Policy Title: Remote Access

Policy Type: Administrative


Approval Date: 05/20/2014 Revised

Responsible Office: Office of Information Technology

Responsible Executive: CIO

Applies to: Office of Information Technology

POLICY STATEMENT

NSU reserves the right to grant or deny remote access capabilities to the University information system at its discretion to any user at any time. In the event remote access is granted, the following conditions are required for each occurrence of remote access.
PURPOSE

This control is intended to establish 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.

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.

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.

NSU:

1. Documents allowed methods of remote access to the information system;

2. Establishes usage restrictions and implementation guidance for each allowed remote access method;

3. Monitors for unauthorized remote access to the information system;

4. Authorizes remote access to the information system prior to connection; and

5. Enforces requirements for remote connections to the information system.

NSU shall:

1. When connected to internal networks from University guest networks or non-University networks, data transmission shall only use full tunneling and not use split tunneling.

2. Protect the security of remote file transfer of sensitive data to and from agency IT systems by means of approved encryption.

3. Require that IT system users obtain formal authorization and a unique user ID and password prior to using the NSU’s remote access capabilities.

4. Document requirements for the physical and logical hardening of remote access devices.

5. Require maintenance of auditable records of all remote access.

6. 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.

Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the University may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to University information system(s) by a user (or process acting on behalf of a user)
communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless. A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., NSU establishes a network connection between University controlled endpoints in a manner that does not require NSU to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access.

Control Enhancements for Sensitive Systems:

1. NSU employs automated mechanisms to facilitate the monitoring and control of remote access methods.

   Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information.

2. NSU uses cryptography to protect the confidentiality and integrity of remote access sessions.

   Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information.

3. The information system routes all remote accesses through a limited number of managed access control points.

4. NSU authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.

5. NSU monitors for unauthorized remote connections to the information system, and takes appropriate action if an unauthorized connection is discovered.

6. NSU ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.

7. NSU ensures that remote sessions for accessing sensitive data or development environments employ two-factor authentication and are audited.

   Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled).
8. NSU disables all TCP and UDP ports except for explicitly identified components in support of specific operational requirements.

Enhancement Supplemental Guidance: NSU can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.

VIOLATIONS

Violations of this policy will be addressed in accordance with relevant University and Commonwealth of Virginia policies, including University Policy 32-01 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.

INTERPRETATIONS

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.

PUBLICATION

This policy shall be widely published and distributed to the University community. To ensure timely publication and distribution thereof, the Responsible Office will make every effort to:

1. Communicate the policy in writing, electronic or otherwise, to the University community within 14 days of approval;
2. Submit the policy for inclusion in the online Policy Library within 14 days of approval;
3. Post the policy on the appropriate SharePoint Site and/or Website; and
4. Educate and train all stakeholders and appropriate audiences on the policy’s content, as necessary. Failure to meet the publication requirements does not invalidate this policy.

REVIEW SCHEDULE

- Next Scheduled Review: 05/28/2015
- Approval by, date: Office of Information Technology and 05/28/2014
Revision History:

- Supersedes (previous policy): OIT 62.8.117 Remote Access

RELATED DOCUMENTS

Virginia Commonwealth State policy SEC501-08 Information Security Standard