Integrated Information Technology Services

POLICIES AND PROCEDURES

Data Breach Notification

POLICY:

Integrated Information Technology Services maintains an Information Incident Response Plan to protect the security, confidentiality, and integrity of personal information of faculty, staff, students, and alumni. As part of this plan, Utica College will notify affected individuals of a data security breach as required by the relevant local, state, or federal laws. Users must report all incidents to the Director of Information Security. All legally required reporting will be done by the Director of Information Security, the Vice President for College Infrastructure and Chief Information Officer, or the Vice President for Legal Affairs and General Counsel or their designees.

SCOPE:

This policy applies to all areas of Utica College that collect, access, maintain, distribute process, protect, store, use, transmit, dispose of, or otherwise handle protected information of faculty, staff, students, or alumni.

REASON FOR POLICY:

This policy provides general guidance to the Utica College community for reporting incidents where Utica College protected information has or may have been compromised.

This process complies with all federal and state laws such as:

Gramm Leach Bliley Act 15 U.S.C. §§ 6801

The Guidance states:

"When a financial organization becomes aware of an incident of unauthorized access to sensitive customer information, the organization should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the organization determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible."

The Guidance allows for a delayed notification if an appropriate law enforcement agency determines such notification will interfere with a criminal investigation.

Health Insurance Portability and Accountability Act of 1996 (HIPAA) 45 CFR §§ 160.103, 164.400-414,

Breaches Affecting 500 or More Individuals

If a breach of unsecured protected health information affects 500 or more individuals, a covered entity must notify the Secretary of Health and Human Services of the breach without unreasonable delay and in no case later than 60 calendar days from the discovery of the breach. The covered entity must submit the notice electronically by clicking on the link below and completing all of the required fields of the breach notification form.

Submit a Notice for a Breach Affecting 500 or More Individuals (to be completed by the Director of Information Security, the Associate Vice President for Information Technology and Institutional Research, or the Vice President for Legal Affairs and General Consul or their designees)

Breaches Affecting Fewer than 500 Individuals

If a breach of unsecured protected health information affects fewer than 500 individuals, a covered entity must notify the Secretary of the breach within 60 days of the end of the calendar year in which the breach was discovered. (A covered entity is not required to wait until the end of the calendar year to report breaches affecting fewer than 500 individuals; a covered entity may report such breaches at the time they are discovered.) The covered entity may report all of its breaches affecting fewer than 500 individuals on one date, but the covered entity must complete a separate notice for each breach incident. The covered entity must submit the notice electronically by clicking on the link below and completing all of the fields of the breach notification form.

Submit a Notice for a Breach Affecting Fewer than 500 Individuals (to be completed by the Director of Information Security, the Associate Vice President for Information Technology and Institutional Research, or the Vice President for Legal Affairs and General Consul or their designees)

NYS Information Security Breach and Notification Act (NYSISBNA) – N.Y. Gen. Bus. Law § 899-aa

In accordance with the requirements set forth in the NYSISBNA, the **College** will disclose any breach of the security of a system containing private information following discovery or notification of the breach to any resident of New York State whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system. In accordance with the NYSISBNA, the required notification may be delayed if a law enforcement agency determines that such notification impedes a criminal investigation. If such a determination has been made, then notification shall take place after such law enforcement agency determines that such notification does not compromise such investigation. Additionally, notification of the breach will be made to the New York State Consumer Protection Board, NYS Office of Cyber Security and Critical Infrastructure Coordination (CSCIC), and the New York State Attorney General using the methods outlined by the NYS Office of CSCIC at this website: https://its.ny.gov/incident-reporting

DEFINITIONS:

Notification. The act of informing the persons affected by the breach and providing required reporting to the applicable governmental agencies.

Private Information. If the information acquired includes a name (first and last name or first initial and last name) in combination with any of the following, and the information was not in an encrypted format, a public notification may be warranted:

- Social Security Number
- Driver's license number
- Bank account, credit, or debit card account number with security, access, PIN, or password that would permit access to the account

Personal information that is publicly and lawfully available to the general public, such as address, phone number, and email address, is not considered private information for the purposes of this policy.

Protected Personal Data (PPD): Includes, without limitation, personally identifiable information (PII), protected health information (PHI), and protected student information (PSI) as described below. PPD includes data maintained in any electronic or hard copy medium.

