UTICA UNIVERSITY

Integrated Information Technology Services

POLICIES AND PROCEDURES

Data Security and Classification

POLICY:

Utica University creates, stores, and maintains data essential for the performance of Utica University and outside entities. All members of the University community have a responsibility to protect Utica University data from unauthorized data generation, access, modification, disclosure, transmission, or destruction.

Permission to access institutional data will be granted to all eligible University employees for legitimate University purposes. Authorization for access to internal, confidential, and sensitive institutional data must be provided by the appropriate division, department, or school. It must be accompanied by an acknowledgment or authorization from the requestor's supervisor and/or data manager.

Where access to internal, confidential, and sensitive institutional data has been authorized, the use of such data shall be limited to the purpose for which access to the data was granted.

SCOPE:

This policy applies to all data created, collected, purchased, rented, stored, or processed by Utica University. This policy applies to employees, students, retirees, alumni, volunteers, vendors, third parties, and all others who create, modify, transmit, and store Utica University data, including, but not limited to, academic partners and auxiliary staff members.

REASON FOR POLICY:

It is essential to protect institutional data from unauthorized modification, destruction, or disclosure. The purpose of this policy is to outline roles and responsibilities within the University community for creating and maintaining an environment that safeguards data from threats to personal, professional, and institutional interests and to establish a comprehensive data security program in compliance with applicable laws. This policy is also designed to document processes for ensuring the security of confidential information; develop administrative, technical, and physical safeguards to protect against unauthorized access or use of this information; provide guidelines and support for all Utica faculty, staff, students, alumni, auxiliary employees, temporary employees, third parties, volunteers, and entities that have been granted an approved set of access credentials; and establish the level of security that must be implemented to protect that data regardless of format (such as recorded, electronic, paper and other physical formats) and form (spoken, text graphic, video).

DEFINITIONS:

Cloud: External storage where data is stored and hosted online by third parties. Examples include Box.com, Engage, Google Drive, Microsoft OneDrive, and others.

Data Manager: The person accountable for determining who has access to information assets within the data manager's functional areas.

Public: Information that may or must be open to the public. While subject to disclosure rules, public data is available to all individuals regardless of their association with Utica University. Examples of public data include:

- Public posted information (website, advertisements, other)
- Press releases
- Sports scores
- Courses listings/descriptions
- Aggregated student data required by the federal government to be made available. Examples of such data are graduation and dropout rates, average standardized test scores.

Internal: Information that has not been declared confidential or restrictive but was created without an intent to be shared publicly. Internal data should not be shared outside the University community without the permission of the person or group that created the data. Any information not explicitly created for public distribution should be considered internal unless otherwise classified with a more restrictive classification.
Examples of internal data include:

- Department meeting minutes (unless publicly posted)
- Internal correspondence (Emails, instant messages)
- Contact lists
- Instructions or procedural documentation not intended for public access
- Zoom recordings

Confidential: Information that must be guarded against unauthorized generation, access, modification, disclosure, transmission, or destruction due to proprietary, ethical, or privacy considerations. This classification also includes data that Utica University is required to keep confidential, either by law (e.g., FERPA) or under a confidentiality agreement with a third party, such as a vendor. This information should be protected against unauthorized disclosure or modification. Confidential data should be used only when necessary for business purposes and should be protected both when it is in use and when it is being stored or transported. Multifactor authentication must be implemented when accessing this data.
Examples of confidential data include:

- Academic records
- Health records
- Social Security numbers
- Encrypted system passwords
- Student and/or financial information
- Legally privileged information.
- Information subject to a confidentiality agreement.

Examples of applicable laws and regulations include:

- Protected Health Information as defined by the Health Insurance Portability and Accountability Act (HIPAA)
- Student educational records as defined by Family Educational Rights and Privacy Act (FERPA) Student financial records as defined by the Gramm Leach Bliley Act (GLBA)
- General Data Protection Regulation (GDPR)

Restricted Use: Information that is highly confidential and may contain research, law enforcement, governmental, or other data. Only those directly involved with these processes are to have access to this information.

- Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored.
- Controlled unclassified information required to be compliant with NIST 800.171
- Data controlled by U.S. Export Control Law such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). ITAR and EAR have additional requirements. See the Export Controls site for details.
- U.S. Government classified data
- Personally identifiable health information that is not subject to HIPAA but used in research, such as human subjects data.
- Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens.
- "Criminal Background Data" that might be collected as part of an application form or a background check.

Multifactor Authentication (MFA): is an authentication method that requires the user to provide two or more verification factors to gain access to a resource.

Wipe/Sanitize: A process that renders all information on physical devices, such as hard drives, unreadable.

