Remote Access Policy
TEC 12.0

Office of Information Technology

Policy type: Administrative
Applies to: Faculty, staff, student employees, students, vendors, and volunteers

POLICY DATES

Issued: 9/16/2019
Revised Last: 4/07/2023
Edited by: Tina Stuchell
Reviewed: 4/07/2023

University of Mount Union recognizes the need of its students, faculty, and staff to access university data when they are not physically on campus. The purpose of this policy is to state the requirements for remote access to computing resources and data hosted at the University of Mount Union using Virtual Private Network (VPN) technology. The use of a VPN allows members of the UMU community to securely access UMU network resources from off campus as if they were on campus.

The Purpose of this policy is to maintain and protect the university informational and computing assets and comply with applicable federal and state legislations. These guidelines are to define baseline security controls for protecting institutional data. Security breaches are more commonplace than ever, and universities continue to be popular targets for attacks. Critical university resources, such as research, business transactions, and student and employee personal data must be protected from intrusion and inappropriate use or disclosure. Devices must be set up and routinely maintained and updated so that they prevent intrusion and other malicious activities.

This policy is reviewed on an annual basis and any changes are process through the Policy Review Committee (PRC). Major changes to this policy must be approved through President Council.

Definitions

Term	Definition
Remote Access	For the purpose of this policy, remote access is defined as any faculty, staff, student, consultant, vendor or any third-party affiliate connecting to the University of Mount Union network using a non-university-controlled network, device or service.
Virtual Private Network (VPN)	VPN is a secured private network connection. It provides a secure encrypted connection, or tunnel, over the Internet between an individual computer/device and a private network.
Information System	Is generally defined as any electronic system that stores, processes or transmits information. For the purpose of this policy, it is any electronic system that stores, processes or transmits institutional data.
Institutional Data	Is defined as any data that is owned or licensed by the University.
Multi-factor Authentication	The process by which more than one factor of authentication is used to verify the identity of a user requesting access to resources. There are three common factors of authentication: something you know (e.g. Password, pin, etc.), something you have (e.ge. smart card, digital certificate, etc.) and something you are (e.g. fingerprint, retinal pattern, etc.). Use of username and password combination is considered single factor authentication, even if multiple passwords are required. Username and password used in conjunction with a smartcard is two-factor authentication. Multi-factor authentication represents the use of two or three factors.
Confidential Data	Institutional data that is not to be released under any circumstance is to be protected. It can include but is not limited to PII data, credit card data, social security numbers, grades, bank account numbers, or any other information that is likely to raise public interest.
Bank Account Numbers	Any routing or identification numbers that can be used to determine banking information including both institutionally owned and University agent owned account information.

Applies to: Faculty, staff, student employees, students and volunteers

Term	Definition
Personal or Private Identifiable Information (PII)	Any information that could be used in the process of identity theft.
Directory Data	Defined per The Family Educational Rights and Privacy Act (FERPA) as information such as a student's name, address, telephone number, date and place of birth, honors and awards, dates of attendance.

Policy Details

This policy provides the security requirements for all University of Mount Union employees, students and contractors who are manipulating and accessing university data classified as confidential from remote locations. This policy does not apply to authorized and authenticated access to email (thru Webmail/OWA/Office365), Learning management system, self-service, and/or any university publicly accessible websites.

Privacy practices and security standards serve to preserve and protect institutional information. This policy incorporates a set of requirements for protecting the University's institutional information. The purpose of this policy is to ensure that all individuals within its scope understand their responsibility in reducing the risk of compromise and take appropriate security measures to protect university resources. Access to university resources is a privilege, not a right, and implies user responsibilities. Such access is subject to university policies (including Acceptable Use, Information Security Policy, etc.), standards, guidelines and procedures, and federal and state laws.

