Christopher Newport University

Policy: Remote Access and Virtual Private Network Policy
Policy Number: 6040

Executive Oversight:	Vice President for Finance and Planning/CFO
Contact Office:	Information Technology Services
Frequency of Review:	Annually
Date of Last Review:	September 2021

A. PURPOSE

This policy establishes the terms of remote use for University communication and computing resources. These resources represent a substantial investment of public dollars. They are finite and intended to be used in support and advancement of Christopher Newport University's mission, purposes and activities by authorized users. Use of these resources is a privilege that is extended to employees, contractors and visitors pursuant to specific terms.

In addition, the University's information technology resources house significant confidential and otherwise sensitive information. The information and the resources themselves are critical to the operation of the University. Therefore, they must be secured at all times, and used only in a manner that maintains that security.

B. POLICY STATEMENT

Remote access to Christopher Newport's secure campus network shall be made available only to authorized users and limited to resources required to perform their job duties. Such remote access shall require the use of multi-factor authentication in addition to the university-issued User ID and password to connect to the network.

Access shall be made available only by authorized Virtual Private Network (VPN) service managed only by the Office of Information Technology Services (ITS) network staff, unless specific approval has been granted by ITS.

Users granted remote access must protect that access from use by any unauthorized individual or entity. Non-university owned equipment used to access the university network from remote locations must be configured to comply with all University policies.

Users are responsible for understanding and complying with this policy and the specifications listed on the VPN request form.

C. DEFINITIONS

Multi-Factor Authentication: Multi-factor authentication is an electronic authentication method in which a user is granted access to a website or application only after successfully presenting two or more pieces of evidence to an authentication mechanism

Remote Access/Virtual Private Network: Any connection that allows direct access to the secured campus network from outside the network, including the establishment of a VPN.

Secure Campus Network: Christopher Newport computer and communication facilities, equipment, systems and data, including all voice, data and video capability.

User: Employees, contractors, consultants, volunteers, and visitors authorized to use University communication and computing resources.

D. PROCEDURES

1. Requests for Remote Access

Include a copy of this policy with new requests for Remote Access.
Requests for remote access shall be submitted via the **Application for Virtual Private Network Services** form to ITS through the online Help Desk. Requests for VPN access must be reviewed and submitted by an employee's supervisor. All VPN requests must be reviewed and approved by a department head or their sponsor, and either the provost or a vice president prior to submission to ITS for approval, and shall explain the job-related need in support of the request.

Once an approved request is received and reviewed by the Information Security Officer (ISO), a VPN account shall be established for the user. All VPN access must be subject to user ID, password authentication, and multi-factor authentication.

Remote access may be granted on a temporary basis in which case the user shall be notified of the date upon which remote access will be reconsidered or withdrawn.

It is the responsibility of the user to ensure that only equipment using up-to-date virus scanning software, with virus definitions, shall connect to university secured networks via a VPN. Additional information about current security standards can be found on the IT Services campus knowledge base.

It is the responsibility of the user with VPN privileges to ensure that unauthorized users are not allowed access to university secured networks by use of their VPN.

2. Termination of Remote Access

When any user granted VPN privileges concludes the relationship with the University, Human Resources must notify ITS and ITS shall revoke any VPN access created for that user in accordance with the Employee Separation Clearance policy. For any other type of account, the sponsoring department head shall notify ITS when VPN access is no longer required and ITS shall revoke VPN access for that user.

When the duties of any user granted remote access change, the supervisor who approved the VPN request must notify ITS when remote access is no longer required by new duties.

3. Review

ITS shall annually review all VPN accounts and notify current supervisors of employees with VPN access. If VPN privileges are not being actively used (within the last 90 days), the supervisor shall be required to recertify the need for remote access.

These requirements shall be included and acknowledged with every request for remote access.

4. Enforcement

Any suspicious activity on the University's network accessed remotely by an authorized user may be subject to withdrawal of remote access and disciplinary action as appropriate to their employment status or other relationship with the University.

Any authorized remote user whose access results in damage to the secure network may be held financially responsible for that damage.

Any violation of this policy may result in termination of remote access, at the discretion of the Information Security Officer, regardless of the consequences of termination of remote access on the user's ability to accomplish job duties, and termination of remote access shall not excuse a failure to perform job duties.

E. REFERENCES

VITA SEC 501- IT Information Security Standard

https://www.vita.virginia.gov/it-governance/itrm-policies-standards/

VITA SEC 501 AC-17 – Remote Access

CNU IT Services Security Standards (https://confluence.cnu.edu)

- Remote Access and Virtual Private Network Standard
- Virtual Private Network (VPN) Account Guidelines

F. APPROVAL AND REVISIONS

Approved By: Policy Committee, November 29, 2017

Revision 1: Policy Committee, March 22, 2019
Revision 2: Policy Committee, March 4, 2020
Revision 3: Policy Committee, August 2021
Revision 4: Policy Committee, September 8, 2021

G. NEXT REVIEW DATE: Fall 2022