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 2021
Edited by: Tina Stuchell
Reviewed: March 2021

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.

This policy is reviewed and updated on an annual basis by the CIO & Director of IT for Security. This is an administrative type of policy which all changes to this policy must be approved by President Council and Policy Review Council.

Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Electronic Storage Media</td>
<td>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.</td>
</tr>
<tr>
<td>Information System</td>
<td>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.</td>
</tr>
<tr>
<td>Institutional Data</td>
<td>Is defined as any data that is owned or licensed by the University.</td>
</tr>
<tr>
<td>Least Privilege</td>
<td>Is information security principle whereby a user or service is provisioned the minimum amount of access necessary to perform a defined set of tasks.</td>
</tr>
<tr>
<td>Multi-factor Authentication</td>
<td>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.g., 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.</td>
</tr>
<tr>
<td>Privileged Access</td>
<td>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.</td>
</tr>
<tr>
<td>Confidential Data</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------</td>
<td>------------</td>
</tr>
<tr>
<td>Controlled Classified Information (CUI)</td>
<td>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.</td>
</tr>
<tr>
<td>Bank Account Numbers</td>
<td>Any routing or identification numbers that can be used to determine banking information including both institutionally owned and University agent owned account information.</td>
</tr>
<tr>
<td>Private Identifiable Information (PII)</td>
<td>Any information that could be used in the process of identity theft.</td>
</tr>
<tr>
<td>Directory Data</td>
<td>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.</td>
</tr>
<tr>
<td>NIST Special Publication 800-171 Environment</td>
<td>NIST is a Federal standard that standardizes security controls applied to CUI and systems and processes involved with this data within federally-funded environments.</td>
</tr>
<tr>
<td>NIST 800-171 Framework</td>
<td>Environment is defined as the systems upon which CUI resides and the physical infrastructure that houses systems. Examples might be a student records system residing on servers in a datacenter. The room(s) or area(s) housing the computer systems along with the computer systems themselves define the environments to which this policy applies.</td>
</tr>
<tr>
<td>Compensating Control</td>
<td>The NIST 800-171 framework consists of 110 elements covering administrative, technical, and operational security controls designed to focus on protecting the confidentiality of unclassified-but controlled information. Those controls are: Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Communications Protection. A compensating control is a mechanism that is put in place to satisfy the requirement for security measure that is deemed too difficult or impractical to implement at the present time. Compensating controls requirement need to mitigate the underlying risk that the requirement is designed to address. The Office of Information Technology will assist responsible parties regarding compensating controls.</td>
</tr>
<tr>
<td>PII</td>
<td>Personal Identifiable Information (PII) is any information about an individual maintained by an agency, including any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother’s maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information (including address).</td>
</tr>
<tr>
<td>GBLA</td>
<td>Gramm-Bliley-Leach Act – requires financial institutions, companies that offer consumers financial products or services to explain their information sharing practices to their customers and to safeguard sensitive data.</td>
</tr>
</tbody>
</table>

**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
- 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.
Information Security Policy

TEC 4.0

Office of Information Technology

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

- 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 TO 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 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 one’s 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
- 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 crosscut 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.
Information Security Policy
TEC 4.0
Office of Information Technology

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

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.

**Controlled Unclassified Information**

Controlled Unclassified Information is any information in any form that law, regulation, or governmentwide policy requires having safeguarding or disseminating controls. The University of Mount Union may receive data shared by the federal government or may create data or information as part of sponsored projects or to conduct federal business. This data, information and related documents may be classified as Controlled Unclassified Information (CUI). The University is obligated to ensure that all systems and processes involved with CUI are compliant with National Institutes of Standards and Technology (NIST) standard found in NIST Special Publication 800-171. This policy provides requirements and guidance so individuals in receipt or development of CUI can conduct research or other business in compliance with CUI regulation. Non-compliance may result in fines or the inability to continue receiving Federal funds associated with the use of this data whether directly received from the government or indirectly through associated covered contracts and contractors.

This policy applies to all data that is classified as CUI as well as technology, system, service, network, department, or personnel that transmit, process, or store CUI. It covers transmission of data and information that is transmitted in any manner, including electronic and paper. This policy applies whether the network connections are remote (cloud) or campus based.

Any person, department or college who handles CUI on behalf of the University must abide by this policy. This policy provides requirements and guidance for all use of CUI for the University. These are the minimum requirements for securing CUI. All environments involved with CUI must comply fully with the NIST 800-171 standards and this policy either directly or through compensating controls.

