INFORMATION SECURITY REQUIREMENTS FOR REMOTE ACCESS

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. By signing below, the employee agrees to comply with all applicable stated requirements.

- 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.
- A virtual private network (VPN) connection must be established during the off-site remote access of restricted data, to insure all exchanges of sensitive information are encrypted. (An exception to this is individual access to Banner Self Service, which is granted by default to all faculty, staff and students for web based self-service processing.)
- Always use Secure Shared Storage: All data must be stored on approved secure storage such as Einstein, CIFS or Office 365 OneDrive.
- 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.)
- All data and work product used and created while engaging in telework is the sole property of the University.
- Understand and comply with special requirements pertaining to authorized usage of Personally Identifiable Information.
- Never transfer Restricted University data via email, USB, CD or other portable media.
- Maintain good information security practices:
    - Never put Restricted Data in email.
    - Never put Restricted Data on USB, CD or other portable media.
    - Keep your computer updated with the latest security patches and antivirus definitions; set automatic updates for Windows and other critical patches.
    - Use unique strong passwords on all your computer systems.
    - Do not put Restricted or Internal Data on portable media (e.g., USB key, CD, DVD, etc.).
    - Don’t click on unknown links in emails.
- 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 traveling.
- Be familiar with and comply with policies pertaining to all data you will work with, such as:
    - TAP 26 Computing Ethics and Guidelines
    - TAP 28 Family Educational Rights and Privacy Act (FERPA)
    - TAP 39 Records Retention Policy
    - TAP 40 Intellectual Property Policy
    - CTS Data Governance Service Requirement
    - CTS Information Security Service Requirement
    - CTS Password Service Requirement

I have read and agree to comply with the above requirements.

_____	_____
Employee Signature	Date
_____	_____
Supervisor Signature	Date
_____	_____
Dean/Department Head/AVP	Date
_____	_____
CTS	Date