FREDONIA
STATE UNIVERSITY OF NEW YORK

Fredonia Virtual Private Network (VPN)
Service Application

Fredonia provides Virtual Private Network ("VPN") Services for employees required to remotely and securely perform work related duties from off-campus, as approved by his/her supervisor, and as necessary in accordance with applicable New York State and SUNY policies and regulations. Fredonia provides two types of VPN remote access methods used to access campus-based IT services:

- **General (Web) -** The SSL VPN Web portal enables remote users to access internal network resources through a secure channel using a web browser. This access method is for the general user that has standard remote access needs. The services are delivered within a modern HTML5 compatible web browser.
- **Advanced (Client)** - The Fredonia VPN Client enables remote users to access internal network resources through a secure tunnel delivered by the end-user installed Fortinet software. This method is designed for users with more advanced needs and will be made available on a case-by-case basis based on business needs.

Services provided by the General (Web) and the Advanced (Client) VPN include the following:

- Hypertext Transfer Protocol (HTTP)
- Hyper Text Transfer Protocol Secure (HTTPS)
- Virtual Network Computing (VNC)
- Remote Desktop Protocol (RDP)
- Secure Shell (SSH)

Fredonia VPN Services are provided to allow approved employee access to University electronic resources when remote work-related business functions are necessary. Employees with Fredonia VPN Service privileges understand and agree to the following:

- It is the employee's responsibility to select, coordinate the installation of, and pay the associated fees for high-speed Internet connectivity via a local Internet Service Provider (ISP).
- It is the employee's responsibility to ensure that unauthorized users are not allowed access Fredonia internal networks via the VPN.
- VPN use maybe controlled using multi-factor authentication.
- Only the Information Technology Services (ITS) approved and configured VPN client may be used for the Advanced (Client).
- Support and connectivity issues related to VPN access are provided by ITS.
- VPN accounts will be annually audited and users no longer requiring VPN access will have such access removed.
- Access may be allowed from either state-issued or personally-owned devices. Such access must be limited to only those systems necessary to meet the required remote business functions.

Please list the University systems, services or applications you are requesting remote access to:

_____

Please complete and return this application to the Information Security Office, 117 Maytum Hall (716) 673-4725.

Name of Individual Requesting VPN Access (Print)	Department Name
Individual Requesting VPN Access Signature	Date
Approving Supervisor's Name (Print)	
Approving Supervisor's Signature	Date
Information Security Officer's Approving Signature	Date