la communauté :

- assurer aux membres de la communauté universitaire une utilisation et une gestion sécuritaires, responsables et éthiques des actifs informationnels;
- sensibiliser et orienter chacune, chacun des membres de la communauté quant à ses responsabilités dans la protection des actifs informationnels dont il faut assurer la confidentialité, l'intégrité et la disponibilité.

Tous les membres de la communauté universitaire devront connaître cette politique et agir conformément à leurs responsabilités, telles que définies dans la Politique sur la sécurité informatique, ainsi que dans les règlements et les normes institutionnelles y afférant.

4. Champ d'application

La présente politique s'applique à l'ensemble des personnes employées de l'Université dans les unités académiques et administratives, aux associations, aux syndicats, à toute autre forme de regroupements à l'intérieur de l'Université et aux étudiantes, étudiants tel que définis dans le Règlement no 2 de régie interne. Elle touche également toute personne physique ou morale appelée à utiliser les actifs informationnels de l'Université.

5. Définitions

Aux fins de la présente politique, voici les définitions des termes suivants :

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'information. Les actifs informationnels de l'Université couvrent les équipements, logiciels, systèmes, données ou informations qui lui appartiennent et ceux qui utilisent ou hébergent des actifs dont l'Université est propriétaire, fiduciaire ou dépositaire.

Authentifiant personnel : une caractéristique exclusive, une information unique et confidentielle ou un objet unique détenu par une personne ou par toute autre entité, permettant de vérifier l'identité de cette personne ou entité. Une signature manuscrite, une empreinte digitale, un mot de passe ou un numéro d'identification personnel sont des exemples d'authentifiant.

Confidentialité : une exigence en vertu de laquelle une information est divulguée, traitée et mise à la disposition des seules personnes ou entités autorisées, selon les modalités établies.

Dérogation : une permission exceptionnelle accordée sur demande à une personne ou à une entité, qui la dégage des exigences liées à une responsabilité, à une norme institutionnelle ou à une mesure de sécurité informatique.

Disponibilité : une exigence en vertu de laquelle la propriété d'un actif informationnel est accessible et utilisable par une personne ou par une entité, dans les conditions autorisées.

Droit d'accès : le droit d'utiliser un actif informationnel selon des modalités qui varient en fonction du niveau de privilège accordé.

Évaluation de la sécurité informatique : l'exercice d'analyse des mesures de protection mises en place pour assurer la sécurité informatique des actifs informationnels.

Fiduciaire ou dépositaire : toute personne ou entité responsable de garder ou d'administrer les actifs informationnels d'une tierce partie lui étant liée.

Incident de sécurité informatique : tout événement susceptible de contrevenir aux objectifs et aux normes institutionnelles de sécurité informatique.

Intégrité : une exigence se rapportant aux données ou aux systèmes. L'intégrité des données est une exigence qui veut que l'information et les programmes ne soient modifiés que d'une manière déterminée et autorisée, tandis que l'intégrité des systèmes est une exigence qui veut qu'un système remplisse les tâches auxquelles il est destiné, libre de toute manipulation non autorisée, qu'elle soit délibérée ou commise par inadvertance.

Invitée, invité : ensemble des individus, associations ou organisations utilisant les actifs informationnels de l'Université sur une base régulière ou ponctuelle et n'étant pas assujetti à un lien d'emploi, à un lien d'étude ou à un lien contractuel formel avec l'Université.

Norme institutionnelle de sécurité informatique : ensemble de spécifications en vigueur à l'Université, 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.

Qualité du service : ensemble des caractéristiques d'un actif informationnel qui offre des données ou services sécuritaires (confidentiels, disponibles, intègres), utiles, performants, fiables et conformes aux exigences.

Relève informatique : ensemble des mesures de planification établies et appliquées en vue de rétablir une disponibilité adéquate des actifs informationnels indispensables à la réalisation de certaines activités.

Responsabilité commune : les responsabilités dont toutes les intervenantes, tous les intervenants identifiés dans le cadre de la Politique sur la sécurité informatique doivent minimalement s'acquitter.

Responsable de systèmes : toute unité organisationnelle ou membre de la communauté désigné responsable et imputable de la gestion de certains actifs informationnels de l'Université. Cet actif peut consister en un actif complet ou en une portion (module) de cet actif.

Responsable d'unité académique : toute personne qui, dans le cadre de ses tâches de service à la collectivité, assume un rôle de direction à titre de doyenne, doyen; de vice-doyenne, vice-doyen ou de directrice, directeur des études; à titre de directrice, directeur de département, de module, d'unité de programme(s), d'école, d'institut, de centre institutionnel de recherche ou de création; à titre d'adjointe, adjoint à la directrice, au directeur de département, de module, d'unité de programme(s) de premier cycle, d'école, d'institut; à titre de titulaire de chaire.

Risque : degré d'exposition des actifs informationnels aux menaces, en fonction de la valeur de ces actifs et des mesures en place pour en préserver la sécurité.

Utilisatrice, utilisateur : l'ensemble des personnes employées par l'Université dans les unités académiques et administratives, les associations, les syndicats et toute autre forme de regroupements à l'intérieur de l'Université, les étudiantes, étudiants tel que définis dans le Règlement no 2 de régie interne, ainsi que toute personne physique ou morale appelée à utiliser les actifs informationnels de l'Université ou à traiter l'information appartenant à l'Université ou à une de ses unités.

6. Structure fonctionnelle

Tous les membres de la communauté universitaire ont des droits quant à la sécurité informatique. Ces droits varient en fonction du ou des rôles que chacune, chacun est appelé à jouer dans la vie universitaire, dans l'utilisation et dans la gestion des actifs informationnels.