Individual users and departments must take actions to protect CUI from unauthorized disclosure and follow the requirements as specified in NIST 800-171. Periodic risk assessment to organizational operations, assets, and individuals, resulting from the operation of information systems and the associated processing, storage or transmission of CUI will be conducted. All environments that are involved with CUI must also operate in a manner that allows incident reporting within 72 hours of cyber incidents involving CUI.

Additional Resource: NIST 800171
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (nist.gov)

**Protecting Personal Identifiable Information (PII)**

Limit collection of PII
- Only collect what is needed for specific business purposes
- Limit the number of copies of reports, and files containing PII
- Every time you create: a form, application, survey, run a query, run a report or generate a file consider if all PII included is truly necessary
- Remember the less you collect the less you need to protect

Limit Use of PII
- Always remember Federal and State law limit the sharing of PII data
- Remember federal law, FERPA, requires written consent to disclose PII from education records unless an exception applies
- FERPA school official exception: PII may be disclosed without consent to other school officials only where there is a legitimate educational interest
- PII data can only be shared with third parties acting as school officials
- Remember to think before sharing data internally, consider if there is a legitimate educational interest and need.
Information Security Policy

TEC 4.0

Office of Information Technology

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

- Use fictional personal data for training and presentations
- Remember University policy requires that the sharing of data with external partners, vendors and servicers must be strictly controlled.
- Data required to be shared in the support of research, accreditors or third party surveys, even when aggregate data is requested, must be reviewed and discussed with the Office of Institutional Research.
- Always think twice before sharing PII.

Safeguard PII

- Safeguard PII data in all formats (this includes electronic and paper formats)
- PII must be protected at rest and in transit
- Data should be protected from loss or unauthorized access
  - Remember sharing of passwords is prohibited
  - Maintain strong passwords
  - Secure all paper containing PII including keep a clean desk and file documents containing PII in locked cabinets
  - Lock your computer screen when not in use
- Always email PII securely
- Always pick up print outs containing PII immediately
- Printers and copiers should be in an access-controlled environment
- PII should never be stored on unsecure/public computers, or portable devices (flash drives, phones).
- Shred paper containing PII in Shred Bins located throughout campus
- Delete/dispose of PII securely at the end of retention period

Governance of PII and its use is administered by the University’s Office of Information Technology with assistance from University Compliance Committee, Risk and Safety Committee and Cyber Security committee of the BOT. It is important that we remain vigilant about protecting the University’s information and compliance.

If there is a business need that requires PII information to be used outside of the University enterprise systems, or if you have concerns about the protection or use of PII, contact the Office of Information Technology.

GLBA Compliancy

Gramm-Leach-Bliley Act (GLBA) addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions such as banks and investment companies. GLBA contains no exemption for colleges or universities. As a result, educational entities that engage in financial activities, such as processing student loans, are required to comply. GLBA and other emerging legislation could result in standards of care for information security across all areas of data management practices both electronic and physical.

GLBA Compliance covers the entirety of the activities and practices of the following offices and individuals:

- Academic and administrative offices that handle electronic or printed personnel records, financial records, transactional records, or student records.
- Academic and administrative offices that transmit confidential information to off-site locations as part of a periodic review or submission requirement.
- Centers and Institutes that provides services and acquire personal or financial information from participants or constituents.
- Faculty serving as directors, coordinators, or program directors for programs collecting protected data.
- Faculty, staff and administrators with contracts to use, access, or provide protected data to or receive from a non-campus entity.

GLBA Compliance covers the following types of data:

- Personal Identifiable Information (PII) – also known as protected data, PII includes first and last name, social security number, date of birth, home address, home telephone number, academic performance record, physical description, medical history, disciplinary history, gender and ethnicity.
Information Security Policy

Office of Information Technology

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

- Financial Information – Information that the University has obtained from faculty, staff, students, alumni, auxiliary agencies, and patrons in the process of offering financial aid or conducting business. Examples include bank and credit account numbers and income and credit histories.
- Student Financial Information – Information that the University has obtained from a student in the process of offering a financial aid award, services or such information provided to the University by another's.

To continue to protect private information and data and to comply with the provisions of the Federal Trade Commission’s safeguard rules implementing applicable provisions of the GLBA, the University expects individuals to comply with this policy. This policy forms part of the overall strategic information security program. The University receives during business as required by GLBA as well as other confidential financial information the University has chosen to include within scope.

