



## OIT 62.008: Virtual Private Networking Policy

**Responsible Executive:** Chief Information Officer (CIO)  
**Responsible Office:** Office of Information Technology  
**Related Policy:** 60.201: Acceptable Use of Technological Resources  
62.005: Firewall Administration  
**Approved-On Date:** June 8, 2005  
**Effective Date:** June 8, 2005  
**Revision Date:** January 29, 2009

### Policy Statement

Access to Norfolk State University (NSU) protected technological resources is available via virtual private networking (VPN) for the purpose of managing technological resources and for University business, education, and research.

### Purpose

The purpose of this policy is to provide guidelines for Remote Access IPSec or L2TP Virtual Private Network (VPN) connections to the NSU network.

### Scope

This policy applies to all NSU employees, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties utilizing VPNs to access the NSU network. This policy applies to implementations of VPN that are directed through an IPSec Concentrator which is a network appliance used for terminating a large number of VPN connections in an orderly, secure, and efficient manner.

### Policy

Approved NSU employees 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. Additionally,

1. It is the responsibility of employees with VPN privileges to ensure that unauthorized users are not allowed access to NSU internal networks.

2. VPN use is to be controlled using either a one-time password authentication such as a token device or a public/private key system with a strong passphrase and strong user authentication through an OIT managed and centralized external database or proxy such as TACACS+, RADIUS, LDAP or something similar.
3. Dual (split) tunneling is permitted and may be configured on VPN connections.
4. VPN gateways will be configured and managed by OIT.
5. All personal computers and workstations connected to NSU internal networks via VPN or any other technology must use the most up-to-date anti-virus software; use either enterprise or personal firewall technology; and, have the latest security-related software patches/fixes installed.
6. VPN users will be automatically disconnected from NSU's network after thirty minutes of inactivity. Users 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.
7. The VPN concentrator is limited to an absolute connection time of 24 hours.
8. Users of computers that are not NSU-owned equipment must configure the equipment to comply with NSU's VPN and Network policies.
9. Only NSU-approved VPN client software may be used.
10. By using VPN technology with personal equipment, users must understand that their computers are 'de facto' extensions of the University's network, and as such are subject to the same rules and regulations that apply to NSU-owned equipment, i.e., their computers must be configured to comply with University security policies, standards, and procedures.