CHRISTOPHER NEWPORT
UNIVERSITY

Remote Access and Virtual Private Network Standard

VERSION 1.3

June 2023
Department: Information Security

Proprietary Statement

Review and Revision History

Date	Version	Description of Change (Affected Sections)	Author
August 2019	1.0	Initial Release - All	Wendy L. Murray
August 2020	1.0	Annual Review	Wendy Corrice
August 2021	1.1	Annual Review	Wendy Corrice
June 2022	1.2	Annual Review	Wendy Corrice
June 2023	1.3	Annual Review	Wendy Wilde

TABLE OF CONTENTS

Introduction:

In accordance with the Christopher Newport University Acceptable Use Policy, all systems owned or managed by the University must be adequately protected to ensure confidentiality, integrity, availability, and accountability of such systems. Virtual Private Networks may be used to establish secure connections from authorized external clients.

Purpose:

The purpose of this compliance standard is to define the tools and practices used for connecting to the University's information technology resources from any host remote to the University. The intent of this standard is to augment the established Telecommuting Policy and minimize the potential exposure to information technology and provide a clear understanding of the technology requirements of remote access. Remote access includes VPN, SSH, and any other technology that may be used to access the University's network remotely on or off-campus.

Scope:

This standard covers any authorized user of Christopher Newport University Information Technology Resources.

Standards Statement:

All Christopher Newport University employees and authorized third parties may utilize the benefits of the Virtual Private Network (VPN) to access University computing resources to which they have been granted access.

VPN gateways are set up and managed by Information Technology Services (ITS) infrastructure staff. No other department may implement VPN services unless approved by ITS.

All computers, including personal computers, connected to the Christopher Newport University internal networks via VPN or any other technology will use the most up-to-date anti-virus software and shall regularly apply critical patches to their computer's operating system.

To protect the integrity and security of data, ITS may require connecting to the VPN before using remote management applications such as Remote Desktop Protocol (RDP) or Secure Shell (SSH) to access a University IT service.

When actively connected to the University network, the VPN will force all traffic to and from the workstation over the VPN tunnel: all other traffic will be dropped.

Dual (split) tunneling is NOT permitted; only one network connection is allowed.

Communications on the University's computer systems may be monitored and/or recorded to ensure the effective operation of these systems and for other legal purposes.

The University reserves the right to monitor for unauthorized VPNs and disable access of those devices performing non-sanctioned VPN service.

VPN Accounts

A Virtual Private Network (VPN) connection is available to all employees and authorized third parties with a need to access resources internal to the campus network.

Accounts requests are made via a VPN Account Request Form and Help Desk Ticket submission at https://help.cnu.edu. The successful completion of online IT Security Training is required before users may download and install the VPN client software to their device. Third-party vendor account requests are made via a Vendor VPN Account Request Form and Help Desk Ticket submission at https://help.cnu.edu. Third party vendor accounts will have a signed copy of the request form forwarded to Procurement upon completion.

VPN access is controlled in accordance with VITA ITRM Information Security Standard (SEC501).

VPN account review shall be performed at a minimum of every 90 (ninety) days.

Telecommuting policy

Telecommuting permits authorized employees to work at alternative locations. 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. For more information on the Telecommuting Policy, Contact Human Resources.

Requirements

Secure remote access must be strictly controlled. Access will be controlled via account ID and password.

Users working with sensitive or confidential data must use GlobalProtect VPN Client.

The University may provide state-owned equipment and materials or authorize the use of personal equipment. It is the employee's responsibility that all possible measures have been taken to secure a remote access connection.

All hosts including personal computers (or other devices) connected to internal networks via remote access technologies must follow University policies and standards.

User Responsibilities

Users, including faculty, staff, students and other agents accessing information technology resources from a non-campus location must be authorized to access the data.

Users must ensure that unauthorized users are not allowed access to the Christopher Newport University campus networks.

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

By using VPN technology with personal equipment, users must understand that their machines are an extension of the institution's network and as such are subject to the same rules and regulations that apply to University-owned equipment.

Authorized users must submit a VPN Request Form to apply for VPN access to the University network.

Exceptions:

Exceptions to this standard will be handled on a case by case basis and approval of the Information Security Officer.

References:

VITA ITRM Information Security Standard (SEC501)

Virginia Department of Human Resource Management Policy 1.75 - Use of Electronic Communication and Social Media

Christopher Newport University Acceptable Use Policy

Christopher Newport University Telecommuting Policy

Christopher Newport University Virtual Private Network Policy - 6040

VPN Staff Account Request Form

VPN Vendor/Consultant Form

Review:

Next Review Date: June 2024