A. PURPOSE

This policy establishes the terms of 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 students, employees, contractors and visitors upon specific terms.

B. POLICY STATEMENT

Remote access to Christopher Newport University’s secure campus network shall be made available only to users who require it in order to perform their job duties. Such remote access shall require the use of the university-issued User ID and password authentication to connect to the network. Access shall be made available only by Virtual Private Network (VPN) service.

VPN services shall be set up and managed only by the Office of Information Technology Services (ITS) network staff, unless specific approval has been granted by ITS.

Remote access shall be limited to only those resources needed to perform job duties. Users are responsible for understanding and complying with this policy and the specifications listed on the VPN request form.

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.

C. DEFINITIONS

Secure Campus Network: Christopher Newport computer and communication facilities, equipment, systems and data, including all voice, data and video capability.
**User**: Employees, students, contractors, consultants and visitors authorized to use University communication and computing resources.

**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.

**D. PROCEDURES**

1. **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. Employee requests must be reviewed and approved by the employee’s supervisor prior to submission, and shall explain the job-related need in support of the request. Non-University user requests must be reviewed and approved by a University sponsor (department head) prior to submission, 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 and password 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.

   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.

   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, ITS must be notified and shall revoke any VPN access created for that user. For non-employee accounts, 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 current supervisor must notify ITS when remote access is no longer required by new duties.
3. **Review**

ITS shall annually review all VPN accounts. If VPN privileges are not being actively used, 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 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

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

G. **NEXT REVIEW DATE:** Spring 2021