PURPOSE

Increases in non-traditional teaching methods and the increased mobility of faculty and students has made remote access to centralized University assets increasingly important. Opening uncontrolled or unsecured paths into any element of the University network or internal computer systems presents additional risk to the entire University infrastructure. Establishing policy centrally and issuing standards from a central authority allows a minimum number of penetrations of the security of the network while still allowing flexibility in the actual remote connection technology used.

SCOPE

This policy applies to all Creighton University staff, faculty, students, contractors, vendors and agents with a Creighton-owned or personally-owned computer or workstation used to connect to the Creighton University network. This policy applies to remote access connections used to do work on behalf of Creighton University, including reading or sending email and viewing web resources.

POLICY

Creighton University’s internal computers systems, networks and data of are critical resources to the University and must be protected against unauthorized and malicious access, and disruption of service. Authorized users of Creighton University computer systems, networks and data may remotely connect to those systems, networks and data for the conduct of University related business only through secure, authenticated and centrally managed access methods.

In order to manage remote access reliably and in a low risk manner, all authorized students, faculty, and staff must use only University approved methods of remote access.

DEFINITIONS

Remote Access
Any access to Creighton University's network through a non-Creighton controlled network, device, or medium.

RESPONSIBILITIES

Information Security is responsible for the approving and securing the remote access methods.

Network Users are responsible for adhering to this policy when accessing Creighton University systems remotely.
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
Remote Access Standards

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.