GESTION COURANTE Numéro **:** 40.28 Page 1 de 7

POLITIQUE DE SÉCURITÉ INFORMATIQUE ET D'UTILISATION DES RESSOURCES INFORMATIQUES DE L'UNIVERSITÉ DE MONTRÉAL

Adoption
Date : 2005-01-11
Délibération : E-965-12

Modifications
Date :
Délibération :
Article(s) :

TABLE DES MATIÈRES

1. Préambule 1
2. Objectifs 2
3. Définitions 2
4. Champ d'application 3
5. Dispositions générales de sécurité informatique 3
6. Règles d'utilisation des ressources informatiques de l'Université 4
7. Rôles et responsabilités 5
8. Non-respect de la politique 7
Annexe 7

1. PRÉAMBULE

La présente politique porte sur la sécurité du réseau informatique de l'Université de Montréal, des équipements informatiques appartenant à l'Université, de tous les équipements informatiques qui utilisent son réseau, ainsi que des données qui y résident ou y transitent. Elle établit des principes pour l'élaboration de règles de sécurité et un cadre pour l'application de ces règles. La politique de sécurité informatique vient en appui à la réalisation de la mission de l'Université.

La réalisation de cette mission requiert le respect de la liberté académique et de la liberté d'expression. L'Université s'abstient donc de toute intervention dans les contenus, sous réserve des situations exceptionnelles prévues, le cas échéant, par la loi, la présente politique, ou autres règles en vigueur à l'Université. L'Université s'attend à ce que les usagers exercent leurs droits et libertés dans le plus grand respect de tous et dans le respect de leurs obligations à l'endroit de l'Université.

La présente politique énonce également les règles d'utilisation des ressources informatiques de l'Université.

La détermination du degré de confidentialité de l'information ne relève pas de la présente politique.

2. OBJECTIFS

- Contribuer à l'atteinte de la meilleure disponibilité possible des ressources informatiques et des données.
- Améliorer la protection des données en fonction du degré de confidentialité de l'information.
- Assurer, dans la mesure du possible, l'intégrité des données qui résident sur les équipements informatiques ou circulent sur le réseau.
- Éviter que les ressources informatiques de l'Université ne soient l'instrument de perturbations de systèmes informatiques externes.
- Encadrer les mesures de protection, de contrôle et de rétablissement du service.

3. DÉFINITIONS

Authentifiants : l'information unique et confidentielle détenue par une personne, qui permet de s'assurer de son identité, comme les mots de passe, certificats, cartes et autres mécanismes.

Données : l'information numérique produite ou acquise dans le cadre des activités universitaires.

Équipement informatique : l'équipement informatique comprend les ordinateurs, serveurs, imprimantes, assistants électroniques et équipements de même nature, ainsi que les logiciels.

Équipement de télécommunication : l'ensemble des équipements et logiciels de télécommunication, tels les commutateurs, routeurs, émetteurs/récepteurs sans fil, permettant aux équipements informatiques sur le réseau de l'Université de communiquer entre eux et avec les équipements informatiques d'autres réseaux.

Fournisseur : toute personne ou entreprise extérieure à l'Université qui a la charge de ressources informatiques ou qui réalise un ou des mandats de consultant.

Règles de sécurité : l'ensemble des règles découlant de la Politique de sécurité telles qu'établies par le Directeur de la sécurité informatique et approuvées par le vice-recteur responsable des TIC.

Réseau de l'Université : les équipements de télécommunication et le câblage qui sont installés dans les bâtiments et sur les terrains qui sont sous la juridiction de l'Université.

Responsable administratif : le doyen, le directeur ou tout autre responsable d'une unité, ainsi que le professeur ou le chercheur responsable d'une recherche qui fait usage des ressources informatiques de l'Université.

Responsable de ressources informatiques : toute personne qui de par sa fonction a la responsabilité de ressources informatiques.

Ressources informatiques : l'équipement informatique et le réseau de l'Université.

