University Client Workstation Anti-Virus Control

Procedure Type:	Administration	**Initially Approved:**	07/18/12
Procedure Sponsor:	CIO, ITS	**Last Revised:**	07/17/19
Administrative Responsibility:	ITS	**Review Scheduled:**	
Approver:	Asad Israeli		

A. PROCEDURES

Mount Royal University administrative and lab computers are centrally managed by an enterprise management system. The Information Technology Services department is responsible for the security and integrity of datacentre, faculty, administrative staff, and student lab computers belonging to Mount Royal University. These computers are maintained and administered by the DataCentre, Office Computing Services and Student Computing Services within the Information Technology department.

1. Purpose

This procedure outlines Mount Royal University's deployment and audit procedures when it comes to Anti-Virus software on University owned and/or maintained machines. This procedure document also lists anti-virus related responsibilities for users and Information Technology staff.

2. Scope

This procedure applies to all computing devices that are connected to the Mount Royal University network via Ethernet connection, wireless connection, modem connection, or virtual private network connection. That are managed and maintained by Student Computing Services and Office Computing Services. IT Services reserves the right to confirm any device attached to the MRU network is compliant with current MRU anti-virus procedure. MRU computing equipment deemed not in compliance will be made compliant by IT Services staff. All other computing equipment, not MRU property, attached to the MRU network will be disconnected until compliance with this procedure has been met and IT Services is satisfied with the level of security and functionality of the device in question. Repeated failure of non-MRU computing equipment to comply with this procedure and other MRU standards may result in a permanent ban of connectivity to the MRU network.

*Client systems will be validated to ensure that systems are complaint to the current client version.

B. DEFINITIONS

(1)	**CIO:**	Chief Information Officer
(2)	**IT:**	Information Technology
(3)	**ITS:**	Information Technology Services

C. DEPLOYMENT PROCESS

Anti-virus agents are deployed in the following manner:

1. Upon new system deployment preparation
2. Upon system reimage
3. Via Domain Policy

Audits

1. On demand, random audits may be performed on department or individual client computers at regular intervals.

2. Bi-annual audits are performed at peak campus connectivity to faculty, staff, and lab computers.

Responsibilities

The following activities are the responsibility of Mount Royal University departments and employees:

1. Departments that allow employees, academic visitors, and contractors to use personally-owned computers on campus must register and seek connectivity approval from Information Technology Services.

2. All employees and academic visitors are responsible for taking reasonable measures to protect against virus infection.

The following activities are the responsibility of Mount Royal University IT Services department:

1. The IT Services department is responsible for maintaining and updating this Anti-Virus Procedure.

2. The IT Services department will keep the anti-virus products it provides up-to-date in terms of both virus definitions and software in use. Software is automatically updated from the vendor site and DATS regularly downloaded and evaluated before campus wide deployment.

3. Mount Royal University computing equipment is set up to automatically seek anti-virus updates daily.

4. The IT Services department will apply any updates to the services it provides that are required to defend against threats from viruses, spyware, and malware.

5. The IT Services department will install anti-virus software on all Mount Royal University owned and installed desktop workstations, laptops and servers.

6. The IT Services department will assist faculty, staff and students in installing anti-virus software according to University standards on personally-owned devices that have been approved connectivity to Mount Royal University network infrastructure.

7. The IT Services department will take appropriate action to contain, remove and assist in recovery from virus infections. The IT department may be required to disconnect a suspect computer from the network or disconnect an entire segment of the network.

8. The IT Services department will attempt to notify the university community of any credible virus threats via campus wide communications. Virus reports will not be acted upon until validation.

D. RELATED POLICIES

- Acceptable Use of Computing and Communication Resources Policy

E. REVISION HISTORY

Date (mm/dd/yyyy)	**Description of Change**	**Sections**	**Person who Entered Revision (Position Title)**	**Person who Authorized Revision (Position Title)**