Title: Acceptable Use Policy - Information Technology
Policy Number*:* 11/9/2016
Contact: Stephen Rieks, Associate Vice President of Information Technology / Chief Information Officer

I. Reason for Policy

Access to information technology is essential to the mission of the State University of New York at Fredonia ("Fredonia") in providing Fredonia students, faculty and staff with educational services of the highest quality. The pursuit and achievement of the SUNY mission of education, research, and public service require that the privilege of the use of computing systems and software, internal and external data networks, as well as access to the Internet, be made available to all those of the Fredonia community. The preservation of that privilege for the full community requires that each faculty member, staff member, student, and other authorized user comply with institutional and external standards for appropriate use, whether on campus or from remote locations.

II. Policy Statement

To assist and ensure compliance with internal and external acceptable usage standards, Fredonia establishes the following policy which supplements all applicable Federal and State policies, including harassment, patent and copyright, student and employee disciplinary policies, and FERPA, as well as applicable federal and state laws.

A. Scope

The following document outlines Fredonia's policy on Fredonia-provided access to electronic information, services, computing facilities, and networks.

All creation, processing, communication, distribution, storage, and disposal of information by any combination of Fredonia resources and non-Fredonia resources are covered by this policy.

Technology resources covered by this policy include, without limitation:

- All Fredonia owned, operated, leased or contracted computing, networking, information resources, whether they are individually controlled, shared, standalone or networked,

- All information maintained in any form and in any medium within the Fredonia's computer resources, and Fredonia data networks
- All physical facilities, including all hardware, software, applications, databases, and storage media.

B. Definitions

Term	Definition
Authentication Credentials	Assigned UserID/Username and PIN/Password {changed by users) that, used in conjunction, authenticates users to privileged computing facilities and resources.
Computing Facilities	All software applications, desktop and mobile computers, networks, and computer peripherals licensed, owned or operated by Fredonia.
e-Services	Fredonia's terminology relating to electronic services such as e-mail, Learning Management System, and electronic library resources.
Internet	All networks external to Fredonia.
Intranet	All networks internal to Fredonia.
Managed	Software and antivirus upgrades being controlled by a server and "pushed" to the desktop or laptop.
Un-managed	A computing device that does not have anti-virus definitions or upgrades implemented automatically. The computer user installs all upgrades manually.
Users	Individuals who make use of Fredonia technology resources. This includes students, faculty and staff, authorized guests, and all persons authorized for access or use privileges by Fredonia including volunteers for local non-profit agencies, scholars visiting from other State University of New York institutions, and the like.

C. Policy Statement

Users of Fredonia's computing resources must comply with federal and state laws, Fredonia rules and policies, and the terms of applicable contracts including software licenses while using Fredonia computing resources.

Users who engage in electronic communications with persons in other states or countries or on other systems or networks may also be subject to the laws of those jurisdictions and the rules and policies

of those other systems and networks. Users with questions as to how the various laws, rules and resolutions may apply to a particular use of Fredonia's computing resources should contact the Chief Information Officer's office for more information.

Users are responsible for ascertaining what authorizations are necessary and such authorizations prior to using Fredonia computing resources. Users are responsible for any activity originating from their accounts which they can reasonably be expected to control.

Accounts and passwords may not, under any circumstances, be used by persons other than those to whom they have been assigned by the account administrator.

In cases when unauthorized use of accounts or resources is detected or suspected, the account owner should change the password and report the incident.

Although there is no set bandwidth, CPU time, or other limit applicable to all uses of Fredonia's computing resources, Fredonia may require users of those resources to limit or refrain from specific uses if, in the opinion of the system administrator, such use interferes with the efficient operations of the system.

Users are also expected to refrain from deliberately wasteful practices such as printing unnecessary large documents, performing endless unnecessary computations, or unnecessarily holding public computers for long periods of time when others are waiting for the same resources.

