## Contents

Introduction ..................................................................................................................................... 3  
Scope ............................................................................................................................................... 3  
Information Security Organization ................................................................................................. 4  
Roles and Responsibilities .............................................................................................................. 4  
  Information Security Officer ....................................................................................................... 4  
  System Owners ........................................................................................................................... 5  
Incident Response Team ................................................................................................................. 5  
  Incident Response ....................................................................................................................... 5  
Policy and Standards ....................................................................................................................... 6  
Status of Policies ............................................................................................................................. 6  
  Approved ..................................................................................................................................... 6  
  Working drafts waiting for approval ........................................................................................... 6  
  Internal to IITS documents ......................................................................................................... 6  
  Policies requiring attention ......................................................................................................... 7  
Risk Management ........................................................................................................................... 7  
  Risk Assessment ......................................................................................................................... 7  
  Risk Mitigation ........................................................................................................................... 7  
Security Awareness and Training ................................................................................................... 7  
Reporting Security Risks ................................................................................................................ 8  
Appendix A Definitions .................................................................................................................. 9
Introduction
Information Security is critical to the mission of Utica College, thus the entire campus is essential to the successful implementation of the Information Security Plan. This comprehensive plan outlines top level polices that define Utica College’s objectives for managing and controlling a secure environment.

The purpose of the Information Security Plan is to:

- Assign development and management responsibilities for information security
- Provide for the confidentiality, integrity and availability of information, regardless of the medium in which the information asset is held (e.g. paper, electronic, oral, etc.)
- Develop risk management strategies to identify and mitigate threats and vulnerabilities to information assets
- Establish and maintain an incident response plan
- Maintain ongoing security awareness and training programs
- Comply with applicable laws, regulations, and Utica College policies

Scope
This policy applies to all faculty, staff, third parties, and any other individual or entity representing Utica College. Every employee of Utica College is responsible for protecting the confidentiality, integrity and availability of the College’s assets in electronic, printed, oral or other formats. The Information Security Officer is responsible for providing training and guidance to the campus community on security issues.
Information Security Organization
Information security is the responsibility of the entire campus. The structure below represents the direct reporting structure at Utica College. The Incident Response team is created on an as needed basis based on the situation. Others become part of this process as needed.

Roles and Responsibilities

Information Security Officer
The Information Security Officer (ISO) coordinates information technology / computer security efforts across the college, identifies security initiatives and standards, coordinates and leads the Computer Incident Response Team. This position works under the supervision of the Chief Information Officer and Vice President of Technology (CIO). In addition to the ISO:

A. Works with college officials and system administrators to develop, implement, plan, and prioritize security initiatives and spending based on appropriate risk management and/or financial methodology.
B. Creates, maintains, monitors, and promotes security policies for network security architecture and network access to ensure compliance and information protection.
C. Oversees incident response planning as well as the investigation of security breaches. Responds to any incident where information may have been compromised.
D. Plans and conducts employee information security education and awareness training.
E. Works with outside consultants as appropriate for independent security audits.

System Owners
All users are responsible for the day to day operations and security of the data in their control. The Information Security Officer is available and should be used for consultations, as each area will not have experts in information security. The owners are ultimately responsible for policies and procedures affecting their area and are responsible for all system and security compromise.

Incident Response Team
The composition of incident response team depends on the situation in question. This team may consist of faculty, staff, students or third party members. At a minimum the following individuals must be notified for a reportable breach.

- Information Security Officer (ISO)
- Coordinator of the Incident Response Team, currently the Information Security Officer
- Legal Counsel
- Department Leadership
- President of the college

Security Incidents may be handled by the Information Security Officer and representatives from the area in question. Other areas across campus may be added as needed. Examples of these areas include

- System administrators
- Network Engineers
- Information technology/records management
- Public Information Officer/Public Affairs
- Government Relations/Legislative Liaison
- Regulatory Affairs
- Campus Ethics and Compliance Officer
- Human Resources/Academic Personnel
- Law enforcement, including FBI, as appropriate
- Other executives, as appropriate
- Records Management
- Internal Audit

Typical incidents include:

- Network Issues
- Hardware Failure
- Software Issues
- Virus/Worm
- Hacker
- Loss of Data (General/Unknown Cause)
- Theft of Data

**Incident Response**
The incident response plan for Utica College is an internal document and always under review. This document covers recovery strategies for the topics listed above. In the event that personally identifiable information (PII) is release, Utica College must report the breach to the NYS Attorney General (AG), the NYS Office of Cyber Security (OCS) and the Consumer Protection Board (CPB).

