The purpose of an Information Technology Standard is to specify requirements for compliance with Old Dominion University Information Technology policies, other University policies, as well as applicable laws and regulations. Standards may include business principles, best practices, technical standards, migration and implementation strategies, that direct the design, deployment and management of information technology.

Information Technology Standard: University Virtual Private Network Standard
Reference Number: 02.5.0
Date of Current Revision or Creation: August 2013

A. PURPOSE
The purpose of this standard is to outline the purpose and use and requirements for using the University’s Virtual Private Network (VPN) technology.

B. DEFINITIONS
Virtual Private Network (VPN) is a secure encrypted network connection over the Internet between an individual and a private network.

University Data - All data or information owned, used, created or maintained by the University whether individually controlled or shared, stand-alone or networked.

C. STANDARDS STATEMENT
All Old Dominion University employees and authorized third parties may utilize the benefits of the Virtual Private Network (VPN) to access University computing resources to which they have been granted access.

VPN gateways are set up and managed by Information Technology Services network staff. No other department may implement VPN services unless approved by the Information Technology Services.
All computers, including personal computers, connected to the Old Dominion University internal networks via VPN or any other technology must use the most up-to-date anti-virus software and must regularly apply critical patches to their computer’s operating system.

To protect the integrity and security of data, ITS may restrict the combined use of the VPN with applications that use the Remote Desktop Protocol (RDP) where used to access a University IT service.

When actively connected to the Old Dominion University network, the VPN will force all traffic to and from the workstation over the VPN tunnel: all other traffic will be dropped.

Dual (split) tunneling is NOT permitted; only one network connection is allowed.

VPN users will be automatically disconnected from Old Dominion University network after thirty (30) 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.

VPN connection time is limited to an absolute continuous connection time of 9 hours. Users may reconnect if necessary.

Communications on the University’s computer systems may be monitored and/or recorded to ensure the effective operation of these systems and for other legal purposes.

The University reserves the right to monitor for unauthorized VPNs and disable access of those devices performing non-sanctioned VPN service.

**VPN Accounts**
A Virtual Private Network (VPN) connection is available to all employees and authorized third parties with a need to access resources internal to the campus network.

Accounts requests are made via an electronic account request form available at [https://midas.odu.edu](https://midas.odu.edu). The successful completion of online training is required before users may download and install the VPN client software to their device.

VPN access is controlled using a unique user account and strong authentication. The minimum standard is a mixed case eight character or more password with at least two digits.

**User Responsibilities**
Users must ensure that unauthorized users are not allowed access to the Old Dominion University campus networks.

Users must ensure that computers connected to the network via VPN are configured with up-to-date anti-virus, operating system updates, and active firewall software.
By using VPN technology with personal equipment, users must understand that their machines are an extension of the institution’s network and as such are subject to the same rules and regulations that apply to University-owned equipment.

**Audits**
Periodic audits of VPN access will be conducted to verify that the actual user connected to the VPN and their account have not been compromised.

**Exceptions**
Any exceptions to this Policy must be approved in writing by the Information Security officer or his designee.

**Enforcement**
Failure to comply may result in disciplinary sanctions consistent with University policies and applicable law.

**D. PROCEDURES, GUIDELINES & OTHER RELATED INFORMATION**

Federal and State Law
University Policy 3500 Use of Computing Resources
University Policy 3505 Information Security Policy
05.4.0 Virus and Malicious Code Protection Standard
09.1.0 Acceptable Use Standard

**E. HISTORY**

<table>
<thead>
<tr>
<th>Date</th>
<th>Responsible Party</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>December 2006</td>
<td>IT Policy Office</td>
<td>Created</td>
</tr>
<tr>
<td>August 2013</td>
<td>IT Policy Office</td>
<td>Updated for clarity and to reflect changes in access</td>
</tr>
</tbody>
</table>