Users must not use computing resources to gain unauthorized access to remote computers or to impair or damage the operations of computers or networks, terminals or peripherals. This includes blocking communication lines, intercepting or sniffing communications, and running, installing or sharing virus programs. Deliberate attempts to circumvent data protection or other security measures are not allowed.

Network services and wiring may not be tampered with or extended beyond the area of their intended use. This applies to all network wiring, hardware and in-room jacks. Users shall not use the residential network to provide Internet access to anyone outside of the Fredonia community for any purpose other than those that are in direct support of the academic mission of Fredonia.

D. User Accounts

Use of Fredonia's computer systems and network requires that a user account be issued by Fredonia. Every computer user account issued by Fredonia is the responsibility of the person in whose name it is issued. Continued use of a previously assigned and previously enabled "@fredonia.edu" email account by an inactive or a transferred student is at the discretion of the Chief Information Office. *S*uch accounts, if re-enabled will not be considered “theft-of-service”. Fredonia recognized clubs and student organizations may be issued a user account.

Faculty advisors shall designate a particular person{s) authorized to act on behalf of the club or organization. This person{s) is responsible for all activity on the account and will be subject to Fredonia's disciplinary procedures for misuse.

The following will be considered theft of services, and subject to penalties described below:

- Using a username without the explicit permission of the owner and of Information Technology Services;
- Allowing one's username to be used by another person;
- Using former system and access privileges after association with Fredonia has ended.

E. Resources

Fredonia's information technology resources are, by nature, finite. All members of the Fredonia community must recognize that certain uses of Fredonia's information technology resources may be limited for reasons related to the capacity or security of Fredonia's information technology systems, or as required for fulfilling Fredonia's mission.

Users shall not use information technology resources to excess. Excessive use of information technology resources by a particular user, or for a particular activity, reduces the amount of resource available to satisfy the needs of other users. Excessive use may degrade or jeopardize system functionality, and can result in significant costs to Fredonia. Some examples of excess use may include writing a program or script or using an Internet bot to perform a repetitive task such as attempting to register for a class or purchasing concert tickets online.

Users shall limit incidental personal use. Incidental personal use is an accepted and appropriate benefit of being associated with Fredonia. Appropriate incidental personal use of technology resources does not result in any measurable cost to Fredonia, and benefits Fredonia by allowing personnel to avoid needless inconvenience.

Incidental personal use must adhere to all applicable Fredonia policies. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's professional responsibilities, or adversely impact or conflict with activities supporting the mission of Fredonia. Examples of incidental personal use may include, sending a personal email or visiting a non-work-related web site.

F. Security & Privacy

Fredonia employs various measures to protect the security of its computing resources and its user's accounts. Users should be aware, however, that Fredonia cannot guarantee security and confidentiality. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords and changing them regularly.

Users shall not intentionally view information of other users, modify or obtain copies of other users' files, access or attempt to access other users' email, or modify other users' passwords without

their permission.

Fredonia computers and networks are designed to protect user personal privacy and as such, users shall not attempt to circumvent these protections. Users shall not develop or use procedures to alter or avoid the accounting and monitoring of the use of computing facilities. For example, users may not utilize facilities anonymously or by means of an alias, and may not send messages, mail, or print files that do not show the correct username of the user performing the operation. Users shall not circumvent or attempt to circumvent security mechanisms or the intent of a system.

Computers are Fredonia owned state assets, as such Fredonia retains the inherent right to access these resources either directly or indirectly through remote access tools and techniques at any time.

While Fredonia does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the Fredonia's computing resources may require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. Fredonia may also specifically monitor or inspect the activity and accounts of individual users of Fredonia's computing resources, including individual login sessions and the content of individual communications, without notice, when:

- The user has voluntarily made them accessible to the public, as by posting to a webpage;
- It reasonably appears necessary to do so to protect the integrity, security, or functionality of Fredonia or other computing resources or to protect Fredonia from liability;
- There is reasonable cause to believe that the user has violated or is violating this policy or any other law or policy;
- An account appears to be engaged in unusual or unusually excessive activity;
- Accessing the account is otherwise required or permitted by law, including but not limited to freedom of information laws, laws governing the conduct of parties engaged in or anticipating litigation, and laws governing criminal investigations.

