Information Security Policy
TEC 4.0

Office of Information Technology

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

POLICY DATES

Issued: 2/8/2011
Revised Last: March 2019
Edited by: Tina Stuchell
Reviewed: March 2020

University of Mount Union expects all institutional information stewards who have access to and responsibilities for institutional information to manage it according to the rules regarding storage, disclosure, access, classification of information as set forth in this policy.

The Purpose of this policy is to maintain and protect the university informational 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.

Definitions

Term	Definition
Electronic Storage Media	Is defined as any electronic device that can be used to store data. This includes but is not limited to internal and external hard drives, CDs, DVDs, Floppy Disks, USB drives, ZIP Disks, Magnetic tapes, SD Cards, etc.
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.
Least Privilege	Is information security principle whereby a user or service is provisioned the minimum amount of access necessary to perform a defined set of tasks.
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.
Privileged Access	Is defined as a level of access above that of a normal user. This definition is intentionally vague to allow the flexibility to accommodate varying systems and authentication mechanisms. In a traditional Microsoft Windows environment, members of the local administrators, domain administrators and enterprise administrator's groups would all be considered to have privileged access. In a traditional UNIX or Linux environment, users with root level access or the ability to sudo would be considered to have privileged access. In an application environment, users with "super-user" or system administrator roles and responsibilities would be considered to have privileged access.
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
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

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, standards, guidelines and procedures, and federal and state laws.

To safeguard the university's institutional information, the following practices for electronic transmission and storage of confidential information. All institutional data must be protected in a reasonable and appropriate manner based on the level of sensitivity, value and/or criticality that the data has to the University. This requirement acknowledges that different types of data require different sets of security controls. The University has defined three classifications of data for this purpose: Confidential, Restricted and Public.

This policy establishes three institutional information security classifications:

1. Confidential (Level 1) Data
2. Restricted (Level 2) Data
3. Public (Level 3) Data

Unless otherwise classified, all information used in the conduct of university business is restricted (Level 2). Institutional information that has been explicitly made available to the public, with no authentication required is public (Level 3).

Confidential (Level 1) Data

Confidential Data: Data should be classified this way when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the university or its affiliates. The highest level of security controls should be applied to confidential data. Examples of confidential data include data protected by state or federal privacy regulations and data protected by confidentiality agreements.

- Social Security Number
- Credit Card Number
- Driver's License Number
- Bank Account Number
- Protected Health Information, as defined by the Health Insurance Portability and Accountability Act (HIPPA)

Restricted (Level 2) Data

Restricted Data: Data should be classified this way when unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the university or its affiliates. By default, all institutional data that is not explicitly classified as confidential or public data should be treated as restricted data. A reasonable level or security controls should be applied to restricted data.

Public (Level 3) Data

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would result in little or no risk to the University and its affiliates. Examples of public data include:

- Press Releases
- University Catalog Information

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

- Research publications

While little or no controls are required to protect the confidentiality of public data some level of controls is required to prevent unauthorized modification or destruction of public data.

Data Storage:
Institutional data storage can be separated by the type of data. For example:

- Credit Card Data may not be stored anytime, in any format written or electronic, under any circumstance by any application or user on Mount Union Campus. Credit Card Processing can only be completed by authorized merchants as defined by the VP of Business Affairs and Controller. Those accepting credit card information must follow guidelines established by the controller and comply with Credit Card Security Policy.
- Social Security Numbers and grades when required to be stored can only be stored on encrypted server drives. It is not to be stored on USB drives, or other mobile media, including mobile devices such as laptops or tablets. Under no circumstances should Social Security Numbers be included in reports and distributed to others.
- Bank Account Numbers must only be stored by agents who require that information and when needed should only be stored encrypted when in digital formats and should be locked and have physical access limited in non-electronic media formats.
- Confidential Data should never be stored on non-university owned systems including personal laptops, desktops, tablets or phones regardless of security settings. Confidential information may only be stored when required business use and then must be stored in secured formats or locations.
- PII when stored must be encrypted if in electronic format. If stored in non-electronic media, it must be physically secured with limited physical access.

Any other institutional data must always be stored in encrypted format.

Data Collection:
The collection of the *social security number* by any agent of the university and its use as an identifier must be avoided, except as required by law.

The collection of *credit card* data must be avoided except where required for transaction purposes and where agents of the institution have been authorized to do so, and only in locations as specified by the Credit Card Security (PCI) Policy. Credit Card data is not be collected by any departments or divisions not explicitly defined in the credit card security policy and approved by the controller of the university.

The collection of *bank account numbers* must be avoided when possible. When necessary it must only be collected by the Office of Business Affairs.

Data Release:
Confidential Data including PII data should never be released, including via email, social media, fax, etc.

Directory Data may be released public without consent, given the university has told the relevant parties about the data and given them a reasonable amount of time to inform the University to not disclose directory information. Per FERPA this must be completed once a year.

The need-to-know email lists are used in order to notify offices of data that must be modified in systems across the institution. The data that is passed, such as address changes, title changes, student withdraw, employee leaving the institution, etc. should not be shared with others and only used in order to perform ones job.

Data Moving:
To limit the impact of improper or accidental moving of data various procedures have been put in place including limiting access and permissions only as required, implementation of shadow volume copy and other backup procedures. And Mount Union data stored on USB drives must be stored/transported using encrypted thumb drives. Data should only be moved by those authorized for such purposes. Examples include:

- Backup purposes

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

- Validation/testing of data for support purposes.

Data Deletion:
When disposing of any confidential data in paper form, all data must be shredded in a cross cut manner. The university currently has several shred it boxes located around campus that must be used for this purpose, if additional locations are needed it is the responsibility of the department to obtain this service through the business office and any associated costs. In 2020 there were an additional eleven Shred N Protect boxes added to the campus.

Confidential electronic data to be destroyed should be destroyed in a manner that completely removes the data from the physical media it is located on. If unsure how to accomplish this obtain assistance through the Office of Information Technology.

Physical media that once had the potential to contain confidential data should be completely destroyed, various methods might include but are not limited to include degaussing. The Office of Information Technology had a degaussing machine.

To limit the impact of improper or accidental deletion of data various procedures have been put in place including limiting access and permissions only as required, implementation of shadow volume copy and other backup procedures.

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.
VP Business Affairs & Director of IT, Assistant Directors of IT	Oversight of information security

Contacts

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

History

This policy was established in 2000, last modified in 2011 part of the PCI compliancy efforts and was placed into the new format in 2016.

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

Issued: 2/8/2011
Revised Last: March 2019
Edited by: Tina Stuchell
Reviewed: March 2020