Mobile Device Policy
TEC 1.0
Office of Information Technology

Policy Type: Administrative
Applies to: Faculty, Staff, Student Employees, Students and Volunteers

POLICY DATES

Issued: 7/1/2015
Revised: March 26, 2020
Edited by: Tina Stuchell

It is the policy of the Office of Information Technology of the University of Mount Union that if you are obtaining your Mount Union email or storing Mount Union data on your personal mobile devices or an institutional owned device, you must comply with the rules and guidelines found below.

Definitions

Term	Definition
Mobile Devices	Devices with mobile access plans for connection, such as mobile phones, including iPhones, Android phones, Window Mobile operating system, etc., Tablets such as Chrombooks, iPads, Surfaces, etc. Laptops.

Policy Details

Mount Union data, including email, stored on a mobile device is the property of Mount Union and must be kept secure.

It is recommended that you keep limited amount of Mount Union data on your device and delete data periodically. If your device has an option to automatically delete data periodically, enable that option. It is also important to take advantage of the antivirus software if it is available for your devices. It is also recommended to encrypt the data if possible.

You are also required to secure the device with a complex password. Set up of the device for connection to the University's email is unique for each type of device. Therefore, the Office of Information Technology cannot give exact instructions for setup, however, does provide general instructions within iRaider to assist with setup. It is also required to have dual authentication, also known as two factor authentication configured.

Under no circumstances should personal identifiable information (PII) or confidential information be stored on a mobile device. PII information is any information that can be used to identify an individual which can include name, social security numbers, bank account numbers, mother's maiden name, date and place of birth or biometric records.

PROCEDURE

You must secure the device with a complex password and/or biometric authentication. It is recommended that both forms are used to provide a backup mechanism if biometric authentication fails. A complex password is something that contains a mix of:

- Capital and lowercase letters
- Numbers (At least 6 numbers if using a PIN)
- Symbols (if supported by your device)
- Do not use names, birthday, etc.
- Biometric
- Facial Recognition
- Fingerprint Recognition

Mobile Device Policy

TEC 1.0

Office of Information Technology

Applies to: Faculty, Staff, Student Employees, Students and Volunteers

You must contact the Office of Information Technology immediately if your device is lost or stolen by contacting the IT Helpdesk via phone or email. The office also retains the right to remotely wipe the device to destroy all data. *Note: This wipe will include personal data including pictures, apps, contacts, etc.

It is required that you set and use automatic security features for your device, such as automatic lock, encryption, etc. Dual authentication/2FA is also required.

All portable devices will contain institutional data when connected to the University's email system. This data must be treated the same as if it resides on an institutionally owned device, therefore you must also comply with the these additional institutional policies.

- Information Security Policy
- Information Privacy Policy
- Technology Resources Acceptable Use Policy
- Data Incident Response Policy
- Additional policies, all policies can be found in iRaider and on the Mount Union public web site.

The Office of Information Technology minimally supports personal mobile devices.

Responsibilities

Position or Office	Responsibilities
Information Technology	

Contacts

Position	Office	Telephone	E-mail/URL
Executive Director of IT & CIO or Director of IT for Security	Information Technology	(330) 823 – 2854	IT@mountunion.edu

History

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

Revised: March 26 2020

Edited by: Tina Stuchell

Reviewed: Mach 26 2020