PURPOSE

The network security policy is intended to protect the integrity of University networks and to mitigate the risks and losses associated with security vulnerabilities to University networks and network resources.

Attacks and security incidents create a risk to the University's mission. The loss of data integrity or unauthorized disclosure of information on financial, administrative, academic, research, and clinical systems deter the activities of University staff, faculty, and students. This policy will allow the University to handle network security responsibly.

SCOPE

This policy applies to all Creighton Network attached devices, regardless of physical location.

POLICY

It is the policy of the University to maintain the security of Information Technology resources. Creighton University expects all individuals using information technology devices connected to the Creighton network to take appropriate measures to address the security of those devices.

It is the responsibility of all Creighton Network users to ensure all networked devices under their control are properly patched against known security vulnerabilities, protected against virus/worm infections, and do not negatively impact other users’ use of the network.

More information is available in the Network Security Standard.

DEFINITIONS

Network Connected Device
A networked device is any piece of equipment that directly connects to Creighton’s network, either via wired or wireless connection; such as personal computers, laptops, servers, network printers, wireless access points, switches, routers, etc.

Security Vulnerabilities
A weakness in system security procedures, system design, implementation, internal controls, etc., that could be exploited to compromise the system’s confidentiality, integrity, or availability.

Patched
The process of finding, testing, and installing a modification (patch) to software that fixes an error in an application already installed on a system; patches are generally supplied by the vendor of the software.

RESPONSIBILITIES
Creighton Network Users are responsible to ensure all networked devices under their control are properly patched against known security vulnerabilities, protected against virus/worm infections, and do not impact other users use of the network.

Information Security Officer is responsible for ensuring network users adhere to this policy.

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
Information Security Malicious Code Policy
Information Security Malicious Code Prevention Standard
Information Security Network Security 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 where University network resources and privileges are threatened by improperly maintained computing devices, Information Security and IT may act on behalf of the University to eliminate the threat by working with the relevant system administrator to quickly patch security holes. In circumstances where there is an urgent situation requiring immediate action, the device may be disconnected from the network by Information Security or IT. Abuse of this policy may lead to revocation of network privileges.