Ces droits visent à définir, du point de vue de la sécurité informatique uniquement, les attentes légitimes que les membres de la communauté peuvent nourrir à l'égard des services offerts par l'Université et ses représentantes, représentants. Ceux-ci, dans le cadre de la gestion des actifs informationnels, ont donc le devoir de respecter ces droits dans toutes les décisions et actions entreprises.

Les membres de la communauté ont également des responsabilités à l'égard de la sécurité informatique. Le respect de ses responsabilités permettra à chacune, chacun, selon son rôle, de contribuer à différents degrés à la sécurité des actifs informationnels. Ces responsabilités sont attribuées autant aux utilisatrices, utilisateurs, qui par une saine utilisation des actifs informationnels assurent leur sécurité et leur stabilité, qu'aux gestionnaires de ces actifs, qui doivent mettre en place des mécanismes raisonnables pour les protéger dans le respect des droits des utilisatrices, utilisateurs.

L'annexe 1 de la Politique sur la sécurité informatique présente de façon détaillée les droits et responsabilités en fonction des rôles des membres de la communauté et des unités organisationnelles.

7. Procédures découlant de la Politique sur la sécurité informatique

7.1 Sensibilisation, information et formation

L'Université, par l'adoption, la diffusion et la mise en œuvre de la Politique sur la sécurité informatique, amorce la sensibilisation de la communauté aux principes énoncés dans la présente politique.

Toute utilisatrice, tout utilisateur a le droit de recevoir les renseignements nécessaires à la bonne compréhension de ses responsabilités en matière de sécurité informatique. À cet effet, elle, il pourra notamment avoir accès à des documents explicatifs et à des formations.

Les modalités de formation et de communication devront être convenues entre les individus concernés, selon les disponibilités respectives des participantes, participants et les modes de formation jugés les plus efficaces.
Les communications concernant la sécurité informatique pourront être effectuées par le biais de plusieurs canaux de communication selon l'auditoire, l'objet et l'urgence de la communication.

Toute utilisatrice, tout utilisateur est responsable de consulter régulièrement les canaux de communication mis à sa disposition à l'Université : boîte de courriels, boîte vocale, avis imprimés, site Web des services, etc., afin de prendre connaissance des informations pertinentes se rapportant à la sécurité informatique.

Toute utilisatrice, tout utilisateur a le droit de demander au Vice-rectorat aux systèmes d'information ou aux Services informatiques – Architecture et sécurité des explications ou des renseignements supplémentaires quant aux modalités d'utilisation, de gestion et de protection des actifs informationnels. Il peut le faire dans la mesure où les renseignements demandés ne compromettent pas la sécurité même des actifs. À la suite de la réception d'une demande légitime, la, le responsable de systèmes, la directrice, le directeur des Services informatiques – Architecture et sécurité ou sa déléguée, son délégué doit fournir l'information demandée dans les meilleurs délais possibles.

7. 2 Traitement des incidents

7.2.1 Communication et traitement des incidents

Dans le cas d'événements affectant potentiellement la confidentialité, l'intégrité ou la disponibilité d'actifs informationnels, les responsables de systèmes, les responsables des unités administratives et académiques, de même que le reste de la communauté universitaire, doivent informer les Services informatiques afin que ces derniers coordonnent les interventions de sécurité informatique, en concertation avec le Vice-rectorat aux systèmes d'information et les autres vice-rectorats concernés.

Chaque événement rapporté fera ensuite l'objet d'un suivi auprès des services et personnes concernés pour investigation, communication des résultats pertinents et proposition de mesures correctives.

7.2.2 Mesures d'urgence

Si l'événement requiert une intervention d'urgence pour protéger la confidentialité, l'intégrité ou la disponibilité d'actifs informationnels, les Services informatiques peuvent, après avoir pris les moyens raisonnables pour aviser les responsables ou les utilisatrices, utilisateurs des actifs informationnels, poser les actions suivantes :

- interrompre ou révoquer temporairement les services offerts à certaines utilisatrices, certains utilisateurs afin de protéger le reste de la communauté, en tentant le plus possible de ne restreindre l'accès qu'au service qui pose problème;
- intervenir sur un actif informationnel suspecté de contrevenir à la Politique sur la sécurité informatique, aux règlements ou aux lois et, au besoin, demander à la personne l'utilisant de s'identifier;
- appliquer les différentes fonctions de diagnostic sur les actifs informationnels;
- mettre en place les mesures urgentes requises afin de circonscrire la crise.

7.2.3 Sanctions

Dans le cas où des incidents de sécurité informatique résulteraient d'agissements volontaires et malicieux d'une utilisatrice, un utilisateur, l'Université peut appliquer des sanctions selon les modalités prévues aux conventions collectives, au Règlement no 2 de régie interne et au Règlement no 12 sur l'utilisation et la gestion des actifs informationnels.

7.3 Normes institutionnelles de sécurité informatique

7.3.1 Type de normes institutionnelles de sécurité informatique

Deux types de normes institutionnelles de sécurité informatique peuvent être élaborés :

1. Normes prescriptives : normes élaborant des obligations et dont l'application est requise pour les membres de la communauté visés par la norme.

2. Normes recommandées : normes élaborant des meilleures pratiques et dont l'application est optionnelle pour les membres de la communauté visés par la norme.

