UQÀM | Université du Québec à Montréal

Directive sur l’administration des systèmes d’information

Dernière mise à jour
18 juin 2026

Responsable de l’application	Vice-rectrice, vice-recteur aux Systèmes d’information
Autorité compétente	Vice-rectrice, vice-recteur aux Systèmes d’information
Signature	Louis-Sébastien Guimond Signé avec ConsignO Cloud (25/06/2026) Vérifiez avec verifio.com ou Adobe Reader. UQÀM
Date d’approbation	18 juin 2026
Date d’entrée en vigueur	18 juin 2026
Date de la dernière modification	

Table des matières

1. Objet

Cette directive traite de l'administration des systèmes d'information de l'Université du Québec à Montréal (ci-après « l'Université »). Elle établit les règles et les contrôles à appliquer pour une gestion sécurisée de ces systèmes et des équipements avec lesquels ils communiquent.

2. Champ d'application

La présente directive concerne tous les systèmes d'information détenus par l'Université et s'applique à toute la communauté universitaire ainsi qu'aux personnes physiques et morales externes détenant un système d'information pour l'Université. Pour plus de clarté, toute personne appelée à utiliser, gérer, exploiter ou traiter les systèmes d'information de l'Université doit respecter la présente directive.

3. Cadre juridique

Cette directive est élaborée en tenant compte notamment du cadre juridique suivant :

a) Politique n^{o} 47 sur la sécurité de l'information.

4. Définitions

Aux fins de la présente directive, les termes suivants se définissent comme suit :

a) personne administratrice d'un système d'information : toute personne qui configure, gère techniquement un système d'information et en assure la maintenance, en tout ou en partie;

b) adresse IP : numéro constitué de quatre nombres entiers séparés par des points, qui identifie de façon unique un système d'information connecté au réseau et en permet la localisation et l'identification;

c) journalisation : enregistrement chronologique, dans un fichier ou une base de données, des opérations effectuées dans un système d'information, un programme ou un fichier;

d) serveur : système d'information qui fournit des services, des données ou des ressources à d'autres systèmes d'information contrôlés par des personnes utilisatrices sur le réseau;

e) système d'exploitation : logiciel faisant office d'interface entre les composants informatiques et l'utilisatrice, utilisateur, qui assure notamment l'exécution des programmes, l'allocation des ressources matérielles et le contrôle des opérations d'entrée-sortie sur les périphériques;

f) test d'intrusion : test visant à reproduire de manière contrôlée les conditions réelles d'une attaque sur un réseau ou un système d'information afin de détecter les failles de sécurité et d'évaluer leur exploitabilité en vue de les corriger;

g) topologie de réseau informatique : disposition physique ou logique des nœuds et des raccordements dans un réseau. La topologie physique du réseau définit l'emplacement des nœuds et leurs interconnexions; la topologie logique décrit la manière dont les données sont transférées entre les nœuds. Ces nœuds comprennent des équipements tels que des commutateurs et des serveurs.

5. Acquisition des systèmes d'information

L'acquisition de systèmes d'information doit se faire conformément à la Politique nº 15 d'approvisionnement responsable. L'unité requérante doit s'assurer de se conformer aux exigences de sécurité et d'obtenir les autorisations internes nécessaires et préalables à toute démarche d'acquisition d'un système d'information.

6. Développement des systèmes d'information

Le développement d'un nouveau système d'information de l'Université doit se faire en respectant la Norme sur le développement des systèmes d'information qui assure, au minimum :

a) le respect des exigences de sécurité établies et de la législation en place, dont la Loi sur la gouvernance et la gestion des ressources informationnelles (LGGRI);
b) la soumission de l'application à une analyse de vulnérabilités en utilisant un outil approuvé;
c) l'obtention d'un plan de remédiation des vulnérabilités avant la mise en production.

L'unité requérante doit s'assurer de se conformer aux exigences de sécurité et d'obtenir les autorisations internes nécessaires et préalables à toute démarche de développement et de mise en production d'un nouveau système d'information.

7. Classification des systèmes d'information

Tout système d'information doit être classifié en fonction de sa valeur et de son importance pour l'Université, en respectant la Norme sur la classification des serveurs institutionnels et autres systèmes d'information.

La direction de la sécurité de l'information aux Services informatiques est responsable de la classification des systèmes d'information.

8. Documentation des systèmes d'information

Tout système d'information doit être documenté dans l'inventaire des systèmes d'information de l'Université, en identifiant, au minimum :

a) le nom du système d'information;
b) l'administratrice, administrateur du système d'information;

c) le type d'utilisation (développement, test, production);
d) la classification de sécurité des informations stockées et traitées;
e) l'adresse IP, s'il y a lieu;
f) le système d'exploitation et sa version, s'il y a lieu;
g) la portée du système d'information.