**Policy and Standards**
All official Utica College policies are vetted through a review and approval process which included input from various groups across campus.

The Responsible Use of Computer Equipment Policy outlines the user responsibilities and expectations while using Utica College resources. This and accompanying policies comply with Utica College conduct, federal, state, and local laws, standards, and guidelines.

**Status of Policies**
To keep current with legal requirements and best practices, Utica College evaluates the need to create and review policies. Approved polices are listed on the Utica College website. Working drafts are kept offline. Internal IITS documents are only accessible to IITS staff. Policies are to be reviewed annually. Policies requiring attention are either nonexistent or very early in the process. These are accessible by those working on the documents.

**Approved**
- Responsible use of Computer Equipment
- Vulnerability and Risk Assessment Policy
- Password Policy

**Working drafts waiting for approval**
- Data Classification and Protection

**Internal to IITS documents**
- Utica College Incident Response plan
- Change Control (includes code review, major network changes, or other events with campus wide impact.)
Utica College Information Security Plan

- IITS Server security policy
- Windows Patch management
- SCC Patch Management
- IITS Access Control
- IITS Administrative Access
- Account management policy

**Policies requiring attention**

- Remote access procedures
- Reporting Lost or Stolen Computers Procedure
- Electronic waste disposal
- Third party Service procedures

**Risk Management**

Every institution has different policies and procedures regulating the secure use of resources. The need to secure information must be balanced with the mission of the college. Utica College has developed a process to assess the threats to the college and reduce any risks to an acceptable level.

**Risk Assessment**

Risk assessments must be conducted to establish a baseline to improve from. These assessments evaluate workflow of data from creation to destruction. The process documents every hand and eye that comes into contact with sensitive data. External auditors and vulnerability assessment experts are used to supplement the internal practices of Utica College.

**Risk Mitigation**

Once risks have been discovered it is up to the institution to develop strategies to reduce those risks to an acceptable level. Acceptable levels are determined by campus and departmental leadership based on the severity of risk, confidentiality required, legal requirements, institutional goals, and short term/long term cost. These controls involve all electronic and physical formats.

**Security Awareness and Training**

Risks and staffing are ever changing so Utica College cannot stand still. Effective outreach requires continual advancements. Utica College designated the Information security officer to be responsible for Security and Awareness training. These sessions are held in classroom, online environments and via email.

Each faculty and staff member receives information security training as part of the orientation process. There are times when general training is not sufficient. The Information Security officer works with offices and individuals to create customized sessions on specific topics.

Users are trained to report all incidents to the Information Security Officer. Campus safety is also involved when personal injury or possible legal issues arise such as the theft of a laptop.
**Reporting Security Risks**
The ISO provides statistics of security incidents as part of annual internal reports to the Presidents’ cabinet. High impact issues are immediately relayed to appropriate individuals with legal counsel, Vice Presidents, Presidents, campus safety, etc.
Appendix A Definitions
Access a personal inspection, review, or communication of protected information. This includes records or data which are oral, written, or electronic.

Controls are mechanisms or procedures that mitigate threats. Among the goals of security controls are to ensure confidentiality, integrity, availability or privacy of information and systems.

Confidentiality assures that information or systems are accessible only by authorized users.

Disclosure when data in print, electronic, or verbal format is released to unauthorized entities.

Confidential Information any information classified as confidential would be harmful to the college, employees, students, or other entity. Examples of confidential information include personally identifiable information (PII), academic records, judicial records, health information, and non-public information, as specified in federal or state law or Utica College policy.

Integrity assures that unauthorized changes in data cannot occur or can be detected if they do occur. Verifying the integrity of information ensures that all information is accurate and complete and that nothing has been incorrectly added, modified, or deleted.

Vulnerabilities are characteristics in a process that can allow a threat to take advantage of the process in question. Processes can be personal interactions, paper based or computer based.