UQÀM | Université du Québec à Montréal

Directive sur la gestion des incidents de sécurité informatique

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

La présente directive a pour objectif d'établir les règles en matière d'incident de sécurité informatique à l'Université du Québec à Montréal (ci-après « l'Université »), et d'en assurer une compréhension et une application uniforme.

La gestion des incidents de sécurité informatique permet d'assurer :

a) une intervention structurée et une réponse optimale à tout incident de sécurité informatique;
b) le confinement rapide des systèmes d'information et des comptes utilisateurs qui sont compromis ou à risque de compromission.

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) hameçonnage : technique de fraude reposant sur l'usurpation d'identité et visant à tromper les destinataires en leur envoyant massivement des messages semblant provenir d'une institution financière ou d'une entreprise reconnue afin de recueillir des informations sensibles, protégées ou confidentielles;

b) pourriel : message électronique non sollicité, généralement envoyé en masse à des fins publicitaires, frauduleuses ou malveillantes;

c) virus (logiciel malveillant) : logiciel indésirable le plus souvent transmis par un réseau ou un support de stockage externe, ayant pour but d'infecter un fichier qui, lorsqu'il est exécuté, lui permettra de se propager et de produire les effets néfastes pour lesquels il a été conçu.

5. Détection des incidents

La détection des incidents de sécurité informatique doit être assurée par des mécanismes qui permettent, au minimum :

a) d'identifier en temps réel les événements associés aux incidents de sécurité informatique;

b) de trier et de prioriser les incidents détectés;

c) d'identifier les événements qui ont le potentiel d'être récurrents à des fins d'amélioration continue.

La cheffe, le chef de la sécurité de l'information organisationnelle (CSIO) est responsable de mettre en place et d'assurer le bon fonctionnement des moyens de détection des incidents de sécurité informatique.

6. Signalement des incidents

La personne utilisatrice d'un système d'information qui détecte, suspecte ou est informée d'un incident de sécurité informatique a l'obligation de le signaler sans délai à la, au CSIO, selon le processus établi.

La, le CSIO est responsable d'informer annuellement les personnes utilisatrices de leur obligation de signaler les incidents de sécurité informatique et de la méthode à utiliser pour effectuer un tel signalement.

7. Catégorisation des incidents

Les incidents de sécurité informatique sont catégorisés en fonction de la Norme de catégorisation et de priorisation des incidents et événements de sécurité pour faciliter l'identification des causes, ainsi que le choix du traitement et de la méthode de remédiation.

Les catégories d'incident de sécurité informatique qui, au minimum, doivent être considérées sont :

a) un appareil ou logiciel non-autorisé;
b) un déni de service;
c) un hameçonnage de masse ou ciblé;
d) le partage accidentel de données;
e) le piratage des systèmes;
f) un code malveillant, virus, service illicite ou rançongiciel;
g) un vol ou une perte d'équipement;
h) la violation des politiques et directives internes.

8. Plan d'intervention

Un plan d'intervention spécifique à chaque catégorie d'incident de sécurité informatique doit être documenté par la direction de la sécurité de l'information. Ce plan d'intervention doit permettre un traitement adéquat des incidents selon leur type d'impact et leur sévérité.

La direction de la sécurité de l'information a la responsabilité d'assurer le suivi du plan d'intervention.

Dans tous les cas, un incident touchant à la confidentialité de renseignements personnels est assujetti à la Procédure sur la gestion des incidents de confidentialité impliquant des renseignements personnels.

9. Documentation des incidents

La direction de la sécurité de l'information doit documenter chaque incident de sécurité informatique et sa résolution dans le registre tenu à cet effet.

10. Responsable de l'application

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

11. Entrée en vigueur

La présente directive entre en vigueur au moment de son adoption par la vice-rectrice, le vice-recteur aux Systèmes d'information.

12. Mise à jour

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