7.3.2 Élaboration, approbation et réévaluation

L'élaboration et la réévaluation des normes institutionnelle de sécurité informatique sont sous la responsabilité de la directrice, du directeur des Services informatiques – Architecture et sécurité. Dans le cadre de leur élaboration, les responsables de systèmes, les employées, employés du Vice-rectorat aux systèmes d'information et, au besoin, les utilisatrices, utilisateurs peuvent être consultés ou participer à des groupes de travail.

La réévaluation des normes de sécurité informatique est un processus constant en fonction des évolutions technologiques, des dispositions législatives et réglementaires.

Les normes recommandées peuvent être émises sans autre autorisation formelle par la directrice, le directeur des Services informatiques – Architecture et sécurité.

Les normes prescriptives doivent être approuvées par la Direction de l'Université.

7.4 Processus de dérogation

7.4.1 Demande

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 sur la sécurité informatique, des règlements ou des normes institutionnelles y afférents, et juge nécessaire de mettre en place un processus de demande de dérogation.

La demande de dérogation doit être formulée par écrit auprès de la directrice, du directeur de la sécurité informatique, ou de sa déléguée, son délégué.

7.4.2 Approbation des dérogations

L'approbation des dérogations aux dispositions de la Politique sur la sécurité informatique, des règlements ou des normes institutionnelles y afférents est la responsabilité de la directrice, du directeur des Services informatiques – Architecture et sécurité, ou de sa déléguée, son délégué. Cette approbation sera accordée à la suite de l'étude du dossier par les différents intervenantes, intervenants concernés (par exemple : le Vice-rectorat aux systèmes d'information, la directrice, le directeur des Services informatiques – Architecture et sécurité, sa déléguée, son délégué, la requérante, le requérant, la directrice, le directeur du département, le service de la requérante, du requérant, etc.).

Dans l'éventualité d'un désaccord entre la requérante, le requérant et la directrice, le directeur des Services informatiques – Architecture et sécurité ou sa déléguée, son délégué quant à la décision rendue, la requérante, le requérant peut présenter une demande de révision de la décision auprès de la vice-rectrice, du vice-recteur aux Systèmes d'information, qui pourra, s'il le juge approprié, consulter les intervenantes, intervenants concernés (Services informatiques – Architecture et sécurité et autres services sous sa responsabilité, requérante, requérant, protectrice, protecteur universitaire, services liés à la gestion des ressources humaines, etc.).

7.5 Gestion, mise à jour et mise en œuvre de la Politique sur la sécurité informatique

7.5.1 Élaboration et réévaluation

L'élaboration et la réévaluation de la Politique sur la sécurité informatique sont sous la responsabilité du Vice-rectorat aux systèmes d'information, en collaboration avec la directrice, le directeur des Services informatiques – Architecture et sécurité, ou sa déléguée, son délégué.

7.5.2 Adoption

L'approbation de la Politique sur la sécurité informatique et des modifications qui devraient y être apportées relève du Conseil d'administration.

7.5.3 Adhésion

L'implantation et l'efficacité d'une politique de sécurité informatique à l'Université requièrent de la part de toute la communauté le respect des pratiques et procédures de sécurité informatique. Les personnes qui sont appelées à jouer différents rôles au sein de l'Université, conformément aux définitions présentées dans les sections 4 et 5 de la présente politique, s'engagent à assumer les responsabilités relatives aux fonctions qu'ils occupent.

7.5.4 Responsabilité de mise en œuvre

La directrice, le directeur des Services informatiques – Architecture et sécurité, ou sa déléguée, son délégué est responsable de développer les mécanismes de soutien à la diffusion et à la mise à jour de la Politique sur la sécurité informatique.
La mise en œuvre et le respect de la présente politique et des directives ou règlements en découlant incombent à toute la communauté de l'Université.

L'autorité administrative de chaque unité doit sensibiliser son personnel, ses étudiantes, étudiants et autres utilisatrices, utilisateurs des actifs informationnels dont elle est responsable, à l'importance des principes de sécurité entourant leur usage.

8. Responsabilité de l'Université

L'Université est responsable de fournir les ressources nécessaires aux membres de la communauté et aux unités organisationnelles afin qu'ils puissent assumer leurs responsabilités quant à la sécurité informatique, et ce, dans un cadre de saine gestion des risques.

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.

ANNEXE 1 – DROITS ET RESPONSABILITÉS

1. Droits et responsabilités de la communauté

Les droits et les responsabilités de la communauté sont applicables à l'ensemble des utilisatrices, utilisateurs des actifs informationnels de l'Université.

1.1 Droits

Les utilisatrices, utilisateurs des actifs informationnels de l'Université ont un droit d'accès à ces actifs, conforme à leur rôle dans l'établissement, ainsi que de préservation de la confidentialité de leur utilisation, sous réserve d'un manquement à la présente politique.

Les utilisatrices, utilisateurs ont le droit d'avoir accès à des services informatiques fiables et disponibles, dans les limites de la capacité de l'Université à leur fournir.

Les utilisatrices, utilisateurs ont le droit d'être informés, sensibilisés et formés à l'égard de leurs responsabilités et de disposer des moyens, par exemple : des guides, des ressources humaines et financières, etc., nécessaires à leur prise en charge.

L'Université accorde un droit d'utilisation personnelle de ses actifs informationnels dans la mesure où celle-ci est conforme aux modalités décrites au Règlement no 12 sur l'utilisation et la gestion des actifs informationnels.

Dans le cas où une utilisatrice, un utilisateur a besoin d'un accès supérieur aux normes institutionnelles prévues dans le cadre de cette politique, elle, il a le droit d'obtenir un tel accès à la condition qu'il ait été approuvé par les responsables des actifs informationnels utilisés.

