PURPOSE

This Standard supports the Malicious Code Prevention Policy and identifies additional detail for the implementation of the policy. This Standard provides an overview of the applicable virus prevention required by the University.

SCOPE

This policy applies to all members of the Creighton University community (staff, faculty, students, contractors, consultants, temporaries, visitors, etc.) while using Creighton’s computing or networking resources. All users are expected to be familiar with and comply with this policy.

STANDARD

University-Standard Package

- Only University-approved anti-virus packages are to be used, where they exist, for each computing platform.

- There is only one approved anti-virus package for each computing platform.

- All computers connecting to Creighton’s network must use the University-approved anti-virus package and conform to this standard.

- The configuration of the standard anti-virus software shall not be disabled or modified in any way except to provide additional protection from viruses.

Package Updates

- Anti-virus package updates, including both anti-virus and virus definition updates, must be applied to all systems as soon as possible after their release.

- The timeframe for distribution of new anti-virus updates must be based on a reasonable balance of internal testing and risk mitigation.

Periodic Scanning

- University approved anti-virus software shall be configured to scan all files on the system’s local disk drive for viruses at least once per week.

E-mail Scanning
Policies and Standards

SECTION: Security

CHAPTER: General

POLICY: Malicious Code Prevention Standard

• All e-mail servers shall have anti-virus software installed to scan e-mail messages for viruses before being sent outside the University.

• All e-mail servers shall have anti-virus software installed to scan all incoming e-mail messages for viruses before being stored in a mailbox.

Operating System Scanning

• University approved anti-virus software shall be configured to scan critical operating system files for viruses every time the operating system is booted.

Removable Media

• University approved anti-virus software shall be configured to scan floppy disks and removable media for boot sector viruses when those media are inserted into protected computers.

Remedies

• Any computer system infected with a virus may be removed from the network at any time.

• Computer systems that are not in full compliance with any part of the requirements defined in this standard may be removed from the network at any time.

DEFINITIONS

Boot Sector Virus
A boot sector virus is a virus that loads into memory when an infected PC is booted and then infects any floppy disk used in the PC. A PC which boots from an infected floppy disk becomes infected.

RESPONSIBILITIES

Network Users are responsible for ensuring they at least meet the requirements defined in this standard.

Systems Administrators are responsible for taking all reasonable action to contain the effects of any system that is infected with a virus or other malicious software.

Information Security is responsible for selecting the University approved anti-virus software and ensuring the standard package is configured to meet this standard.

ADMINISTRATION AND INTERPRETATIONS

Internal Use Only
DRAFT
This standard shall be administered by Information Security. Questions regarding this policy should be directed to the Information Security Officer.

AMENDMENT/TERMINATION OF THIS POLICY

The University reserves the right to modify, amend or terminate this standard at any time. This standard does not constitute a contract between the University and its faculty or employees.

REFERENCES TO APPLICABLE STANDARDS

- Information Security Philosophy
- Information Security Governance Policy
- Information Security Exception Policy
- Malicious Code Prevention Policy

EXCEPTIONS

Requests for an exception to this standard must be submitted via the Policy Exception Request Form. All exception requests will be handled in accordance with the Information Security Exception Policy and Standard.

VIOLATIONS/ENFORCEMENT

Any known violations of this standard should be reported to the University’s Information Security Officer at 402-280-2386 or via e-mail to infosec@creighton.edu.

Violations of this standard can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with University procedures.

The University may advise law enforcement agencies when a criminal offense may have been committed.