Virtual Private Network (VPN) Service Requirements

Effective Date: 2/19/2019
Responsible Officer: Charles Bartel, Vice President and Chief Information Officer

Purpose:

Remote connectivity to campus is a critical tool for our community and its members. Computing and Technology Services (CTS) provides a Virtual Private Network (VPN) as a method of securing communications between your computer and the University network from home, business travel locations, conferences, or other non-work locations using public internet. The need to keep remote access secure for authorized users is a critical component of the campus VPN. These Service Requirements apply to all users of technology and associated processes at Duquesne.

Service Requirements related to VPN Access:

1. VPN connections are only permitted from institutionally managed machines that are maintained for patches, updates, and endpoint protection.
2. Installation of the VPN will be performed by a member of CTS.
3. Devices that require VPN connectivity must connect to the campus network at least once every 90 days.
4. VPN users must be approved by your department/division Dean/VP as well as the Chief Information Office (CIO).

The unauthorized or improper use of Duquesne University’s technology environment, including the failure to comply with these service requirements, constitutes a violation which may result in the loss of access, university disciplinary actions and/or legal prosecution under federal, state and local laws, where applicable. Users are expected to adhere to T.A.P. 26 - Computing and Ethics Guidelines which can be found at http://www.duq.edu/taps.

The University reserves the right to amend these service requirements at any time without prior notice and to take such further actions as may be necessary or appropriate to comply with other published policies and with applicable federal, state, and local laws.