University System of New Hampshire

REMOTE ACCESS SECURITY STANDARD

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: ET&S Cybersecurity GRC
Approved Distribution: Public
Status: IN FORCE

1. Introduction

The purpose of this standard is to establish authorized methods for remotely accessing University System of New Hampshire resources and services securely.

Major security concerns with remote access include the lack of physical security controls, the use of unsecured networks, the connection of infected devices to internal networks, the availability of internal resources to external hosts, potential damage to resources, and unauthorized access to information.

2. Standard

Remote Access Standards:

- This Standard applies to any authorized user accessing University Technology Resources from an external network using remote access solutions.
- Approved remote access technologies must be used to connect to USNH technology resources from a non-university location.
- Authorized users must never share their credentials to facilitate remote access authentication for unauthorized individuals.
- Multi-factor authentication (MFA) is required for all remote access solutions when feasible.
- Institutionally owned devices or personal devices that are connected to a USNH network or USNH information technology resource, or that are used to conduct USNH business, are required to meet minimum security standards outlined in the Endpoint Management Standard for remote access.
- Devices and software used for remote access must be approved by the Information Security Officer/designated security representative.

University System of New Hampshire

- When feasible, remote access technologies must use a centrally managed authentication system for administration and user access authentication.

- Remote access traffic is subject to monitoring for anomalous and malicious behavior. Remote access logs will be kept for a minimum of 90 days and must contain successful/unsuccessful login attempts, event type, date/time, associated user, remote and local IP Address.

- At a minimum of 90 minutes of inactivity, remote access sessions must require re-authentication or devices must utilize lockout/screen lock mechanisms based on operational needs to prevent unauthorized access.

- Remote access sessions must time out after 24 hours and require re-authentication before re-use.

- Any requirements for extended access must submit a security exception request.

Virtual Private Network (VPN) Access:

- USNH provides Virtual Private Networks ("VPNs") (e.g., Global Protect, Pulse Secure) to permit access to University Information Systems.

- All authorized USNH users may utilize the benefits of the USNH Virtual Private Network (VPN) to access University computing resources to which they have been granted access.

- Enterprise and/or other USNH VPN gateways are managed by or in conjunction with USNH ET&S Information Technology Services network and security staff.

- Remote VPN access to USNH Resources is only permitted using the following approved VPN technologies: Global Protect / Pulse Secure.

- VPN gateways may only be established by ET&S Networking. No other department or individual may implement VPN Gateways to USNH Technology Resources without prior authorization. USNH reserves the right to monitor unauthorized VPNs and disable access of those devices that could cause harm to the stability of the USNH network.

- USNH VPNs will employ at minimum AES-256 Advanced Encryption Standard to ensure confidentiality over remote connections.

- The use of “Split Tunneling - routing some of your applications or device traffic through an encrypted VPN, while other applications or devices have direct access to the internet” should only be used if there is an operational need.

- Remote access VPN may **not** be permitted from some locations, such as embargoed or sanctioned countries.

- Authorized users must always disconnect from a VPN solution when not utilizing it.

Remote Desktop Access:

- The University provides programs or operating system features that allow authorized users to connect remotely to a physical or virtual computer located on the Campus Network on which a remote computer resides (“Remote Desktop”).

- Remote Desktop access is subject to permissions granted by University Information System owners.

- Remote Desktop access solutions (e.g., Remote Desktop Protocol) are provided to permit authorized users access to computers located on-campus from an off-campus location.

- Use of unauthorized third-party remote desktop services (e.g., gotomypc.com, logmein.com) is strictly prohibited unless the service utilizes Enterprise Directory Services and 2FA for Authentication. Authorized Users must never install or configure unapproved Remote Desktop solutions on their University Device that permits connections from other devices.

- Remote Desktop access is provided for both personal devices and University devices.

- Remote Desktop access, or similar secure, approved solutions, must be utilized when a personal device is the only option available to conduct Privileged Access to a University Information System.

- Remote Desktop access screen must be configured to lock and require user to re-authenticate if left unattended for more than 15 minutes.

- After no more than 180 minutes of inactivity, Authorized Users must automatically be signed out of Remote Desktop access and must reauthenticate.

University System of New Hampshire

SSH (Secure Shell) Remote Access:

Secure Shell is a network protocol used to access a remote machine or to execute commands on a remote machine. It provides secure encrypted communications between two hosts over an unsecured network. It is critical that remote access services are protected and implemented in such a way that does not put USNH resources at risk.

The following requirements do not apply to sessions where access occurs from one campus to another, or where access is restricted to trusted hosts.

- Inbound SSH Access is limited to USNH networks and specific use cases. To request direct inbound SSH Access without the use of the USNH VPN, please submit a security exception request.
- Recognized best practices must be implemented to secure the SSH server against unauthorized access, such as firewalls and other network-based access controls. Additional examples may include but are not limited to requiring certificate and password authentication, deny-by-default firewall rules, active denial of hosts performing brute-force attacks, and disabling remote login for a superuser account.

Third Party Remote Access:

- Vendors and contractors must have a USNH Sponsored Account to utilize USNH remote access solutions.
- All third parties must adhere to all USNH policies and standards.
- All third parties granted remote access to USNH technology resources are responsible for ensuring the external networks used to access the USNH network are secure.
- USNH does not guarantee a remote access connection to the USNH network to any third-party.
- Connections provided to third parties will be based on the principle of least privilege to conduct business relative to the contractual relationship established.

Telecommuting and Remote Work Guidance - Telecommuting permits authorized employees to work at an alternative location for all or a portion of the work week. The telecommuting policy outlines conditions applicable to employees working in alternative locations, including compliance, work schedules, compensation, use of equipment and materials, expenses, and confidentiality. Please contact your supervision for guidance on telecommuting policies. Information can be found at: https://www.usnh.edu/human-resources/flexible-work-arrangements

Exceptions - Any exceptions to this Standard must be approved through the USNH ET&S Cybersecurity exception process.

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

Definitions

Remote Access is any access to USNH's network from an external, non-USNH network.

User includes anyone who accesses and uses USNH's information technology resources.

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

3. CONTACT INFORMATION

For USNH community members: Questions about this standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, & Compliance (GRC) via this Support Form.

A community member may submit other requests here: Submit an IT Question.

4. DOCUMENT HISTORY

Effective Date: October 14, 2022
Drafted: Dave Yasenchock. October 14, 2022, v01
Revised, USNH Cybersecurity GRC Standards Committee, October 14, 2022
Reviewed by: Dr. David Yasenchock, Director Cybersecurity GRC, October 14, 2022
Approved by: Thomas Nudd, Chief Information Security Officer, October 14, 2022