Policies and Standards

SECTION: Security
CHAPTER: General
POLICY: Malicious Code Prevention Policy

PURPOSE

Computer viruses, worms, trojans, etc. have the potential of bringing harm to Creighton's computing network. The spread of malicious code can be linked to productivity and/or financial loss. This loss will always result in some type of financial impact to the University. Further, the reputation and credibility of Creighton University could be damaged due to the distribution of a virus. Creighton takes a strong stance on the prevention of infection by viruses. This policy defines Creighton’s stance on malicious code prevention.

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.

POLICY

All computers connected to Creighton’s computing network must have current virus protection measures in place, as defined in the Malicious Code Prevention Standard.

DEFINITIONS

Malicious code
Malicious code is computer programming code or files that are developed for the purpose of doing harm. Thus, malicious code includes computer viruses, worms, and Trojan horses.

RESPONSIBILITIES

System Users of the Creighton network must ensure that files from all sources are scanned before loading them on the network, or their local PC.

System Administrators must ensure that all software introduced to a server is scanned for viruses, before implementing the software on a production server.

Information Security has the sole authority to approve a product to be used for primary and secondary virus prevention and detection.

ADMINISTRATION AND INTERPRETATIONS

This policy 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 policy at any time. This policy 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 Standard

EXCEPTIONS

Requests for an exception to this Policy 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 policy 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 policy 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.