PURPOSE

This standard provides guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the Creighton University network.

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.

STANDARD

**University Approved Remote Access Method:** IPSec or L2TP Virtual Private Network (VPN) connections are the Universities approved remote access method.

**User Responsibility:** Approved Creighton University staff, faculty, students, contractors, and authorized third parties (customers, vendors, etc.) may utilize the benefits of VPNs, which are a "user managed" service. This means that the user is responsible for selecting an Internet Service Provider (ISP), coordinating installation, installing any required software, and paying associated fees. VPN is the security mechanism that builds the secure tunnel between the users ISP and the University network.

**Unauthorized Access:** It is the responsibility of the user with VPN privileges to ensure that unauthorized users are not allowed access to Creighton’s internal networks.

**Network Security:** Dual (split) tunneling is NOT permitted; only one network connection is allowed. All computers connected to Creighton’s internal networks via VPN or any other technology must use the most up-to-date anti-virus software that is the corporate standard; this includes personal computers.

Users of computers that are not Creighton-owned equipment must configure the equipment to comply with Creighton's Remote Access and Network policies.

**VPN Configuration:** VPN gateways will be set up and managed by Creighton University’s Information Security Department.

VPN users will be automatically disconnected from Creighton’s network after thirty minutes of inactivity. The user must then logon again to reconnect to the network. Pings or other artificial network processes are not to be used to keep the connection open.

The VPN concentrator is limited to an absolute connection time of 24 hours.
## Policies and Standards

<table>
<thead>
<tr>
<th>SECTION: Security</th>
<th>NO.</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHAPTER: General</td>
<td></td>
</tr>
<tr>
<td>POLICY: Virtual Private Network Standard</td>
<td>PAGE 2 OF 3</td>
</tr>
</tbody>
</table>

Only Creighton-issued VPN clients may be used.

**Information Security Policy Compliance:** By using VPN technology with personal equipment, users must understand that their machines are a de facto extension of Creighton’s network, and as such are subject to the same rules and regulations that apply to Creighton-owned equipment, i.e., their machines must be configured to comply with Creighton’s Information Security Policies.

### DEFINITIONS

**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.

**ISP**
Internet Service Provider is a third-party company who will sell provisional access to the Internet. Examples of local ISP are Cox Communications, America Online, Radiks, MSN, etc. It is the user’s responsibility to have access to the Internet via an ISP in order to utilize Creighton’s VPN/Remote Access mechanism.

**IPSec**
Short for IP Security, a set of protocols developed to support secure exchange of packets at the IP layer. IPsec has been deployed widely to implement Virtual Private Networks (VPNs).

**L2TP**
Short for *Layer Two (2) Tunneling Protocol*, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems.

**VPN Concentrator**
A device in which VPN connections are terminated.

### 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.

### REFERENCES TO APPLICABLE STANDARDS

- Information Security Philosophy
- Information Security Governance Policy
- Information Security Exception Policy
- Remote Access Policy
Remote Access Standard

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.