Finalement, une utilisatrice, un utilisateur a le droit, si aucune autre mesure palliative n'est disponible, de déléguer de façon restreinte et temporaire certains accès à une tierce partie. Elle, il demeure néanmoins responsable de l'utilisation des accès légitimes effectuée par cette tierce partie. L'octroi et la gestion de ces accès doivent être faits en conformité avec les normes institutionnelles et procédures prévues à cet effet.

1.2 Responsabilités

Les utilisatrices, utilisateurs doivent respecter les directives prescrites dans le cadre de la présente politique et du Règlement no 12 sur l'utilisation et la gestion des actifs informationnels et du Règlement no 14 relatif à l'emprunt d'équipement informatique et de télécommunications, en matière d'utilisation des actifs informationnels :

- en utilisant un authentifiant personnel pour gérer leurs accès aux actifs informationnels de l'Université et en préservant la confidentialité et l'intégrité de cet authentifiant;
- en tenant compte des droits d'accès accordés ainsi que de leurs modalités d'utilisation afin de préserver l'intégrité et la disponibilité des actifs informationnels;
- en respectant les droits d'accès tel que prévu lors de l'octroi;
- en assurant la protection des actifs informationnels sous leur responsabilité;
- en respectant les normes institutionnelles de sécurité informatique;
- en ayant recours aux actifs informationnels de l'Université conformément au cadre législatif auquel l'Université est soumise.

Dans le cas de l'octroi d'un privilège temporaire, l'utilisatrice, utilisateur doit limiter son utilisation des actifs informationnels de l'Université aux modalités prescrites dans le cadre de cette autorisation.

Outre ces responsabilités, les utilisatrices, utilisateurs doivent prendre connaissance des consignes de sécurité informatique qui sont portées à leur attention et agir conformément aux recommandations pertinentes lorsqu'ils utilisent les actifs informationnels.

De plus, les utilisatrices, utilisateurs qui constatent un incident de sécurité informatique doivent informer les Services informatiques afin que ceux-ci puissent coordonner les interventions de sécurité informatique et, dans la limite où cette collaboration ne leur porte pas un préjudice personnel, collaborer avec les services appropriés dans le cadre des exercices d'évaluation de la sécurité informatique et d'investigations d'incidents de sécurité informatique.

2. Droits et responsabilités des étudiantes, étudiants

2.1 Droits

Outre les droits et responsabilités dévolus à toutes, tous les membres de la communauté, les étudiantes, étudiants ont droit à un accès aux actifs informationnels conforme aux activités académiques ou aux activités de vie étudiante qui leur sont offertes en tant qu'étudiante, étudiant inscrit à l'Université.

2.2 Responsabilités

Les étudiantes, étudiants ont le devoir de faire un usage des actifs informationnels qui soit conforme aux vocations de ces actifs, et ce, dans le respect de la présente Politique, ainsi que des règlements et normes institutionnelles de sécurité informatique y afférents.

3. Droits et responsabilités des professeures, professeurs, chargées de cours, chargés de cours, maîtres de langue et autre personnel administratif et de soutien à l'enseignement, à la recherche et à la création

Quoique les corps d'emplois de professeures, professeurs, de chargées de cours, chargés de cours et de maîtres de langue, ci-après appelés le personnel d'enseignement et de recherche, soient distincts sur le plan de leurs rôles et responsabilités à l'Université, ils ont néanmoins, au sens de la sécurité informatique, des droits et responsabilités convergents.

3.1 Droits

Outre les droits et responsabilités accordés à l'ensemble de la communauté, le personnel d'enseignement et de recherche a le droit de faire une utilisation des actifs informationnels qui réponde aux besoins de formation, de recherche et de rayonnement de l'Université.

De plus, le personnel d'enseignement et de recherche a le droit, moyennant l'acceptation de modalités spécifiques d'utilisation et de gestion des actifs informationnels à leur charge, de déléguer certaines responsabilités de sécurité informatique aux Services informatiques – Architecture et sécurité ou à une responsable, un responsable de systèmes.

3.2 Responsabilités

Le personnel d'enseignement et de recherche de l'Université doit respecter la présente politique, les normes institutionnelles de sécurité informatique ainsi que les règlements en matière d'utilisation des actifs informationnels.

Le personnel d'enseignement et de recherche est également responsable, avec le soutien de la directrice, du directeur de la sécurité informatique, ou de sa déléguée, son délégué :

- d'identifier les besoins de sécurité informatique (confidentialité, intégrité et disponibilité) inhérents aux actifs informationnels dont il est responsable ou fiduciaire;
- de communiquer avec les ressources habilitées à lui offrir un soutien dans l'éventualité où il n'a pas la possibilité de mettre en œuvre les mesures de protection nécessaires;
- de participer, en collaboration avec les responsables de systèmes appropriés, au processus d'autorisation et de gestion des accès informatiques conformément aux normes institutionnelles de sécurité informatique et procédures émises par ces derniers;
- de fournir, sur une base volontaire, un soutien aux activités d'identification des besoins de sécurité informatique et aux tests de fonctionnalité dans le cadre des projets technologiques.

4. Droits et responsabilités du personnel administratif et de soutien

4.1 Droits

Outre les droits et responsabilités dévolus à tous les membres de la communauté, le personnel administratif ou de soutien a le droit de faire usage des actifs informationnels qui lui permettent d'exécuter les tâches inhérentes à son poste à l'Université.

De plus, le personnel administratif et de soutien a le droit, avec l'approbation de la supérieure immédiate, du supérieur immédiat et moyennant l'acceptation de modalités spécifiques d'utilisation et de gestion des actifs informationnels à leur charge, de déléguer certaines responsabilités de sécurité informatique aux Services informatiques – Architecture et sécurité ou à une responsable, un responsable de systèmes.