Usager : toute personne qui utilise les ressources informatiques de l'Université, à l'exception des abonnés du service fourni aux locataires des résidences de l'Université de Montréal.

4. CHAMP D'APPLICATION

Cette politique s'applique aux usagers, à l'exception des abonnés du service Internet fourni aux locataires des résidences de l'Université de Montréal. Elle s'applique également aux fournisseurs de l'Université.

5. DISPOSITIONS GÉNÉRALES DE SÉCURITÉ INFORMATIQUE

1. L'usager ne doit pas nuire au fonctionnement des ressources informatiques de l'Université.

2. Il est nécessaire de s'authentifier pour accéder aux ressources informatiques à accès contrôlé.

3. L'usager ne peut pas :

   a. dévoiler ses authentifiants; acquérir, utiliser ou dévoiler ceux d'un autre usager ou d'une ressource informatique;

   b. utiliser des privilèges auxquels il n'a pas droit, même si cela est techniquement possible;

   c. contourner ou modifier le fonctionnement des systèmes d'authentification ou de contrôle d'accès aux ressources informatiques.

4. Le réseau de l'Université est un réseau privé, distinct de l'Internet. Il est protégé par l'application des règles de sécurité en vigueur dans l'établissement.

5. Toute modification au réseau de l'Université, notamment l'ajout d'équipement de réseau et l'interconnexion avec d'autres réseaux, requiert l'accord explicite de la Direction générale des technologies de l'information et de la communication (DGTIC).

6. Les équipements informatiques doivent être conformes aux règles de sécurité en vigueur. L'accès des équipements informatiques au réseau de l'Université est accordé en fonction de la conformité à ces règles.

7. L'usager doit prendre les mesures nécessaires pour protéger les données en sa possession en fonction de leur degré de confidentialité. L'usager ne doit pas altérer ou détruire des données sans l'accord de celui ou ceux qui en ont la responsabilité.

8. L'usager ne doit pas tenter d'accéder à des données sans autorisation, ni d'intercepter des communications notamment le courriel.[1]

9. À l'exception des situations prévues à l'article 10, le responsable de ressources informatiques ne peut accéder aux données d'un usager que sous réserve d'une autorisation préalable des autorités compétentes et selon les règles de l'Université. Dans tous les cas, ces interventions et leurs motifs sont consignés.

10. Dans le cas de menace immédiate à la sécurité des ressources informatiques, le responsable de ressources informatiques peut prendre sans délai les mesures nécessaires de protection, de contrôle et de rétablissement du service. Il doit en informer le Bureau de la sécurité informatique dans les plus brefs délais et informer les usagers concernés des mesures prises.

11. Lorsque la gestion de ressources informatiques exige qu'une surveillance de leur utilisation impliquant l'accumulation de données personnelles soit exercée, les usagers en sont informés à l'avance.

6. RÈGLES D'UTILISATION DES RESSOURCES INFORMATIQUES DE L'UNIVERSITÉ

1. L'utilisation des ressources informatiques doit être essentiellement dédiée à la réalisation de la mission de l'Université. Ainsi, ces ressources informatiques ne doivent pas être utilisées par l'usager pour un usage personnel, pour des activités commerciales, de publicité ou de sollicitation.

[1] L'usager doit savoir que le courriel n'offre aucune garantie de confidentialité ni d'intégrité des données ou documents qui transitent par ce medium. Voir également la *Directive relative à l'utilisation du courrier électronique* de la Division des archives du Secrétariat général.

2. L'usager doit utiliser les ressources informatiques avec circonspection. L'Université peut aviser l'usager que son utilisation des ressources informatiques est abusive dans le contexte de leur partage équitable et voir à ce que la situation soit corrigée.

3. L'usager ne peut :

   a. enfreindre les droits de propriété intellectuelle appartenant à autrui. Sans limiter la généralité de ce qui précède, tous usages non autorisés d'œuvres protégées par droit d'auteur, tels des logiciels, des fichiers numériques et autres, sont interdits;

   b. véhiculer ou exposer son entourage à des contenus à caractère obscène ou pornographique avec l'aide des ressources informatiques;

   c. tenir des propos haineux ou utiliser les ressources informatiques à des fins de harcèlement, de menace, de diffamation ou de tout acte réprimé par la réglementation de l'Université ou par les lois et les règlements.