Access Credentials: any user name, identification number, password, license or security key, security token, PIN, or other security code, method, technology, or device used, alone or in combination, to verify an individual's identity and authorization to access and use the services.

Domain: an area of control or a sphere of knowledge.

University Owned Device: Any Utica University device or system that is managed and maintained by Utica University.

- Laptops, desktops, or other endpoint equipment purchased and maintained by Utica University (Should have an ITS tag)
- Utica University Remote desktop servers
- Utica University Engage/Canvas LMS Systems
- Utica University Google drive and Gmail

PROCEDURE:

Users

Users are expected to respect the confidentiality and privacy of individuals whose records they access, observe ethical restrictions that apply to the information they access, and abide by applicable laws and policies concerning accessing, using, or disclosing information.

Data Managers

Data managers determine who has access to information assets within the data manager's functional areas. A data manager may decide to review and authorize each access request individually or define a set of rules that determine who is eligible for access based on business function, support role, etc. Access must be granted based on the principles of least privilege – giving requestors access to only the data they need to do their jobs – as well as separation of duties. These rules must be documented concisely. The data manager is also responsible for reviewing who has been given access twice per year to ensure accuracy.

Divisions, departments, and schools must ensure that all decisions regarding collecting and using institutional data follow relevant laws/regulations and University policies and procedures. Divisions, departments, and schools must ensure that appropriate security practices are used to protect institutional data.

The data manager is responsible for overseeing access to confidential information under their domain. The data manager:

- Approves all requests for access via the IITS Ticketing Database.
- Reviews, biannually, access to data stored on Utica University servers, Google Drive, Box.com, Microsoft OneDrive, and any other service hosting Utica University data.
- Ensures that all procedures are followed.
- Reports potential and confirmed incidents of unauthorized access to the Information Security Officer.

Securing Data:
Utica University uses various media and vendors to create, modify, transmit, and store data. Utica University data managers determine appropriate data classifications based on the type of information being classified. Internal, confidential, and restricted use data may have additional constraints due to privacy protections mandated by federal, state, or local regulations and laws. The classification level assigned to data will guide data managers and others that may collect, process, or store data.

Aggregated data should be classified based upon the most secure classification level. If any document is confidential, then all documents in the aggregate are considered confidential.

Unclassified data shall be assumed to be confidential and should only be shared appropriately.

Public Data: Public data must be controlled from creation to destruction and applies to information that Utica University has approved for release to the public. Access is typically available and may be kept in unlocked storage devices or publicly available websites. When the data is no longer needed daily, it should be archived or disposed of. Guidance for records retention and destruction is found in the Records Retention policy.

Internal Data: Internal data must be controlled from creation to destruction, and access will be granted only to those employed or affiliated with Utica University.
Electronic and hard copies must be handled in accordance with the Records Retention policy and must be:

- Stored in a manner to securely protect the data.
- Not be posted in any public location in hard copy or electronic format.
- Destroyed securely.
- Hard copies must be shredded or use another process that destroys the data beyond recognition or reconstitution.

- Electronic storage must be sanitized appropriately before disposal. See the University's Records Retention policy for data destruction procedures.

Confidential Data: Confidential data must be controlled from creation to destruction. Confidential data access will be granted only to those employed or affiliated with Utica University who require such access to perform their job or to those individuals permitted by law.
Electronic and hard copies must be handled in accordance with the Records Retention policy and must be

- Stored in a manner to securely protect the data.
- Disclosed only to those with a need to access the information, with permission granted by the data manager.
- Stored in locked or password-protected environments.
- Have passwords that comply with the University's Computer Passwords policy;
- Not be posted in any public location in hard copy or electronic format.
- Protected by multifactor authentication.
- Only be created, downloaded, or transferred from or onto University owned devices
- Destroyed in a secure manner.
- Hard copies must be shredded or use another process that destroys the data beyond recognition or reconstitution.
- Electronic storage must be sanitized appropriately before disposal. See the University's Records Retention policy for data destruction procedures.

Restricted Use Data: Restricted Use data must be controlled from creation to destruction. Access will be granted only to those affiliated with Utica University who require such access to perform their job or to those individuals permitted by law. Sensitive data must meet all requirements of confidential data. Additionally, it may also require additional protection measures such as segmentation from other electronic or hard copy resources to prevent unauthorized access by persons without a need to know.