4.2 Responsabilités

Le personnel administratif et de soutien de l'Université doit respecter la présente politique, les normes institutionnelles de sécurité informatique ainsi que les règlements en matière d'utilisation des actifs informationnels.

Il est, de plus, chargé d'assister les cadres ainsi que les responsables d'unités académiques et les responsables de systèmes, avec le soutien de la directrice, du directeur des Services informatiques – Architecture et sécurité, ou de sa déléguée, son délégué :

- en identifiant les besoins de sécurité informatique (confidentialité, intégrité et disponibilité) inhérents aux actifs informationnels dont il est responsable ou fiduciaire;
- en participant au processus d'autorisation et de gestion des accès informatiques conformément aux normes institutionnelles de sécurité informatique et procédures émises par les responsables de systèmes, quand ces derniers leur délèguent la responsabilité

d'autoriser des accès;
- en fournissant, sur une base volontaire ou s'il est assigné à cette tâche par la, le cadre dont il relève, un soutien aux supérieures immédiates, supérieurs immédiats et aux responsables de systèmes dans l'identification des besoins de sécurité informatique et dans la réalisation des tests de fonctionnalité dans le cadre des projets technologiques.

5. Droits et responsabilités de la, du cadre ou de la, du responsable d'unité académique

5.1 Droits

Outre les droits et responsabilités dévolus à toutes, tous les membres de la communauté, une employée, un employé agissant à titre de cadre ou de responsable d'unité académique a également le droit de faire une utilisation des actifs informationnels qui lui permette d'exécuter les tâches propres à sa fonction de direction.

La, le cadre, la, le responsable d'unité académique a le droit d'être informé des incidents touchant l'application de la présente politique dans son unité.

Dans l'un ou l'autre cas, elle, il peut également appliquer des règles de sécurité informatique plus restrictives que celles définies dans les règlements et les normes institutionnelles de sécurité informatique, si elle, il juge que ces restrictions sont requises par la nécessité du service et qu'elles respectent les principes de la Politique sur la sécurité informatique.

De plus, une, un cadre ou une, un responsable d'unité académique a le droit, moyennant l'acceptation de modalités spécifiques d'utilisation et de gestion des actifs informationnels à leur charge, de déléguer certaines responsabilités de sécurité informatique aux Services informatiques – Architecture et sécurité ou à une, un responsable de systèmes.

5.2 Responsabilités

Une, un cadre, une, un responsable d'unité académique s'engage à respecter la présente politique, les normes institutionnelles de sécurité informatique ainsi que les règlements en matière d'utilisation des actifs informationnels.

Plus spécifiquement, une, un cadre, une, un responsable d'unité académique est également responsable, avec le soutien de la directrice, du directeur de la sécurité informatique, ou de sa déléguée, son délégué :

- d'identifier les actifs informationnels dont elle, il est responsable ou fiduciaire et de désigner à la directrice, au directeur de la sécurité informatique, ou à sa déléguée, son délégué une ou un responsable de systèmes;
- de préciser les besoins de sécurité informatique (confidentialité, intégrité et disponibilité) inhérents aux actifs informationnels dont elle, il est responsable ou fiduciaire;
- d'intégrer les besoins de sécurité informatique identifiés à sa planification stratégique lorsque approprié;
- de participer, en collaboration avec les responsables de systèmes concernés, au processus d'autorisation et de gestion des accès informatiques conformément aux normes institutionnelles de sécurité informatique et procédures émises par ces dernières, derniers;

- de fournir un soutien aux activités d'identification des besoins de sécurité informatique, d'approbation des solutions proposées et de réalisation de tests de fonctionnalité dans le cadre des projets technologiques.

Cette personne doit mettre en place les mesures de sécurité préconisées par la présente politique et les règlements et normes institutionnels y afférents. Elle doit sensibiliser le personnel sous sa responsabilité aux différents aspects de la sécurité informatique. Dans l'éventualité où elle n'est pas en mesure de mettre en œuvre les mesures de protection requises, elle doit communiquer avec les ressources habilitées à lui offrir un soutien.

De plus, elle doit collaborer aux investigations en vue de résoudre les problèmes de sécurité informatique ayant pour cible des actifs informationnels de l'Université.

Finalement, cette personne doit, au besoin, donner son appui à la directrice, au directeur de la sécurité informatique, à sa déléguée, son délégué dans l'exercice de vérification de la sécurité informatique des actifs sous sa responsabilité, définir avec elle, lui un plan d'action si des mesures correctives sont nécessaires et superviser sa mise en application.

6. Droits et responsabilités des responsables de systèmes

6.1 Droits

Outre les droits et responsabilités dévolus à toutes, tous les membres de la communauté, les responsables de systèmes ont le droit, au même titre que toutes les autres utilisatrices, tous les autres utilisateurs, de faire usage des actifs informationnels qui leur permettent d'exécuter les tâches inhérentes à leur emploi à l'Université.

De plus, les responsables de systèmes ont le droit, moyennant l'acceptation de modalités spécifiques d'utilisation et de gestion des actifs informationnels sous leur responsabilité, de déléguer certaines responsabilités de sécurité informatique aux Services informatiques – Architecture et sécurité.

6.2 Responsabilités

Les responsables de systèmes de l'Université s'engagent à respecter la présente politique, les normes institutionnelles de sécurité informatique ainsi que les règlements en matière d'utilisation des actifs informationnels.