Toute modification de statut d'un système d'information doit automatiquement entraîner celle des informations relatives à ce système dans l'inventaire des systèmes d'information de l'Université par les personnes qui en sont responsables. Dans le cas où la personne responsable du système d'information n'a pas accès à cet inventaire, elle doit aviser les Services informatiques de toute modification afin que ces derniers mettent à jour ledit inventaire.

9. Retrait des systèmes d'information

Le retrait de systèmes d'information doit se faire en respectant la Norme sur le retrait des systèmes d'information qui assure, au minimum, de :

a) retirer le système d'information de l'inventaire;
b) supprimer ou migrer toutes les données du système d'information;
c) modifier toutes les règles de pare-feu relatives au système d'information;
d) libérer l'adresse IP et le nom du système dans les systèmes de contrôle, s'il y a lieu.

10. Configurations minimales de sécurité

10.1 Postes de travail, serveurs et équipements de télécommunication

Tout appareil, personnel ou institutionnel, serveur ou équipement de télécommunication qui est utilisé sur le réseau informatique de l'Université doit respecter, au minimum, la configuration établie dans la Norme sur les configurations minimales de sécurité des systèmes d'information. Les services informatiques sont responsables d'assurer la conformité de tout poste de travail, serveur ou équipement de télécommunication appartenant à l'Université.

De plus, les logiciels et le système d'exploitation de tout poste de travail, personnel ou institutionnel, serveur ou équipement de télécommunication qui est utilisé sur le réseau informatique de l'Université ou pour s'y brancher à distance doivent être à jour. Toutes les mises à jour de sécurité disponibles pour ces logiciels et équipements doivent être installées.

La personne qui utilise un poste de travail personnel pour accéder à distance aux systèmes d'information de l'Université est responsable d'assurer sa conformité avec la Norme sur les configurations minimales de sécurité des systèmes d'information.

La direction de la sécurité de l'information peut bloquer l'accès au réseau à tout appareil, personnel ou institutionnel, s'il n'est pas conforme à la norme établie.

10.2 Réseau informatique

La configuration du réseau informatique de l'Université doit se faire en s'assurant, au minimum, que :

a) le réseau de l'Université respecte les zones spécifiques établies dans la topologie du réseau et les règles de sécurité afférentes à chacune des zones, conformément au Procédurier de la sélection d'une zone réseau;
b) toute communication entrante ou sortante du réseau de l'Université transite uniquement par des équipements autorisés par la direction de la sécurité de l'information;
c) toute modification de règle de communication ou relative à une zone sur le réseau soit approuvée par la direction de la sécurité de l'information.

11. Vérifications, journalisation et alertes

11.1 Vérifications

La direction de la sécurité de l'information doit, périodiquement, faire des tests de sécurité automatisés avec des outils d'analyse statique et dynamique, pour détecter les vulnérabilités, s'il en est.

Des tests d'intrusion sur les systèmes d'information doivent également être faits périodiquement pour évaluer leur résilience face aux attaques informatiques.

Concernant les systèmes d'information qui sont désignés comme étant les plus critiques, une firme externe doit être mandatée périodiquement pour y effectuer des tests d'intrusion.

11.2 Journalisation

Tout système d'information de l'Université doit faire la journalisation des événements y survenant. Ces journaux d'événements doivent être redirigés vers les outils spécifiques maintenus par les services informatiques.

L'accès aux outils et aux journaux d'événements doit être configuré pour que seuls les membres du personnel ayant besoin d'y accéder dans le cadre de leur travail puissent les consulter.

Les journaux d'événements doivent permettre les vérifications nécessaires à la détection des menaces et vulnérabilités, favorisant la mise en place de mesures de mitigation appropriées.
Les journaux d'événements ne doivent pas contenir de données sensibles.

11.3 Alertes

Des alertes doivent être générées automatiquement en cas de détection d'un comportement anormal ou suspect sur un système d'information, et doivent permettre une analyse en temps réel du comportement de même qu'une priorisation des incidents potentiels.

Le traitement des alertes doit être fait en respectant la Norme de catégorisation et de priorisation des incidents et événements de sécurité qui vise à assurer une priorisation efficace en fonction du risque et de l'impact potentiel.

12. Responsable de l’application

La vice-rectrice, le vice-recteur aux Systèmes d’information est responsable de l’application de cette directive.

13. Entrée en vigueur

La présente directive entre en vigueur dès son adoption par la vice-rectrice, le vice-recteur aux Systèmes d’information.

14. Mise à jour

Cette directive est mise à jour minimalement tous les cinq ans.