All University employees that interact with PII data during their daily activities are required to comply with GLBA regulations and take training course while handling the personally identifiable information (PII).

Network Security

Network attacks launched from the Internet or from the University’s network can cause significant damage and harm to information resources including the unauthorized disclosure of confidential information. To provide defensive measures against attacks, firewall and network filtering technology is used in a structured and consistent manner.

The University maintains appropriate configuration standards and network security controls to safeguard information resources from internal and external network mediated threats. Firewalls and IDS systems are deployed at the campus border and IPS systems are deployed on core services to augment normal system security measures to prevent denial of service attacks, malicious code, or other traffic that threatens systems within the network or that violates university information security.

Firewalls and IDS/IPS systems are maintained on a regular basis. Rules on these systems are reviewed monthly. The responsibility to maintain, monitor and updating firewalls and IDS/IPS systems is the responsibility of the Director of IT for Security. When events occur, it is the responsibility of the Director of IT for Security to notify CIO with required notification and response expectations as soon as possible after an event. Logging of these regular reviews are required.

Log Management

The creation and retaining of system audit logs to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity is an important element of network security. Reviewing and management of system logs is an important of system and network security. The University partners with Bitlyft to assist with log management. Monitoring organizational critical systems, including inbound and outbound communications traffic, to detect attacks.

Maintaining visibility, remediation and indication of any potential attacks is completed by Bitlyft. Bitlyft as a key security partner with the University, monitoring critical systems including Firewalls, Office 365, Microsoft Exchange, and Active Directory. Review of Bitlyft findings is conducted on a weekly basis by the Director of IT for security. In addition, monthly review meetings are conducted with Bitlyft and critical findings and alerts in the event of an audit log process failure are reported on an immediate basis. Director of IT for Security is responsible for the oversight of log management.

Vendor Management

Prior to selection as a potential supplier for goods and services to Mount Union, potential vendors are required to be considered as holding a “qualified” status with the University. This may be accomplished in a variety of ways such as checking references, site visits, or trade publications. The financial stability of public entities may be investigated with publications or services such as Dun & Bradstreet. For privately held companies, audited financial statements, bank or trade references may be requested.

To comply with Federal regulations set forth in the Gramm-Leach-Bliley Act (GLBA), all vendors for IT purchases relating to computer software and systems, cloud software, and data back-up will be asked to provide SOC2 reports and a copy of their most recent audited financial statements. The Director of Information Technology for Security and the Purchasing
Information Security Policy

TEC 4.0

Office of Information Technology

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

Office will review these documents to determine vendor eligibility. Vendors that do not provide satisfactory copies of these documents may not be approved for use. SOC2 and financial health for key vendors will be reviewed on an annual basis by the Purchasing Office and Director of IT for Security. The list of key vendors will be kept within the Purchasing Office. For more information see the University’s Purchasing Policies and Procedures document.

Network Scans

Independent network testing is completed on an annual basis. This is a requirement of the Office of Information Technology. These tests consist of both internal and external penetration tests and external PCI scans. These tests are overseen by the Director of IT for Security and results are shared with CIO, President Council Members and Board of Trustee. The results of these scans are audited and reviewed on a regular basis and any necessary steps are taken as a result of these tests to improve network security. These tests include general IT controls, penetration, and are completed to meet other compliancy requirements.

Responsibilities

<table>
<thead>
<tr>
<th>Position or Office</th>
<th>Responsibilities</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of Information Technology (CIO and Director of IT For Security)</td>
<td>Update of Policy &amp; Protection of Data</td>
</tr>
<tr>
<td>Users of Data</td>
<td>Protecting institutional data</td>
</tr>
<tr>
<td>VPs, Deans, Directors, Department Heads, Supervisors</td>
<td>Implementation of this policy within their respective units.</td>
</tr>
<tr>
<td>VP Business Affairs &amp; CIO, Director of IT for Security</td>
<td>Oversight of information security</td>
</tr>
</tbody>
</table>

Contacts

<table>
<thead>
<tr>
<th>Subject</th>
<th>Office</th>
<th>Telephone</th>
<th>E-mail/URL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Office of Information Technology</td>
<td>330.823.2854</td>
<td><a href="mailto:IT@mountunion.edu">IT@mountunion.edu</a></td>
</tr>
</tbody>
</table>

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 2021
Edited by: Tina Stuchell
Reviewed: March 2021