Ces personnes sont également responsables, avec le soutien de la directrice, du directeur des Services informatiques – Architecture et sécurité, ou de sa déléguée, son délégué :

- d'identifier les actifs informationnels dont elles sont responsables ou fiduciaires;
- de définir les besoins de sécurité informatique (confidentialité, intégrité et disponibilité) inhérents aux actifs informationnels dont elles sont responsables ou fiduciaires;
- de mettre en place les mesures de protection nécessaires et, dans l'éventualité où elles ne disposent pas des moyens pour les mettre en œuvre, de communiquer avec les ressources habilitées à leur offrir un soutien à cet effet;
- d'intégrer les besoins de sécurité informatique identifiés à leur planification stratégique lorsque approprié;

- d'élaborer, de tester et de maintenir à jour les procédures inhérentes à la planification de la relève informatique des équipements dont elles ont la responsabilité et de coordonner ces activités avec les services concernés;
- d'élaborer et de coordonner des procédures d'autorisation et de gestion des accès informatiques conformes aux normes institutionnelles de sécurité informatique;
- d'informer et de former le personnel chargé d'appliquer les procédures;
- de collaborer avec la directrice, le directeur de la sécurité informatique, ou sa déléguée, son délégué afin d'établir les normes institutionnelles de sécurité informatique et mécanismes de protection nécessaires à la sécurité des actifs informationnels dont elles sont responsables et d'appliquer ces normes institutionnelles de sécurité informatique et ces mécanismes;
- d'assurer la continuité des activités informatiques grâce à une surveillance régulière des actifs informationnels dont elles sont responsables;
- de fournir un soutien aux activités d'identification des besoins de sécurité informatique, d'approbation des solutions proposées et de réalisation de tests de fonctionnalité dans le cadre des projets technologiques;
- d'encadrer, dans la mesure où les projets de développement informatique sont sous leur responsabilité, le processus de gestion de projet, de manière à ce que les besoins de sécurité informatique soient intégrés dans son élaboration même, à ce que la directrice, le directeur des Services informatiques – Architecture et sécurité, ou sa déléguée, son délégué donne son approbation à la solution proposée, à ce que des tests des caractéristiques de sécurité soient effectués et à ce que la mise en place des modifications aux systèmes respecte les normes institutionnelles et procédures de sécurité informatique.

Les responsables de systèmes doivent sensibiliser les utilisatrices, utilisateurs qu'elles, ils soutiennent aux différents aspects de la sécurité informatique.

De plus, elles, ils doivent collaborer aux investigations pour résoudre les problèmes de sécurité informatique ayant pour cible des actifs informationnels de l'Université.

Finalement, elles, ils doivent, au besoin, donner leur appui à la directrice, au directeur des Services informatiques – Architecture et sécurité, ou à sa déléguée, son délégué dans l'exercice de vérification de la sécurité informatique des actifs sous leur responsabilité, définir avec elle, lui un plan d'action si des mesures correctives sont nécessaires et superviser sa mise en application.

7. Droits et responsabilités de la directrice, du directeur du Service de la prévention et de la sécurité

7.1 Droits

Dans le cadre de sa mission fondamentale de prévention et de protection des personnes et des biens, la directrice, le directeur du Service de la prévention et de la sécurité a un droit d'utilisation prioritaire des systèmes informatiques essentiels à la préservation immédiate de la sécurité des personnes et des biens.

De plus, la directrice, le directeur du Service de la prévention et de la sécurité a le droit d'être informé des incidents de sécurité informatique se rapportant aux personnes, aux biens ou aux équipements, étant donné l'impact qu'ils ont sur l'atteinte même de sa mission de préservation de la sécurité des personnes et des biens.

7.2 Responsabilités

La directrice, le directeur du Service de la prévention et de la sécurité doit coordonner les tâches suivantes :

- planifier et coordonner avec la directrice, le directeur des Services informatiques – Architecture et sécurité, ou sa déléguée, son délégué la gestion de crises informatiques et assurer la continuité des services tout en veillant à la sécurité des personnes et des biens;
- fournir un soutien aux Services informatiques – Architecture et sécurité dans le cadre des enquêtes de sécurité informatique et coordonner les interventions d'organismes externes responsables de la protection publique;
- assister les responsables de systèmes dans le choix et la mise en œuvre des mesures de protection nécessaires pour assurer la sécurité physique des actifs informationnels.

8. Droits et responsabilités du personnel du Vice-rectorat aux systèmes d'information

8.1 Droits

Dans le cadre de sa mission fondamentale de prestation de services informatiques, le Vice-rectorat aux systèmes d'information a le droit de prendre les mesures nécessaires pour protéger les actifs informationnels sous sa responsabilité. Dans un contexte de mesures d'urgence ou de plaintes, il a également un droit de circonscrire l'accès à tout actif informationnel qui peut avoir une incidence sur la prestation des services qu'il soutient.

Le Vice-rectorat aux systèmes d'information a le droit de procéder à toutes les vérifications d'usage qu'il estime nécessaires pour s'assurer du respect des dispositions de cette politique ou des modalités d'utilisation prescrites lors de l'autorisation de l'accès aux actifs informationnels.

8.2 Responsabilités

Le Vice-rectorat aux systèmes d'information, en tant qu'unité organisationnelle, a la responsabilité de fournir à ses employées, employés, dans la limite des ressources qui lui sont octroyées, les moyens nécessaires à la réalisation de leurs tâches de protection des actifs informationnels et de coordonner leur travail dans le cadre de la réalisation de ces tâches.

