Anti-Virus Policy

1.0 Overview

The purpose of this policy is to provide a framework for processes that are intended to prevent the spread of computer viruses.

2.0 Purpose

3.0 Scope

This policy applies to all Clarkson University employees and affiliates.

4.0 Policy

Anti-Virus software serves as a frontline of defense against the spread of computer viruses. As such, the following guidelines should be observed at all times:

- Always run the Clarkson University standard, supported anti-virus software.
- NEVER open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Delete spam, chain, and other junk email without forwarding, in accordance with Clarkson University's *Acceptable Use Policy*.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access unless there is a demonstrated business requirement to do so.
- Always scan a USB key from an unknown source for viruses before using it.
- If lab testing conflicts with anti-virus software, run the anti-virus utility to ensure a clean machine, disable the software, then run the lab test. After the lab test, enable the anti-virus software. When the anti-virus software is disabled, do not run any applications that could transfer a virus, e.g., email or file sharing.

5.0 Enforcement

6.0 Definitions