G. Laws and Fredonia Policies

Users must employ technology resources consistent with local, state and federal laws and Fredonia policies. Examples include but are not limited to:

- Users shall comply with all federal copyright law.
- Users shall not download, use or distribute illegally obtained media (e.g. software, music, movies).
- Users shall not upload, download, distribute or possess pornography unless written approval has been granted by the Vice President of Academic Affairs / Provost office to accommodate academic research. Research of this nature shall be conducted in an isolated environment approved by the Associate Vice President of Information Technology/ Chief Information

Officer

H. Commercial Use

Computing resources are not to be used for personal commercial purposes or for personal financial or other gain.

Occasional personal use of Fredonia's computing resources for other purposes is permitted when it does not consume a significant amount of those resources, does not interfere with the performance of the user's job or other Fredonia assigned responsibilities, and is otherwise in compliance with this policy.

Further limits may be imposed upon personal use in accordance with normal supervisory procedures concerning the use of Fredonia's equipment.

I. Enforcement

Users who violate this policy may be denied access to Fredonia's computing resources and may be subject to other penalties and disciplinary action, including possible expulsion or dismissal. Alleged violations will be handled through Fredonia's disciplinary procedures consistent with the terms and conditions of the governing labor agreements (if applicable).

Fredonia may suspend, block or restrict access to an account, independent of such procedures, when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of Fredonia's or other computing resources or to protect Fredonia from liability.

Fredonia may also refer suspected violations of applicable law to appropriate law enforcement agencies.

When Information Technology Services becomes aware of a possible violation, Information Technology Services will initiate an investigation in conjunction with relevant campus offices including the President's Cabinet members, Human Resources, and University Police in accordance with collective bargaining rights for applicable unions. Users are expected to cooperate fully in such investigations when requested.

In order to prevent further unauthorized activity during the course of such an investigation, Information Technology Services may suspend authorization for use of all computing facilities for the user(s) involved in the violation.

XI. Related Documents, Forms, and Tools

A. Information Security Program (Word Doc)
B. Information Management and Cyber Security Policy (PDF)
C. Federal Policies
D. Gramm-Leach-Bliley Act

E. FERPA (Family Educational Rights and Privacy Act)
F. HIPPA (Health Insurance Portability and Accountability Act)
G. FISMA (Federal Information Security Management Act)

XII. Website Address for this Policy
http://home.fredonia.edu/its/acceptable-usage-policy

V. Authority for Policy

Authority for policies is the President's Cabinet

Information Management and Cyber Security Policy

March 2010

TABLE OF CONTENTS

PURPOSE

This policy defines security requirements that apply to the information assets of the entire SUNY Fredonia enterprise. Any unit of SUNY Fredonia may, to meet its individual business needs or to satisfy specific legal requirements such as listed below exceed the security requirements instituted in this document; but all units must, at a minimum, achieve the security levels required by this policy.
HIPAA http://www.hhs.gov/ocr/privacy/index.html
FERPA http://www.ed.gov/policy/gen/guid/fpco/ferpa/index.html
Graham Leach Bliley, ISO17799 http://www.ftc.gov/os/2002/05/67fr36585.pdf
New York State Information Security Breach and Notification Act, http://www.cscic.state.ny.us/security/securitybreach

The primary objectives of this policy and security program are to:

- Manage the risk of security exposure or compromise of SUNY Fredonia information assets;
- Designate responsibilities for the protection of SUNY Fredonia information;
- Optimize the integrity and reliability of SUNY Fredonia information assets;
- Reduce opportunities for the introduction of errors in information assets supporting SUNY Fredonia business processes;
- Protect SUNY Fredonia senior management and staff, and preserve senior management's options in the event of an information asset misuse, loss or unauthorized disclosure;
- Promote and increase the awareness of information security at SUNY Fredonia.
- Support the Mission Statement of SUNY Fredonia.