- Personally Identifiable Information (PII): An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted or redacted or protected by another method that renders them unreadable or unusable by unauthorized person:
    - Social Security number;
    - Motor vehicle operator's license number or non-driver identification card number;
    - Financial account number or credit or debit card number, if circumstances exist in which the number could be used without additional identifying information, access codes, or passwords;
    - Account passwords or personal identification numbers or other access codes for a financial account.

- Protected Health Information (PHI): Protected Health Information (PHI) – Includes identifiable health information as defined at 45 CFR §160.103 that is transmitted or maintained by the College's covered HIPAA components; PHI also includes identifiable health information that is obtained by a College employee or someone working on behalf of the College pursuant to an agreement with another organization or governmental entity that which is protected under the HIPAA/HITECH Act.

- Protected Student Information (PSI): Student education records maintained by the College, whether by academic or administrative units, and protected under the Family Educational Rights and Privacy Act (FERPA) and as described more fully in the Utica College FERPA Disclosure policy (http://www.uvm.edu/policies/student/ferpa.pdf).

Security Breach:

1. The unauthorized acquisition of electronic data or a reasonable belief of an unauthorized acquisition of electronic data that compromises the security, confidentiality, or integrity of PII maintained by Utica College as defined by NYS Information Security Breach and Notification Act (NYSISBNA) – N.Y. Gen. Bus. Law § 899-aa
2. A breach of unsecured protected health information, regardless of the form and format of the information (i.e., electronic, paper) in accordance with the HIPAA Breach Notification rule, 45 CFR § 164.402 and HITECH Act (P.L. 111-5, § 13407); or
3. An unauthorized acquisition or reasonable belief of an unauthorized acquisition of PII or PSI that College officials determines to merit notification to affected persons notwithstanding the lack of regulatory obligation to do so.

Security Incident: An event that a user has reason to believe may be a security breach.

User: Any user, including any faculty, staff, consultant, contractor, student, or agent thereof.

PROCEDURE:

Identifying and Reporting Security Incidents

Any office or individual aware of a potential breach of security containing protected information must immediately report the potential breach of security to IITS by phone (315) 792-3115 or email helpdesk@utica.edu. The Information Security Officer (ISO) will be notified.

As directed by the ISO, the reporter shall follow instructions regarding securing data and preserving evidence. In the event that a public notification of the security breach may be warranted, the ISO will consult with the Vice President for Legal Affairs and General Counsel, Vice President for Presidential Affairs and Chief Marketing and Communications Officer and others to formally begin the breach notification plan in accordance with all Federal and State laws and regulations. Details of the data breach process are found the College's Incident Response Plan.

Notice Requirements

Depending on the determination, Utica College will take one of the following next steps:

- If PPD was breached and notification is required or merited, affected individuals shall receive a notice of the incident, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement agencies.

- If PII was breached, affected individuals must be provided notice in accordance with legal requirements.

- If PHI was breached, affected individuals must be provided notice without unreasonable delay and in no case later than 60 days from discovery of the breach.

The method of noticing a breach of PPD may vary dependent on the number of individuals affected, the cost of notifying, and the normal means of communication with affected individuals, but in all instances as guided by the applicable legal requirements.

Utica College may outsource some or all of the breach notification requirements depending on the nature and extent of the breach.

Documentation

Utica College will document all reported information security incidents. Documentation responsibilities include:

- Log of incidents received
- The evaluation process and outcome of the evaluation
- Recommended corrective action to contain the incident and prevent future incidents
- Breach determination outcome
- Identification of responsible department
- Documentation of notice made to affected individuals, federal offices, state offices, and business associates, where applicable

RESPONSIBILITY:

It is the responsibly of all employee to notify IITS of any suspected security breach by phone (315) 792-3115 or helpdesk@utica.edu. The Information Security Officer (ISO) will be notified. The ISO will coordinate efforts with the Vice President for Legal Affairs and General Counsel, Vice President for Presidential Affairs and Chief Marketing and Communications Officer and other appropriate personnel.

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 Help Desk by phone at (315) 792-3115 or email helpdesk@utica.edu.

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.

Laura Casamento, President Date

Effective Date: October 31 2017
Promulgated: November 3 2017

Last Revised: April 7, 2021
Promulgated: