POLICY:

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

Permission to access institutional data will be granted to all eligible College employees for legitimate College purposes. Authorization for access to private and sensitive institutional data must be granted by the appropriate division, department, or school and must be accompanied by an acknowledgement or authorization from the requestor’s supervisor and/or data owner.

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

SCOPE:

This policy applies to employees, students, retirees, alumni, volunteers, vendors, third parties, and all others who create, modify, transmit, and store Utica College 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 essential roles and responsibilities within the College 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 establish processes for ensuring the security of confidential information; establish administrative, technical, and physical safeguards to protect against unauthorized access or use of this information; provide guidelines and support for all UC faculty, staff, students, alumni, 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 format) 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, and others.

Data Owner: The person accountable for determining who has access to information assets within the data owner’s functional areas.

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

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

Private: Information that must be guarded against unauthorized generation, access, modification, disclosure, transmission, or destruction due to proprietary, ethical, or privacy considerations. Any information not created specifically for public distribution should be considered private unless otherwise classified with a more restrictive classification.

Examples of private data include:
- Academic records
- Health records
- College partnerships
- Social Security numbers
- System passwords
- Student and/or financial information

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) and the Gramm Leach Bliley Act (GLBA)
- Cardholder data as defined by the Payment Card Industry (PCI) Data Security Standard.
- General Data Protection Regulation (GDPR)

Sensitive: 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.

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

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 with respect to accessing, using, or disclosing information.

Data Owners
Data owners are responsible for determining who has access to information assets within the data owner’s functional areas. A data owner may decide to review and authorize each access request.
individually or may 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 in a concise manner. The data owner 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 the collection and use of institutional data are in compliance with the relevant laws/regulations, and with College policies and procedures. Divisions, departments, and schools must ensure that appropriate security practices, consistent with the data handling requirements in this policy, are used to protect institutional data.

**Securing Data**

Utica College uses various media and vendors to create, modify, transmit, and store data. Utica College data owners determine appropriate data classifications based on the type of information being classified. Sensitive and private 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 provide guidance to data owners 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 private, then all documents in the aggregate are considered private.

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

**Public Data:** Public data must be controlled from creation to destruction, and applies to information that has been approved by Utica College 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 on a daily basis it should be archived or disposed of. Guidance for records retention and destruction are found in the [Records Retention](#) policy.

**Private Data:** Private data must be controlled from creation to destruction, and access will be granted only to those persons employed or affiliated with Utica College who require such access in order to perform their job, or to those individuals permitted by law.

Electronic and hard copies must be handled in accordance to the [Records Retention](#) policy and must be:

- Stored in a manner to securely protect the data;
- Disclosed only to those with a need to have access to the information, with permission granted by the data owner;
- Stored in appropriate locked or password protected environments;
- Have passwords that comply with the College’s [Computer Passwords policy](#);
- Not be posted in any public location in hard copy or electronic format;
- 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 prior to disposal. See the College’s [Records Retention](#) policy for data destruction procedures.

The data owner is responsible for overseeing access to private information under their control. This person:

- Approves all requests for access via the Network ID Request or Change of Access form located at [http://www.utica.edu/academic/iits/compuserservices/forms/index.cfm](http://www.utica.edu/academic/iits/compuserservices/forms/index.cfm).
- Reviews, biannually, access to data stored on Utica College servers, Google Drive, Box.com, and any other service hosting Utica College data.
- Ensures that all procedures are followed.
- Reports potential and confirmed incidents of unauthorized access to the Director of Information Security.
Sensitive Data: Sensitive data must be controlled from creation to destruction, and access will be granted only to those persons affiliated with Utica College who require such access in order to perform their job, or to those individuals permitted by law. Sensitive data must meet all requirements of private data, but may also require additional protection measures such as segmentation from other electronic or hard copy resources to prevent unauthorized access by members of the public, visitors, or other persons without a need to know.

Cloud: Utica College recommends that users exercise caution when storing information with unsecured cloud service providers. Before storing data on a non-Utica College server or with a third-party with whom the College 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 in regards to security and intellectual property, human subject privacy regulations, and confidentiality agreements
- Critical nature of the information

If cloud providers or services are used, provider contract 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 complete the Data Risk Analysis Vendor Form.

The Director of Information Security 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 private nor sensitive data may be placed on unprotected personal devices or cloud service providers to ensure the protection of Utica College information.

Sending information protected by privacy rules and regulations (described above) via unencrypted email is prohibited. Private and sensitive data must not be sent using unencrypted email. Likewise, private or sensitive data must not be stored on web servers where it might be inadvertently accessed or indexed by public search engines such as Google or Bing. Contact the Director of Information Security who can help identify secure options for specific use.

College-owned and Personal Device Security
Employees are responsible for the physical security of their mobile device(s), and devices should be kept in their owners’ physical presence whenever possible. In accordance with the Data Breach Notification Policy, College employees must report instances in which institutional data is at risk of unauthorized modification, disclosure, or destruction to the Director of Information Security. This includes data stored in devices owned and not owned by Utica College 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 College-owned device or personal device containing Utica College data or used to access Utica College 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 personal devices on which UC information is stored.

IITS manages devices owned by the College including the use of features to remotely wipe a lost or stolen device. Users are strongly encouraged to install remote wipe programs on all personally owned mobile devices which allow for the ability to remotely wipe lost or stolen devices, assuming it
connects to Internet to get the command to wipe its information. The process of wiping a mobile device will result in the loss of all data but is necessary to protect Utica College data.

RESPONSIBILITY:

The Director of Information Security has overall responsibility for assessing data security risks and assisting users in mitigating against such risks.

The Vice President for Legal Affairs and General Counsel will work with the Director of Information Security to determine whether service providers have adequate protections in place 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 with respect to accessing, using, or disclosing information.

Data owners are responsible for determining who has access to information assets within the data owner’s functional areas and for reviewing who has been given access twice per year to ensure accuracy.

Divisions, departments, and schools are responsible for ensuring that all decisions regarding the collection and use of institutional data are in compliance with the relevant laws/regulations and with College 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 College 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 College acknowledges that College policies may not anticipate every possible issue that may arise. The College 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 College (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 Director of Information Security. Use of College computing resources is also subject to the College’s Code of Student Conduct, the College’s policy on Academic Misconduct, and all other generally applicable College policies including:

Responsible Use of College 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 College policies may apply or be related to this policy. To search for related policies, use the Keyword Search function of the online policy manual.