SCOPE

This policy is applicable to entities, staff and all others who have access to or manage SUNY Fredonia information. This policy encompasses all information systems for which SUNY Fredonia has administrative responsibility. It addresses all digital information which is created or used in support of SUNY Fredonia business activities. Where conflicts exist between this policy and a SUNY Fredonia departmental policy, the more restrictive policy will take precedence.

Information security refers to the protection of information from accidental or unauthorized access, destruction, modification or disclosure. Digital information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by computer automated means. Digital information is relayed in a variety of methods, including through computer networks and portable media, such as jump drives, CD's and DVD's. Digital information is also stored and retrieved in several formats, including but not limited to computer databases or transmissions, tapes, CD ROMs, diskettes, computer generated reports, hard copy documentation, e-mail messages, and voice mail.

This policy must be communicated by supervisors to all employees and all others who have access to or manage SUNY Fredonia digital information. This security policy is technology independent and does not include implementation standards, processes or procedures.

DEFINITIONS

Authorized User refers to any individual granted credentials to access SUNY Fredonia Information Technology Resources.

Credentials refer to the unique username and password provided each authorized user to access SUNY Fredonia resources.

Database Administration - The function of applying formal guidelines and tools to manage the university's information resource and specifying, implementing, and maintaining access control to assure that Data Users have the appropriate authorized access needed to perform assigned duties or to fulfill university roles is termed database administration. Responsibility for database administration activities is shared among the Data Stewards, Data Experts/ and ITS Database Administrators.

Data Definition - Data Stewards and Data Experts provide data descriptions so Data Users know what shareable data are available, what the data mean, and how to access and process the data. These data about the data are referred to as data definitions and sometimes called metadata. Data definitions may be stored in an integrated or complementary database known as a ***Metadata Repository***. Data definitions should be based on actual usage, documented and modified only through procedures established by the Data Stewards, and periodically reviewed for currency.

Data Integration Model is a logical construct that describes the data entities that comprise the University Enterprise Database (UEDB) and the relationship among those entities. The Data Stewards, or designated Data Experts and ITS Database Administrators, collaborate to establish and maintain a university-wide Data Integration Model that describes all major data entities of the UEDB and the relationships among those data entities. Included in the model are the linkages among data collected or maintained by the various organizational units of the university.

Data Ownership - The UEDB is a university resource; individual units or departments may have stewardship responsibilities for portions of the enterprise data.

Data Warehouse refers to a query-only database containing historical point-in-time data and summary information from university operational systems. The data warehouse is used to support business analysis and decision-making.

Digital Information is defined as the representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by computer automated means.

Digital Systems refers to the computer platform on which digital information is stored and used.

Highly Sensitive Information refers to information that is considered confidential. (Reference "Information Management and Security Procedural Document" for categorization detail.)

Information Assets refers to the data and resources owned and protected by SUNY Fredonia.

Metadata Repository refers to a database system that contains descriptive information

about the university's enterprise data and administrative systems. The repository is a complementary facet of the Data Warehouse.

Moderately Sensitive Internal Business-Use Data refers to those elements of the UEDB that may be accessed by all employees of the university, with authorization, for the conduct of university business. (Reference "Information Management and Security Procedural Document" for categorization detail.)

Non-sensitive Public Data refers to the elements of the UEDB that are available to the general public, including people outside of SUNY Fredonia. (Reference "Information Management and Security Procedural Document" for categorization detail.)

Open-port facilities refers to the communication end point in computer networking configured to accept units of data.

Portable Computing Devices and Information Media refers to any mobile computing device such as a laptop, smart phone, personal data assistant, flash drive or other storage media.

Sensitive (or critical) systems and applications refers to systems such as the Student Information System and Human Resource system that house confidential student and employee data.

SUNY Fredonia Application Owners refers to the users of software such as Banner, ANGEL, People Admin, Smart Catalogue, Digital Measures, etc.