To safeguard the university's institutional information, the following practices for remote access include:

- All employees must have requested access and have been given approval for access by area Vice President and Director of IT for Security on an annual basis. Applications deadline is August 31st of each year.
- All students must have requested access and have been given approval for access by the Director of IT for Security. Student access must be granted on an annual basis.
- Any vendor accounts accessing on-premises systems must use VPN and have had appropriate approval access granted. Vendor VPN access must be approved on an annual basis.
- All individuals and machines connecting remotely must comply with university policies.
- All individuals connecting remotely shall only connect to or have access to machines and resources they have permission and rights to use.
- All devices connecting remotely shall have current anti-virus software and all operating system and applications updates and patches. Firewalls should be enabled if possible.
- UMU employees and authorized third parties using the VPN must ensure that unauthorized users are not allowed access to internal university networks and associated information/data.
- The use of personal or home machines when accessing confidential, financial or PII information of the University is strictly prohibited.
- The user is approved by the department and the university to work remotely.
- All reasonable efforts are made to protect university data.
- Users who connect remotely to the University systems that contain confidential/restricted data re required by university policy to use the campus VPN to maintain security of university data.
- Any remote access users who are utilizing the remote connection should remain connected for only as long as necessary to conduct business related work for the university.
- At no time is a remote user to remain connected for more than 12 continual hours.
- At no time is a remote user to connect to UMU 's network to any other network or device beyond the initial device making the connection. This includes, but is not limited to split tunneling, dual homing or otherwise re-routing UMU's traffic beyond the intended endpoint.
- Remote access users are not permitted to download or otherwise store university data which is considered confidential or contains Personally Identifiable Information (PII) on their personal remote computing devices. This

includes the transfer of such data to a personal cloud service such as Dropbox or Google Drive. Please see the Information Security Policy for additional information.

- Remote access users agree to immediately report to UMU any incident or suspected incidents of unauthorized access and/or disclosure of company information.
- Any device connecting to UMU's computing resources is subject to monitoring, which may include but is not limited to date, time, duration of access, identification of endpoint and all traffic which traverses the network.
- Users needing access to their work desktop machines, or who need wider access to campus resources, must use the VPN in conjunction with an approved remote access application. The need and intended use for this type of access must be clearly defined in the application for remote access.
- VPN access is reviewed weekly and any activity outside of normal business hours (6am-10pm, MTWTHF) will be reviewed and discussed with employee and area VP.

The Director of IT for Security is responsible for documenting and implementing controls for all remote access methods implemented with the university and is also responsible for monitoring remote access methods for unauthorized use and taking appropriate action upon discovery of unauthorized use including notification of such information to the Incident Response Team. Employment at UMU does not automatically guarantee the granting of remote access privileges. Remote access privileges must be approved and maybe revoked at any time. Director of IT for Security is responsible to oversee vendor VPN access and monitoring of vendor access.

The area Vice President and Director of IT for Security is responsible for approval of remote access requests. The Director of IT for Security is responsible for maintaining log files related to these requests.

Procedure Details

In order to support this policy, the following procedures have been put in place.

1. Individuals can request Remote Access/VPN by completing the Technology Remote Access Request Form located on Ellucian Experience under forms and then technology.
2. Requests will be reviewed and notification of approval or denial from the Director of IT for Security will be completed within 5-7 days.
3. All requests will be logged and managed within the Office of Information Technology.
4. All requests must be renewed on an annual basis by completing the Technology Remote Access Request Form prior to August 31st of each year.
5. Any activity outside of normal business hours (6am-10pm, MTWTHF) will be viewed on a weekly basis by network services. Abnormal activity will be discussed and reviewed with the employee and area VP.
6. Logging and monitoring of remote access activity is to be completed on a regular basis (monthly). This includes access by faculty, staff, students and third-party vendors.

Responsibilities

Position or Office	Responsibilities
Office of Information Technology	Update of Policy & Protection of Data
Users of Data	Protecting institutional data
VPs, Deans, Directors, Department Heads, Supervisors	Implementation of this policy within their respective units.
Director of IT for Security, VP Business Affairs & CIO	Oversight of information security

Applies to: Faculty, staff, student employees, students and volunteers

Contacts

Subject	Office	Telephone	E-mail/URL
	Office of Information Technology	330.823.2854	**IT@mountunion.edu**

History

This policy was established in 2019 part of GLBA compliancy efforts.

All changes must be listed sequentially, including edits and reviews. Note when the policy name or number changes.

Issued:	9/16/2019
Revised:	4/07/2023
Edited:	Tina Stuchell
Reviewed:	4/07/2023