   Cette règle est complétée par la *Directive relative à la diffusion de contenus sur le réseau Internet* (Annexe).

4. L'usager ne peut faire l'envoi de courriels non sollicités, appelés communément pourriels, particulièrement en lot.

5. L'Université n'assume aucune responsabilité, directe ou indirecte, quant aux dommages, pertes, manques à gagner ou inconvénients qui pourraient découler de l'utilisation, de l'interruption ou de l'arrêt définitif des ressources informatiques.

7. RÔLES ET RESPONSABILITÉS

1. **Usager** : chaque usager a la responsabilité de se conformer à la présente politique et aux règles qui en découlent. Il ne doit pas atténuer ou contourner les mesures de sécurité qui s'appliquent sur les ressources informatiques qu'il utilise.

   L'usager d'un équipement informatique n'appartenant pas à l'Université (étudiant, fournisseur ou autre) est responsable de la sécurité de cet équipement. Il doit s'assurer qu'il est configuré selon les règles de sécurité de l'Université.

2. **Responsable administratif** : le responsable administratif a la responsabilité de voir au respect de la présente politique pour le personnel et les activités qui relèvent de lui, pour les fournisseurs de services informatiques avec qui l'unité fait affaires, ainsi que pour les étudiants, les invités et les autres usagers qu'il parraine.

3. **Responsable de ressources informatiques** : le responsable de ressources informatiques doit s'assurer que la présente politique est appliquée et que les ressources informatiques dont il a la charge soient conformes aux règles de sécurité de l'établissement ainsi qu'aux meilleures pratiques de sécurité.

   Le responsable de ressources informatiques doit conseiller le responsable administratif sur les questions de sécurité informatique et s'assurer qu'il est informé des problématiques de sécurité reliées au fonctionnement de son unité. Il doit aussi assurer les communications avec le Bureau de la sécurité informatique, notamment avec le Directeur de la sécurité informatique et l'officier de sécurité informatique. Il doit enfin collaborer aux mesures décidées par ces personnes en réponse aux évènements de sécurité informatique.

4. **Directeur de la sécurité informatique** : sous l'autorité du vice-recteur responsable des technologies de l'information et de la communication (TIC), le directeur de la sécurité informatique de l'Université est responsable de la gestion de la présente politique et des règles qui en découlent. Ses responsabilités comportent notamment :

   - l'élaboration des règles de sécurité pour adoption;
   - le suivi et la gestion des événements de sécurité informatique d'importance, notamment l'organisation et la coordination des actions nécessaires au contrôle de l'événement ainsi qu'au rétablissement du bon fonctionnement des ressources informatiques;
   - l'analyse post-mortem de ces événements;
   - l'analyse des besoins de sécurité informatique de l'Université, afin d'élaborer des plans de gestion de la sécurité, tenant compte de l'évolution des meilleures pratiques en ce domaine;
   - la diffusion aux membres de la communauté universitaire de la présente politique, des règles de sécurité qui en découlent et des meilleures pratiques de sécurité informatique;
   - le soutien aux divers intervenants, dont les Responsables de ressources informatiques, dans l'acquittement de leurs responsabilités ayant trait à la sécurité informatique.

5. La présente politique relève du vice-recteur responsable des TIC.

6. Un Comité sur la sécurité informatique formé par le vice-recteur responsable des TIC le conseille sur l'évolution de la politique et des règles de sécurité qui en découlent ainsi que sur les règles d'utilisation des ressources informatiques de l'Université.

8. NON-RESPECT DE LA POLITIQUE

Si l'usager contrevient à la présente politique, l'Université pourra lui retirer le droit d'utiliser les ressources informatiques sans délai, sous réserve des autres sanctions applicables.

ANNEXE

Directive relative à la diffusion de contenus sur le réseau Internet