SUNY Fredonia Electronic Resources refers to information available online via the SUNY Fredonia network or the World Wide Web.

System Administration - The function of maintaining and operating hardware and software platforms is termed system administration. Responsibility for system administration activities belongs to the Computing Services unit of ITS.

UEDB (University Enterprise Database) is a conceptual term used to identify that body of data critical to university planning, management, and business operations of both administrative and academic units. This data may reside in different database management systems and on different machines, but in aggregate may be thought of as forming one logical university resource, which is called the UEDB. The UEDB contains data from multiple operational areas that need to be integrated in order to support institutional research, business analysis, reporting, and decision making.

University Information System is a conceptual term used to identify the collection of computer hardware, software, and network connections, which together form the integrated system underlying the logical University Enterprise Database (UEDB).

POLICY

Part 1. Preface

This policy is a statement of the goals, ethics, responsibilities and accepted behaviors required to establish and maintain SUNY Fredonia's information security objectives; it sets the direction, offers broad guidance and defines senior management's requirements for digital information security related processes and actions. Compliance is mandatory. This

policy follows the framework of ISO17799 for Security Policy guidelines and is consistent with existing SUNY Fredonia policies, rules and standards. This policy documents many of the security practices already in place. Senior management is fully committed to information security and agrees that every person employed by or on behalf of New York State government has important responsibilities to continuously maintain the security and privacy of SUNY Fredonia data.

Part 2. Document Change Management

Requests for changes to this policy should be presented by the SUNY Fredonia Information Security Program Team to Senior Management. If senior management agrees to the change(s), the Information Security Program Team will be responsible for communicating the approved change(s) to the SUNY Fredonia community. The document is maintained by the office of Associate Vice President for ITS.

This policy and supporting policies and standards will be reviewed on an annual basis.

Part 3. Data Management Roles and Responsibilities

Authorized User refers to any individual granted credentials to access SUNY Fredonia Information Technology Resources.

Chief Information Officer, CIO: (at Fredonia the comparable title is Associate Vice President for Information Technology Services-AVPITS)-The university official responsible for overseeing the management of university-wide data systems. The CIO will make recommendations for policy and problem resolutions in consultation with the Data Steering Committee and the Information Technology Advisory Board (ITAB) to the ITS Executive Board (Data Trustees).

Database Administrators (DBAs): Data administration involves the application for formal guidelines and the appropriate tools to manage SUNY Fredonia's information resources (provide a secure infrastructure in support of data including, but not limited to, providing physical security, backup and recovery processes, granting and terminating access privileges as authorized by data stewards, and implementing and administering controls over the information). The University Data Administration function (within the Office of the Vice President for Information Technology) exists to support and further the goals of the University data management committees and structure.

Data Experts/Managers: Data Experts/Managers in functional areas have day-to-day responsibilities for managing business processes, establishing business rules for the production transaction system as related to data capture, maintenance, and dissemination.

Data Steering: Data Steering is a representative group of IT and Data Stewards which makes recommendations to the Information Security Program Team and to Senior Management. These recommendations are related to data, issues, and standards that affect more than one administrative area. Data Steering will establish and document data management standards and procedures, including integration standards for code mappings and crosswalks between administrative applications and systems, and insure that individual responsibilities and procedures are clearly outlined and appropriately communicated.

Data Stewards: Data Stewards are University officials (e.g Directors, Managers, or their designees) having direct operational level responsibility for information management (capture, maintenance, and dissemination of data). Data stewards are responsible for:

working with Data Trustee/Owner to classify data, approving data access on behalf of Data Trustee/Owner, determining/specifying user access level(s), securing paper infrastructure and implementing and enforcing departmental policy and procedures.

Data Trustees/Owners: Data Trustees/Owners are senior University officials (e.g. Deans, VPs, AVPs, or their designees) responsible for overseeing the establishment of data management policies and procedures, the assignment of data management responsibility (assigning data stewards) and promoting data resource management for the good of the entire University.

