VERMONT TECH

Manual of Policy and Procedures

Title: **Virtual Private Network (VPN)**	*Number:* **T 126**	*Page(s):* **3**
	Date: **February 18, 2020**	

PURPOSE

The purpose of this policy is to establish and communicate requirements for creating and using Virtual Private Network (VPN) connections to and from the VTC network in order to ensure that confidential information remains private over non-trusted networks. This policy applies to all computer devices including personal computers, handheld computers, smart phones, and other mobile devices that access the internet.

STATEMENT OF POLICY

What is VPN:

A Virtual Private Network (VPN) creates a secure, encrypted pathway between you and the school's network. While connected to our VPN, all of your activity is securely routed through our server and onto our network, so your device will act as if it were on-campus.

Why use the VPN:

If you are working remotely off-campus and need to access college resources that are only available internally, you will need to connect into the VPN. Additionally, any time that you are connected to a public network and are conducting college business, you will need to be connected to the VPN to create a secure tunnel to protect VTC data. Being on our network will provide you the benefits associated with being on our network, including our secure firewalls and other anti-malware protocols to prevent access to malicious sites.

Access Guidelines:

VPN access can be requested by submitting a support ticket to helpdesk.vsc.edu. Approval of access will be reviewed by the Chief Technology Officer and with the direct supervisor and/or faculty member when appropriate. Review of who has access to VPN will be reviewed on a semester-to-semester basis, with removal of access rights being possible due to any security concerns. This policy will need to be reviewed and signed by the user prior to getting VPN access.

Guidelines for Using the VPN:

- Practice safe computing:
    - Since it will allow others onto our network, it is important that you do not leave your device unsupervised while connected to the VPN. Lock your computer every time you leave your device.
    - If you are connecting to the VPN from a personal device, you are required to keep your device up-to-date, including operating system patches and security software such as anti-virus software. By using VPN technology to access VTC's network, users must understand that their computers are an extension of the network and must, therefore, be configured in accordance with all applicable information security policies. Please reference our mobile policy, found here, for best practices on mobile device management.
- Work responsibly:
    - Remember that everything you do while connected to the VPN is routed through the college's network, so please work responsibly and work as if you were on campus.
- Connect before you start working:
    - Connecting to the VPN will disrupt normal network activity for a moment. Make sure to connect to the VPN before working to prevent any disruption.
- Disconnect when not in use:
    - When you are done working, it is important to remember to disconnect from the VPN.
- This policy aligns with other VSCS policies: Data Security and Operational Policies. Please visit the associated link for more information on security policies and best practices.

Enforcement:

Violation of any of the constraints of this policy or procedures will be considered a security breach and may be subject to discipline as outlined in the employee and student handbooks. Additionally, individuals may be subject to the loss of resources and access privileges.

Please note that while gaining VPN access supports remote work, including working from home, approval of gaining access to VPN *does not* signal official approval to work from home. Please reference Policy T 218 Work Outside Normally Designated Locations (NDL) for further information on process for requesting permission to work from home.

In signing this document, you:

- Understand and agree to this policy and the guidelines outlined above.

_____

Signature (printed), Date

_____

Supervisor Signature (printed), Date

POLICY MODIFICATION HISTORY

I. The following dates reflect chronological changes made to this policy which are henceforth considered depreciated.

a) Enacted 2/18/2020

Signed By: Patricia Moulton
President