Le personnel du Vice-rectorat aux systèmes d'information, outre ses responsabilités à titre d'employée de soutien, employé de soutien, de supérieure immédiate, supérieur immédiat ou d'utilisatrice, utilisateur des actifs informationnels, a certaines responsabilités spécifiques découlant de la mission du Vice-rectorat aux systèmes d'information en matière de prestation de services informatiques et de télécommunications. Ainsi, ce dernier doit offrir ou soutenir les activités suivantes, tout en s'assurant que la communauté soit mise au courant et, au besoin, formée :

- identifier les actifs informationnels dont il est responsable ou fiduciaire et désigner une, un responsable de systèmes en mesure de répondre à la directrice, au directeur de la sécurité informatique, ou à sa déléguée, son délégué;
- évaluer les risques et besoins en matière de sécurité informatique (confidentialité, intégrité et disponibilité) inhérents aux actifs informationnels dont il est responsable ou fiduciaire;

- mettre en place les mesures de protection nécessaires et, dans l'éventualité où il ne dispose pas des moyens pour les mettre en œuvre, communiquer avec les ressources habilitées à offrir un soutien à cet effet;
- intégrer dans sa planification stratégique les besoins de sécurité informatique déjà identifiés, tant dans ses propres projets que dans ceux évalués pour des tiers;
- assurer la continuité de service des actifs informationnels sous sa responsabilité en mettant en place des mesures de protection préventives ainsi que des procédures d'urgence en cas d'incidents;
- préserver la pérennité des actifs informationnels les plus importants en offrant aux responsables de systèmes certaines modalités de service de copies de sauvegarde;
- consolider la sécurité des actifs informationnels en définissant des procédures d'autorisation, de gestion et de contrôle des accès;
- collaborer avec la directrice, le directeur de la sécurité informatique, ou sa déléguée, son délégué, au développement des normes institutionnelles de sécurité informatique et mécanismes de protection nécessaires à la sécurité des systèmes et voir à leur application;
- participer au processus de gestion des dérogations aux normes institutionnelles de sécurité informatique établies;
- collaborer à l'investigation et au traitement des incidents ou problèmes de sécurité informatique;
- encadrer les projets technologiques dont il a la charge, de manière à ce que les besoins de sécurité informatique soient intégrés dans leur élaboration même et à ce que la solution proposée soit approuvée; veiller également à ce que des tests de caractéristiques de sécurité soient effectués et à ce que la mise en place des modifications aux systèmes soit sécuritaire;
- assurer la continuité des activités informatiques en procédant à une surveillance régulière : continuité des opérations, incidents de sécurité, niveau de service, etc., des actifs informationnels dont le service est responsable.

8.3 Désignation de la, du Responsable de la sécurité informationnelle (RSI)

La vice-rectrice, le vice-recteur aux Systèmes d'information agit à titre de Responsable de la sécurité informationnelle de l'Université (RSI) au sens de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement [RLRQ, c. G-1.03 (LGGRI)] et de la Directive sur la sécurité de l'information gouvernementale (DSIG). À ce titre, la, le Responsable de la sécurité informationnelle a pour responsabilités de :

- conseiller la Direction sur les orientations stratégiques en sécurité informatique;
- assurer la coordination et la cohérence des actions de sécurité informatique menées au sein de l'Institution par toutes les intervenantes, tous les intervenants;
- coordonner la mise en œuvre des processus;
- communiquer dans l'Institution les orientations et les priorités d'intervention gouvernementales en matière de sécurité informatique et celles émanant du Ministère;
- soumettre à la Direction, minimalement de façon biennale, la politique, les directives, les cadres de gestion, les priorités d'action, les éléments de reddition de comptes incluant le bilan des réalisations ainsi que tout événement ayant mis ou qui aurait pu mettre en péril la sécurité informatique;
- soumettre annuellement à la Direction la déclaration des risques à portée gouvernementale (RPG);
- établir des liens avec les autres responsables de la sécurité informationnelle.

9. Droits et responsabilités de la directrice, du directeur des Services informatiques – Architecture et sécurité , ou de sa déléguée, son délégué

Le mandat de la directrice, du directeur des Services informatiques – Architecture et sécurité ou de sa déléguée, son délégué consiste à :

- assurer aux membres de la communauté universitaire une utilisation et une gestion sécuritaires, responsables et éthiques des actifs informationnels;
- sensibiliser et orienter chacune, chacun des membres de la communauté quant à ses responsabilités dans la protection des actifs informationnels dont il faut assurer la confidentialité, l'intégrité et la disponibilité.

9.1 Droits

La directrice, le directeur des Services informatiques – Architecture et sécurité, ou sa déléguée, son délégué, outre ses droits à titre de membre du personnel du Vice-rectorat aux systèmes d'information, peut procéder à une évaluation des risques informatiques d'un système de l'Université et formuler des recommandations aux membres de la communauté quant aux meilleures pratiques de protection des actifs informationnels.

La directrice, le directeur des Services informatiques – Architecture et sécurité, ou sa déléguée, son délégué peut, de sa propre initiative ou par mandat, procéder au contrôle de la conformité des actifs informationnels et des procédures appliquées avec les normes institutionnelles de sécurité informatique en vigueur, tel que prévu à l'article 6.1 du Règlement no 12 sur l'utilisation et la gestion des actifs informationnels dans le but d'informer la, le responsable des risques encourus par ses actifs.

Elle, il est également habilité à investiguer dans les cas d'incidents de sécurité informatique, à coordonner la résolution des problèmes et la stratégie de communication, ainsi qu'à représenter la Direction de l'Université dans le cadre des activités courantes se rapportant à la sécurité informatique, tout en respectant les mandats propres aux services liés à la gestion des ressources humaines, au Bureau des relations de travail, au Service de la prévention et de la sécurité, au Service des affaires juridiques et au Service des communications.