Data Users: Data users are individuals who need and use SUNY Fredonia data as part of their assigned duties or in fulfillment of assigned roles or functions within the University community. Individuals who are given access to sensitive data have a position of special trust, and as such, are responsible for protecting the security and integrity of those data. Anyone who has intentionally breached the confidentiality and/or compromised the integrity of protected data/information (e.g., category HS data) may be subject to disciplinary action and/or sanctions up to, and including discharge or dismissal in accordance with SUNY Fredonia policy and procedures. Additionally, breach of confidentiality and/or compromising integrity of data/information that are protected by law, acts, or regulations, will result in criminal prosecution.

Information Security Program Team (ISec): The Information Security Program Team, appointed by the SUNY Fredonia President, will coordinate and oversee implementation of information security awareness program activities, will approve and support major initiatives to enhance information security, and will develop a process to measure compliance with policy. The Information Security Program Team is responsible for investigating (and responding to) all alleged security violations.

Information Technology Services (ITS): ITS is responsible for the *data* processing infrastructure and computing network which support *information owners*. It is the responsibility of ITS to support this policy and provide resources needed to enhance and maintain the required level of digital *information security*.

Non-SUNY Fredonia Employees: Employees such as FSA, Contractors, Consultants, Vendors and other persons, to the extent of their present or past access to SUNY Fredonia information assets are also covered by this policy.

Senior Management: Senior Management includes the President and Vice Presidents (known as members of the SUNY Fredonia President's Cabinet).

SUNY Fredonia Employees: It is the responsibility of all employees to protect SUNY Fredonia information and resources, to note variances from established procedures, and to report such variances for suspected security incidents to the appropriate supervisor(s) and to the Director of Internal Control, co-chair of the Information Security Program Team.

Supervisors: Supervisors will be responsible for the implementation of this and other information security policies and the compliance of their employees. Supervisors must educate their employees with regard to information security issues, including information retention policies. Supervisors will explain the issues, the rationale for the policies, the role(s) individuals have in safeguarding information assets, as well as the consequences of non-compliance. It is the responsibility of the supervisor to notify DBA and System Administrators when staff members terminate employment.

System Administrators: System Administrators are the staff members responsible for administering security tools, auditing security practices, identifying and analyzing security *threats* and solutions, implementing specific security *controls* and responding to security violations. They have administrative control over *user*-IDs and passwords and the associated processes for reviewing, logging, implementing access rights, emergency privileges, exception handling, and reporting requirements.

Part 4. Information Security Policy

Information is among SUNY Fredonia's most valuable assets and SUNY Fredonia relies upon that information to support its mission of teaching, research and service as well as its business activities. Information must be protected from the time it is created, through its useful life, and authorized disposal since quality and availability of that information is key to SUNY Fredonia's ability to carry out these missions. Therefore, the security of SUNY Fredonia's information, and of the technologies and systems that support it, is the responsibility of everyone concerned. Each authorized user of SUNY Fredonia information has an obligation to preserve and protect said information assets in a consistent and reliable manner. Information must be classified and protected based on its importance to business activities, risks and security practices as defined in ISO 17799, a Code of Practice for Information Security Management, and as implemented by this policy. Security controls provide the necessary physical, logical and procedural safeguards to accomplish those goals. Information security management enables information to be shared while protecting the information and its associated computer assets including the network over which the information travels. SUNY Fredonia Data Trustees and Stewards are responsible for ensuring that appropriate physical, logical and procedural controls are in place on these assets to preserve the confidentiality, integrity, availability and privacy of SUNY Fredonia information.

Individual Accountability

Individual accountability is the cornerstone of any security program. Without it, there can be no security. Individual accountability is required when accessing all SUNY Fredonia electronic resources or when terminating employment. Access to SUNY Fredonia computer systems and networks is provided through the use of individually assigned unique computer identifiers known as user-ID and password. Individuals who use SUNY Fredonia computer resources must only access resources to which they are authorized. Passwords must be treated as confidential information and must not be disclosed. All individuals are responsible for all activities performed under their user-ID. For the user's protection and for the protection of SUNY Fredonia resources, passwords (or other tokens or mechanisms used to uniquely identify an individual) **must not be shared**. Upon termination of employment, individuals are required to archive or delete information according to record retention policy.

