

Compliance Standard

Title: Virtual Private Network Standard
Reference Number: 5.4.4

Purpose

This compliance standard is to state the requirements for remote access to centralized computing resources using the Virtual Private Network technology.

Scope

This standard pertains to all information technology resources used to conduct university business or used to transmit or store sensitive data. The standard is strongly encouraged for all IT systems; however, its application should not impede instruction and research activities. Any activity should not introduce unacceptable risk to the business operations protected by this standard.

Virtual Private Network

Any authorized user willing to comply with the established requirements may use VPN technology. User access must be managed in a manner designed to minimize risk, ensure user and data confidentiality over an insecure medium such as the Internet, and maintain the integrity of the connecting client system and University systems that the user connects to through the Virtual Private Network (VPN.)

Users must ensure that unauthorized use or users are not allowed access to the University network or access through the University network through the VPN to other networks.

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

When actively connected to the University network, the VPN configuration will force all traffic to and from the PC over the VPN tunnel. Dual (split) tunneling technology or connectivity is not permitted; only one network connection is allowed to be active while the VPN is in use.

VPN gateways are set up and managed by OCCS personnel only.

All computers connected to the network via VPN must be configured with up-to-date anti-virus, operating system updates, and active firewall software.

Users will be automatically disconnected from the VPN after thirty minutes of inactivity. Users may logon again to reconnect to the network. Pings or other artificial network processes cannot be used to keep the connection open or active.

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

Only OCCS-approved VPN clients and configurations may be used.

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

Scans of connecting systems where the University's IP address space is extended to the connecting system will be conducted on a periodic basis to insure that connecting systems are

Old Dominion University Technology Policies, Standards, Procedures and Guidelines

protected and being kept up to date. Systems found with weak or insufficient security will be immediately and forcibly disconnected from the VPN.

VPN access will be denied to the user and their supervisor will be notified. Reauthorization may be granted after security issues are resolved.

Enforcement

Any employee found to have violated this **policy** may be subject to disciplinary action.

Users of the Virtual Private Network (VPN) are required to submit an approved application for remote access.

Definitions

Remote Access is any access to ODU's network through a non controlled network, device, or medium.

Virtual Private Network (VPN) is a secure method for accessing a remote network via "tunneling" through the Internet.

User includes anyone who accesses and uses the Old Dominion University information technology resources.

Policy References

ODU faculty, staff and students are bound by all applicable laws, policies, standards and procedures and guidelines. For reference, some frequently referenced documents are noted. This is a non-inclusive list and not intended to limit applicability of any other law or policy.

Ⓢ Policy Foundation:	Federal and State Law, including Copyright law Policy 3500 Use of Computing Resources
📄 Related Standards:	Data Classification Standard Acceptable Use Standard Remote Access Standard
📄 Related Procedures, Forms:	Application for VPN Access Form
① Related Guidelines:	None
✂ Maintenance:	Office of Computing and Communications Services
✓ Effective Date:	Reviewed on an annual basis
✓ Approved by:	Rusty Waterfield Acting Assistant Vice President, Office of Computing and Communications Services
✓ Approved: December 2006	Information Technology Advisory Council <input checked="" type="checkbox"/> Required for Standard

**Old Dominion University
Technology Policies, Standards, Procedures and Guidelines**