Outre ces droits spécifiques, la directrice, le directeur des Services informatiques – Architecture et sécurité, ou sa déléguée, son délégué a les droits nécessaires à l'exercice des responsabilités qui lui sont attribuées dans le cadre de la protection des actifs informationnels.

9.2 Responsabilités

Outre les responsabilités à titre de membre du personnel du Vice-rectorat aux systèmes d'information, la directrice, le directeur des Services informatiques – Architecture et sécurité, ou sa déléguée, son délégué a notamment les responsabilités spécifiques suivantes découlant de son poste :

- mettre en œuvre des mécanismes de sensibilisation, d'information et de formation (groupes d'intérêts, comités, etc.) visant à assurer une meilleure diffusion des enjeux et des connaissances se rapportant à la protection des actifs informationnels;
- consolider l'inventaire des actifs informationnels communiqué par les responsables des systèmes;
- soutenir le personnel d'enseignement et de recherche, les cadres, les responsables d'unités académiques, les responsables de systèmes et le Vice-rectorat aux systèmes d'information dans l'évaluation des risques technologiques et des besoins de sécurité informatique inhérents aux actifs informationnels de l'Université;
- intégrer les résultats de l'analyse de risques dans la planification stratégique de la sécurité informatique;
- assurer une veille stratégique des vulnérabilités et opportunités d'amélioration de la sécurité informatique;
- protéger les actifs informationnels de l'Université en définissant des politiques, normes institutionnelles de sécurité informatique, procédures et règlements relatifs à la sécurité informatique et en vérifiant la conformité des pratiques avec ces règles;
- développer, mettre à jour et diffuser des programmes de sensibilisation et de formation à l'égard de la sécurité informatique;
- coordonner les équipes d'interventions ponctuelles requises en cas de crise de sécurité informatique;
- investiguer dans les cas d'incidents de sécurité informatique qui lui sont rapportés et coordonner la résolution des problèmes et la communication avec les services concernés;
- participer aux différents projets technologiques afin d'harmoniser les aspects de sécurité informatique;
- coordonner le processus de dérogation à la Politique sur la sécurité informatique, ainsi qu'aux normes institutionnelles et aux règlements y afférant;
- agit à titre de coordonnatrice sectorielle, coordonnateur sectoriel de la gestion des incidents (CSGI) au sens de la Loi sur la gouvernance et la gestion des ressources informationnelles des organismes publics et des entreprises du gouvernement, [RLRQ, c. G-1.03 (LGGRI)] et de la Directive sur la sécurité de l'information gouvernementale (DSIG). La coordonnatrice sectorielle, le coordonnateur sectoriel (CSGI) apporte son soutien à la, au Responsable de la sécurité de l'information (RSI) au niveau tactique, notamment en ce qui a trait à la mise en œuvre des mesures d'atténuation des risques et à la mise en place des processus officiels de la sécurité de l'information.

10. Droits et responsabilités de la Direction de l'Université

10.1 Droits

À titre de responsable de la gestion courante, la Direction de l'Université a le droit d'intervenir dans la gestion de la Politique sur la sécurité informatique et d'en demander une révision au moment où elle le juge opportun, et ce, par l'entremise du Vice-rectorat aux systèmes d'information, à titre de responsable de la sécurité informatique des actifs informationnels sous sa charge.

La Direction de l'Université a également le droit de mandater les services appropriés pour mettre en place ou renforcer les mesures de sécurité informatique prescrites dans le cadre de la Politique sur la sécurité informatique ou pour en évaluer le respect par la communauté.

La Direction de l'Université possède également un droit de regard sur l'état de conformité de la protection des actifs informationnels de l'établissement avec la Politique sur la sécurité informatique, les règlements et les normes institutionnels y afférents.

10.2 Responsabilités

La Direction de l'Université a, en ce qui a trait à la sécurité informatique, les devoirs spécifiques suivants :

- approuver les évaluations de risques qui lui sont soumises ainsi que les plans d'action s'y rattachant;
- fournir un soutien formel aux mesures proposées de sécurité informatique qu'elle approuve;
- statuer, à la suite des recommandations des intervenantes, intervenants concernés, sur les demandes de dérogation aux politiques, normes institutionnelles et règlements qui font l'objet d'un litige aux instances inférieures;
- approuver et revoir, au besoin, la Politique sur la sécurité informatique, les règlements et les normes institutionnelles de sécurité informatique prescriptives s'y rattachant.

11. Droits et responsabilités des invitées, invités

11.1 Droits

Outre les droits et responsabilités dévolus à tous les membres de la communauté, les invitées, invités de l'Université ont droit d'avoir accès aux actifs informationnels nécessaires à l'atteinte de l'objectif de leur visite à l'Université, sous réserve de certaines restrictions (modalités d'accès, droits de licence, etc.).

11.2 Responsabilités

Les invitées, invités s'engagent à respecter la présente politique, les normes institutionnelles de sécurité informatique ainsi que les règlements en matière d'utilisation des actifs informationnels. À cet égard, elles, ils s'engagent notamment à assumer les responsabilités communes décrites au paragraphe 6.1.2 applicables à l'accès accordé dans le cadre de leur visite à l'Université.
Dans le cas où le besoin d'accès aux services dépasse les accès généralement accordés aux invitées, invités, il est possible de faire une demande d'autorisation d'accès afin d'obtenir la connexion requise.