Confidentiality/Integrity/Availability

A. All SUNY Fredonia information will be protected from unauthorized access to help maintain information's confidentiality and integrity. The information owner will classify and secure information within their jurisdiction based on the data classification guidelines in the "Information Management and Security Procedural Document" according to the information's value, sensitivity to disclosure, consequences of loss or compromise and ease of recovery.
B. Information will be readily available for authorized use as needed by the user in the normal performance of their duties. Appropriate processes will be implemented to ensure the reasonable and timely recovery of all SUNY Fredonia information, applications

and systems, regardless of computing platform, should that information become corrupted, destroyed, or unavailable for a defined period.

C. Business impact analysis will be performed periodically to determine the criticality of SUNY Fredonia processes and establish a schedule for backup and recovery of those systems and data to ensure their timely recovery in the event of an extended outage. When performing a business impact analysis, the data stewards as charged by senior management, will:
    - Identify all key business processes and assess their criticality to the operation of SUNY Fredonia. The information owners (data trustees and stewards) will determine maximum acceptable time to recover each key business process in the event of a disruption;
    - For each critical process, an inventory will be developed of all of the assets required to perform the process or to resume the process in the event of a disaster. Considerations of assets will include but are not limited to staff, accommodations, communications, IT assets, networking and data;
    - Perform a threat analysis to determine the threats the organization and its data are subject to. These threats could include natural disasters or man-made events;
    - Perform a risk assessment to determine the likelihood that a threat would or could occur;
    - Develop and test plans to recover the assets within the time frame required to meet the requirements of the lines of business.

Policy and Standards Relationship

SUNY Fredonia will develop standards that support the implementation of this policy for systems and technologies being used within their domains. These security standards will be produced and implemented to ensure uniformity of information protection and security management across the different technologies deployed within SUNY Fredonia. The standards can be used as a basis for policy compliance measurement.

Part 5. Security Organization Policy

SUNY Fredonia's Information Security Program Team (*ISec* Team) is responsible for researching and managing information security issues. The SUNY Fredonia ISec Team reports to the President who is responsible for its organization and leadership. The ISec Team is a campus-wide organization of Information owners and professionals who contribute to the overall mission of the function. Members are nominated to the function by the leadership of their respective business or academic area and are typically supervisors authorized to commit resources for their responsibility area. ISec Team members remain accountable to their leadership who define their degree of authority in their responsibility area. The ISec Team must include director-level members for SUNY Fredonia's central infrastructure and major distributed IT areas. The ISec Team operates as a standing committee guided by policy and standard procedures.

The mission of the *ISec* Team is to:

- Develop, deploy and maintain an information security architecture that will provide security policies, mechanisms, processes, standards and procedures that meet current and future business needs of SUNY Fredonia;
- Provide information security consulting to SUNY Fredonia regarding security threats that could affect SUNY Fredonia computing and business operations and make recommendations to mitigate the risks associated with these threats;

- Assist senior management in the implementation of security measures that meet the business and academic needs of SUNY Fredonia;
- Develop and implement security training and awareness programs that educate SUNY Fredonia students, employees, contractors and vendors with regard to SUNY Fredonia's information security requirements;
- Investigate and report to senior management breaches of security controls, and implement additional compensatory measures when necessary to help ensure security safeguards are maintained;
- Assist with the development, implementation and maintenance of disaster recovery processes and techniques to maintain SUNY Fredonia business continuity in the event of a disaster or extended period of computer resource unavailability.

