Université de Montréal

Direction générale des technologies
de l'information et de la communication

Directive sur les systèmes d'exploitation en usage à l'Université de Montréal

Novembre 2016

1.0 Préambule

Tout réseau informatique dans lequel les ordinateurs peuvent communiquer entre eux, et particulièrement l'Internet, sont potentiellement des environnements à risque pour un ordinateur. Quoiqu'un grand nombre de mesures de protection et contrôle soient prises sur notre réseau pour le rendre plus sécuritaire, tout ordinateur qui s'y trouve est à la merci d'un courriel ou contenu Web infecté par un virus jusque-là inconnu, d'un ver qui se propage en utilisant les vulnérabilités du système et de plusieurs autres vecteurs d'attaques.

En ce qui concerne la sécurité informatique, une des façons les plus sûres de se prémunir contre ces risques est de bien gérer son ordinateur. Un aspect important de cette bonne gestion est de s'assurer que le système d'exploitation et les autres programmes de cet ordinateur sont toujours le plus à jour possible.

Dans la poursuite de l'objectif d'avoir des systèmes d'exploitation à jour, l'Université doit évidemment s'appuyer sur les mises à jour des éditeurs. Or, les éditeurs ne soutiennent pas leurs produits indéfiniment : il vient un moment où un éditeur déclare qu'un produit logiciel ne sera plus mis à jour, même en cas de découvertes de nouvelles vulnérabilités de sécurité informatique. C'est alors qu'un ordinateur devient potentiellement vulnérable et à risque pour lui-même et pour le réseau, incluant tous les ordinateurs et utilisateurs qui en dépendent. La règle générale applicable dans ce cas est qu'un système d'exploitation (ou autre logiciel présentant des vulnérabilités) ne doit plus être présent sur le réseau de l'Université une fois que son éditeur ne le soutient plus.

La liste au point 4 tire explicitement les conclusions de cette règle pour les versions existantes des systèmes d'exploitation Windows et Mac OS, mais la règle s'applique aussi aux diverses distributions des systèmes d'exploitation Linux, UNIX ou autres, de même qu'aux logiciels.

La présente directive s'appuie sur la Politique de sécurité informatique et d'utilisation des ressources informatiques de l'Université de Montréal.

2.0 But

Cette directive a pour but de définir les systèmes d'exploitation qui seront permis sur le réseau de l'Université de Montréal pour les plates-formes Windows et Macintosh.

3.0 Portée

Cette directive s'applique à tout système présent sur le réseau de l'Université de Montréal. Chaque unité administrative ou chaque usager est responsable d'appliquer cette directive à ses propres équipements.

4.0 Directives

4.1 Versions permises de Windows

Postes de travail : 7, 8 et 10

Serveurs : 2008, 2008 R2, 2012 et 2012 R2.

4.2 Versions permises d'Apple Mac OS X

10.9, 10.10, 10.11

Note : Les systèmes utilisant la nouvelle version 10.12 (Sierra) sont actuellement permis, mais des tests exhaustifs sont en cours pour un support officiel.

4.3 Chacune des versions permises doit être maintenue à jour en tout temps. Les correctifs de sécurité publiés doivent être appliqués dès que possible ou à l'intérieur d'un délai raisonnable qui normalement ne doit pas dépasser 3 semaines.

5.0 Application

Un poste de travail ou un serveur qui ne se conforme pas à cette directive pourrait se voir refuser le droit d'accès au réseau de l'Université de Montréal.

6.0 Révision

Cette directive remplace la version précédente de la Directive sur les systèmes d'exploitation en usage à l'Université de Montréal, émise en septembre 2015.

Yves Bouchard
Directeur général
DGTIC