Cloud: Utica University recommends that users exercise caution when storing information with unsecured cloud service providers. Before storing data on a non-Utica University server or with a third-party with whom the University does not have a negotiated contract, users should consider the following:

- Who owns the data once posted.
- Privacy rules and regulations (like FERPA, HIPAA, etc.)
- The safety of personal, non-public information like SSNs, credit card information, etc.
- The value of the intellectual property of the data to the user and the user's department.
- Requirements imposed by grant funding regarding security and intellectual property, human subject privacy regulations, and confidentiality agreements.
- Critical nature of the information.

If cloud providers or services are used, provider contracts and terms of service must address data security procedures before the provider or service is used. As many general audience cloud providers do not address these concerns, users should contact the Information Security Officer to complete a data security assessment.

The Vice President for Infrastructure & Chief Information Officer, Information Security Officer, and the Vice President for Legal Affairs and General Counsel will determine if the protections in place and contractual language are sufficient for the information being considered.

Neither Confidential nor Restrictive Use data may be placed on personal devices or cloud service providers to protect Utica University's information.

Sending information protected by privacy rules and regulations (described above) via unencrypted email is prohibited. Confidential and sensitive data must not be sent using unencrypted email. Likewise, neither confidential nor sensitive data should be stored on web servers where it might be inadvertently accessed or indexed by public search engines such as Google or Bing. Contact the Information Security Officer, who can help identify secure options for specific use.

University-owned and Personal Device Security
Employees are responsible for the physical security of their mobile device(s), and devices should be kept in their managers' physical presence whenever possible. In accordance with the Data Breach Notification Policy, University employees must report instances in which institutional data is at risk of unauthorized modification, disclosure, or destruction to the Information Security Officer. This includes data stored in devices owned and not owned by Utica University and in any format, including but not limited to hard copy, desktop, laptop, file server, cloud, tablet, mobile device, USB drive, CD/DVD, etc.

If a University-owned device or personal device containing Utica University data or used to access Utica University data is lost or stolen, the user must immediately notify the Office of Campus Safety and Integrated Information Technology Services. To mitigate against loss or theft of data, users are strongly encouraged to use passwords, PINs, pattern locks, or fingerprint locks on devices in which UC information is stored.

IITS manages devices owned by the University. IITS has implemented and maintains features to wipe and lock a lost or stolen University-owned device remotely. It is recommended to only use Utica University equipment for all University-related duties and do not create, download, or transfer Utica University data onto personal devices. While accessing Confidential or Restrictive Use data only Utica University equipment may be used and users may not create, download, or transfer Confidential or Restrictive Use data onto personal devices.

RESPONSIBILITY:

The Vice President for Infrastructure & Chief Information Officer and the Information Security Officer have overall responsibility for assessing data security risks and assisting users in mitigating against such threats.

The Vice President for Legal Affairs and General Counsel will work with the Information Security Officer to determine whether service providers have adequate protections to address data security procedures.

Users are responsible for protecting the confidentiality and privacy of individuals whose records they access, observing ethical restrictions that apply to the information they access, and abiding by applicable laws and policies concerning accessing, using, or disclosing information.
Data managers are responsible for determining who has access to information assets within the data manager's functional areas and reviewing who has been given access twice per year to ensure accuracy.

Divisions, departments, and schools are responsible for ensuring that all decisions regarding collecting and using institutional data follow the relevant laws/regulations and with University policies and procedures. Divisions, departments, and schools are also responsible for ensuring that

appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.

ENFORCEMENT:

Enforcement of Utica University policies is the responsibility of the office or offices listed in the "Resources/Questions" section of each policy. The responsible office will contact the appropriate authority regarding faculty or staff members, students, vendors, or visitors who violate policies.

Utica University acknowledges that University policies may not anticipate every possible issue that may arise. The University therefore reserves the right to make reasonable and relevant decisions regarding the enforcement of this policy. All such decisions must be approved by an officer of the University (i.e. President, Provost and Senior Vice President for Academic Affairs, Vice President for Financial Affairs, Senior Vice President for Student Life and Enrollment Management, or Vice President for Legal Affairs and General Counsel).

RESOURCES/QUESTIONS:

For more information, contact the Information Security Officer. Use of University computing resources is also subject to the University's Code of Student Conduct, the University's Academic Honesty policy, and all other generally applicable University policies, including:

Responsible Use of University Computing Resources Policy

Computer Passwords Policy

Data Breach Notification Policy

Vulnerability and Risk Assessment Policy

Records Retention Policy

Employee Code of Conduct

Please note that other Utica University policies may apply or be related to this policy. To search for related policies, use the Keyword Search function of the online policy manual.

Laura M. Casamento, President _____ Date

Effective Date: 03/09/2019
Promulgated: 03/18/2019

Last Revised: 05/06/2022
Promulgated: 05/06/2022