



OIT 62.504: Remote Access

Responsible Executive: Information Security Officer
Responsible Office: Office of Information Technology
Related Policy: 60.603: Encryption
Approved-On Date: 2/28/2011
Effective Date: 7/1/2011
Revision Date: 2/1/2011

I. Policy Statement

Remote Access requirements identify the steps necessary to provide for the secure use of remote access to resources used by the COV. OIT provides centralized access to Norfolk State University (NSU) protected technological via virtual private networking (VPN) for the purpose of managing technological resources and for University business, education, and research.

II. Purpose

The purpose of this policy is to provide guidelines for Remote Access IPsec, L2TP, SSL Virtual Private Network (VPN) connections to the NSU network. Additionally, this policy applies to remote access technologies, such as Secure Shell, Remote Desktop and other remote access technologies.

III. Scope

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

IV. Requirements

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. When actively connected to the University network, VPNs will force all traffic to and from the PC over the VPN tunnel; all other traffic will be dropped except in case of split tunneling as described below.
4. Dual (split) tunneling is NOT permitted; only one network connection is allowed unless granted in writing by an approved waiver coordinated through the Information Security Officer.
5. University VPN gateways will be configured and managed by OIT.
6. 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.
7. 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.
8. The VPN concentrator is limited to an absolute connection time of 24 hours.
9. Users of computers that are not NSU-owned equipment must configure the equipment to comply with NSU's VPN and Network policies.
10. Only NSU-approved VPN client software may be used.
11. 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.

Whether remote access to COV resources provided by OIT or by another entity, the remote access provider shall:

1. Protect the security of all remote access to the agency's sensitive IT systems and data by means of encryption, in a manner consistent with Section 6.3.

Note: This encryption requirement applies both to session initiation (i.e., identification and authentication) and to all exchanges containing sensitive data.

2. Protect the security of remote file transfer of sensitive data to and from agency IT systems by means of encryption, in a manner consistent with Policy 62.603 Encryption.
3. Document requirements for use of remote access and for remote access to sensitive data, based on agency and COV policies, standards, guidelines, and procedures.
4. Require that IT system users obtain authorization and a unique user ID and password prior to using the agency's remote access capabilities.
5. Document requirements for the physical and logical hardening of remote access devices.
6. Require maintenance of auditable records of all remote access.
7. Where supported by features of the system, session timeouts shall be implemented after a period of no longer than 30 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented.

V. Violations

Violations of this policy will be addressed in accordance relevant University and Commonwealth of Virginia policies, including University Policy 60.201 and Department of Human Resources Management Policy 1.75. The appropriate level of disciplinary action will be determined on an individual case basis by the appropriate executive or designee, with sanctions up to or including termination or expulsion depending upon the severity of the offense.

VI. Interpretation

The Information Security Officer is responsible for official interpretation of this policy. Questions regarding the application of this policy should be directed to the

Office of Information Technology. The Information Security Officer reserves the right to revise or eliminate this policy.