PURPOSE

These standards are designed to minimize the potential exposure to Creighton University from damages which may result from unauthorized use of Creighton resources. Damages include the loss of sensitive or University confidential data, intellectual property, damage to public image, damage to critical internal systems, etc.

SCOPE

This standard 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.

Remote access implementations that are covered by this standard include, but are not limited to, dial-in modems, frame relay, ISDN, DSL, VPN, SSH, cable modems, etc.

STANDARD

**Remote Access Privilege Approval:** Access to university internal networks from remote locations including homes, hotel rooms, wireless devices and off-site offices is not automatically granted with network or system access. Systems that contain confidential student, personnel and financial data will be available for off-site remote access only after an explicit request is made and approved by the data steward for the target system. Access will be permitted through a centrally managed virtual private network (VPN) that provides encryption and secure authentication. Access may be revoked at any time for reasons including non-compliance with security policies, request by the user's supervisor or negative impact on overall network performance attributable to remote connections.

**Administration/Authentication:** The administration and authentication system for remote access will be centrally managed. Authentication for remote access will be strong. Passwords will not traverse the network in the clear text and must meet minimum requirements as documented in University security policies.

**Responsibility for User-IDs:** All users who require remote access privileges (including affiliates) are responsible for the activity performed with their personal user-IDs, whether or not these user-IDs are connecting via external network facilities. User-IDs must never be shared with associates, friends, family members, or others. User-IDs may not be utilized by anyone but the individuals to whom they have been issued. Similarly, users are forbidden from performing any activity with user-IDs belonging to other individuals.

**Anti-Virus and Firewall Protection:** External computers or networks making remote connection to university internal computers or networks must utilize an active virus scanning...
Remote Access Security: Creighton University staff, faculty, students, contractors, vendors and agents with remote access privileges must ensure that their Creighton-owned or personal computer or workstation, which is remotely connected to Creighton's network, is not connected to any other network at the same time, with the exception of personal networks that are under the complete control of the user. Reconfiguration of a home user's equipment for the purpose of split-tunneling or dual homing is not permitted at any time.

Unauthorized Remote Access Mechanisms: Departments or individuals who wish to implement non-standard Remote Access solutions to the Creighton University production network must obtain prior approval from the Information Security Department.

**DEFINITIONS**

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

Cable Modem
Cable companies such as Cox Communications provide Internet access over Cable TV coaxial cable. A cable modem accepts this coaxial cable and can receive data from the Internet at over 1.5 Mbps.

Dial-in Modem
A peripheral device that connects computers to each other for sending communications via the telephone lines. The modem modulates the digital data of computers into analog signals to send over the telephone lines, then demodulates back into digital signals to be read by the computer on the other end; thus the name "modem" for modulator/demodulator.

DSL
Digital Subscriber Line (DSL) is a form of high-speed Internet access competing with cable modems. DSL works over standard phone lines and supports data speeds of over 2 Mbps downstream (to the user) and slower speeds upstream (to the Internet).
ISDN
ISDN is a form of high-speed Internet access competing with cable modems and DSL.

Dual Homing
Having concurrent connectivity to more than one network from a computer or network device. Examples include: Being logged into the University network via a local Ethernet connection, and dialing into AOL or other Internet service provider (ISP). Being on a Creighton-provided Remote Access home network, and connecting to another network, such as a spouse's remote access.

Split-tunneling
Simultaneous direct access to a non-Creighton network (such as the Internet, or a home network) from a remote device (PC, PDA, etc.) while connected into Creighton's network via a VPN tunnel.

VPN
Virtual Private Network (VPN) is a method for accessing a remote network via "tunneling" through the Internet. VPN's provide both encryption and secure authentication.

RESPONSIBILITIES

Network Users are responsible for ensuring they meet or exceed the requirements defined in this standard.

Information Security is responsible for ensuring the adherence to this standard.

ADMINISTRATION AND INTERPRETATIONS

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
Remote Access Policy
Cryptography Policy
Encryption Standard
Virtual Private Network (VPN) Standard
Acceptable Use 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 policies.

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