DUQUESNE UNIVERSITY
Computing and Technology Services

Information Security Remote Access Service Requirements

Effective Date: 1/5/2023
Responsible Officer: Charles Bartel, Vice President and Chief Information Officer

The following security requirements, which defines secure remote access and the required tools and practices, is intended to ensure that remote access to the Duquesne University network and restricted data (Defined in the CTS Data Governance Service Requirement) is performed in a secure fashion.

- Comply with Duquesne University policies and procedures as well as federal, state, and local laws.
- If accessing restricted data, a university owned and managed device must be used. Personal devices are not permitted to access or use restricted data.
- Remote access is restricted to approved technology provided by Computing and Technology Services (CTS). This includes the university virtual private network (VPN) or SSH Secure Gateway. These systems require MultiPass accounts and Multifactor Authentication.
- Access to university web sites and web services must be protected with the latest supported and secured TLS encryption.
- Secure Shared Storage must be used when working with Restricted Data: Details are listed on the CTS Storage Services website. Duquesne University Data may not be stored on your local workstation, or on any portable media (e.g., USB key, CD, DVD, external hard drive, etc.)

- Maintain good information security practices:
  - Never put Restricted information in email
  - Never transfer Restricted University data via email, USB, CD, or other portable media unless encrypted
  - Keep your computer updated with the latest security patches; set automatic updates for Windows, Apple and other critical application patches
  - Install and leverage endpoint protection provided by CTS, such as Sophos Intercept X Endpoint Detection and Response (EDR)
  - Follow the CTS password and credential service requirements.
  - Don't click on suspicious links in emails or download unapproved software
- Protect University computers and laptops:
  - Don't leave your laptop unattended
  - Lock down screens or log off before leaving your computer
  - Ensure that your PC/laptop is physically secured
  - Be particularly careful with laptops when travelling
  - Encrypt mobile devices where possible and supported by CTS
- Be familiar with and comply with policies pertaining to all data you will work with, such as:
  - TAP 26 Acceptable Use of Computing Resources

- TAP 28 Family Educational Rights and Privacy Act (FERPA)
- TAP 39 Records Retention Policy
- CTS Service Requirements

By connecting and utilizing the Duquesne University Remote Access solutions such as the University Virtual Private Network (VPN) or SSH Gateway you agree to comply with the above requirements.

Enforcement:

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 https://duq.edu/tap-26.

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.

Revision Date	Reason for Change	Author
10/5/2022	Updates to policy	Tom Dugas, Chief Information Security Officer (CISO)
1/5/2023	Updates to Website Links	Tom Dugas, Chief Information Security Officer (CISO)