Part 6. Asset Classification and Control Policy

Information Management

A. Information, like other assets, must be properly managed from its creation, through authorized use, to proper disposal. As with other assets, not all information has the same use or value, and therefore information requires different levels of protection. Information will be classified based on the classification guidelines in the "Information Management and Security Procedural Document" according to its value, sensitivity, consequences of loss or compromise, and/or legal and retention requirements.
B. All information will have the information or data steward established within SUNY Fredonia's lines of business that will be responsible for assigning the initial information classification and make all decisions regarding controls, access privileges of users, and daily decisions regarding information management. Periodic high-level business impact analyses will be performed on the information to determine its relative value, risk of compromise, etc. Based on the results of the assessment, information will be classified into one of SUNY Fredonia's information classifications, where appropriate.
C. Each classification will have a set or range of controls, designed to provide the appropriate level of protection of the information and its associated application software commensurate with the value of the information in that classification.

Privacy and Handling of Private Information

A. Privacy of an individual's information must be respected throughout its lifetime.
B. SUNY Fredonia's systems hold personal identifiable information (i.e., any information that is unique to any individual) to carry out the business of SUNY Fredonia.
C. The protection of the privacy of personal information is of utmost importance and SUNY Fredonia must conduct business so as to protect the rights of privacy of all members of the public, business partners, and SUNY Fredonia community.
D. All SUNY Fredonia employees with access to personal information are required to respect the confidentiality of that personal information.
E. Personal data, including information about students, employees, members of the public, organizations and business partners, collected and maintained by SUNY Fredonia must:
    - Be used only for the stated purpose for which it was gathered;
    - Be gathered in lawful and fair circumstance;
    - Be kept for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose;
    - Not be disclosed without specific consent or as authorized by law;
    - Be available for review by authorized individuals;
    - Be corrected if errors are known to exist or if the individual identifies errors;

- Be erased where appropriate if the individual requests consistent with applicable laws; and
- Be protected using system access controls, or be stored in a locked cabinet or office. (If this information is stored by a third-party, the third-party must contractually abide by these rules.)
- Be destroyed in a manner consistent with that required by law or regulations.

Release of Private Information to Third Party Consultants

"Private information" defined in the New York State Information Security Breach and Notification Act (which is part of the "Internet Security and Privacy Act") and considered "Highly Sensitive Information" by SUNY Fredonia definition must not be released as storable data to third party consultants without security procedures that demonstrate SUNY Fredonia's third party diligence in protecting the data and ensuring its proper distribution when no longer needed. "Private or highly sensitive information" shall mean personal information (e.g., information concerning an individual which, because of name, number, symbol, mark or other identifier, can be used to identify an individual) in combination with any one or more of the following data elements: (1) social security number; (2) driver's license number or non-driver identification card number; (3) account number, credit or debit card number, in combination with any required security code, access code, or password which would permit access to an individual's financial account. It does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

Campus procedures must include:

- Data Trustee approval of the need for the release;
- SUNY Fredonia approved mechanism for encrypting the data;
- Approval by the third party for receiving the data;
- Third party assurance of proper security for the stored data and its subsequent destruction;
- Logging of the transfer to record the date, type of sensitive data, type of security, location of written approval, and parties to the transfer on both sides;
- Recording of the third party's written statement of subsequent secure destruction of the data.

Protection of Third Party Information

A. Confidentiality of any third party confidential information must be respected throughout its lifetime.
B. SUNY Fredonia's systems hold confidential information from third party entities to carry out the business of the organization. The protection of the confidentiality of this information is of utmost importance and SUNY Fredonia conducts business so as to protect the rights of all partners including constituents, governments and vendors. All employees with access to such information are required to respect the confidentiality of that business information and not disclose the information to other third parties. Confidential information obtained from relationships with third parties must:
    - Be used only for the stated purpose it was gathered;
    - Be gathered in lawful and fair circumstance;
    - Be kept for the amount of time required by law or regulations or as long as it remains relevant for its primary purpose;
    - Not be disclosed without specific consent or as authorized by law;
    - Be available for review by authorized third parties;
    - Be corrected if errors are known to exist or if the third party identifies errors;

- Be erased where appropriate if the third party requests consistent with applicable laws; and
- Be protected using system access controls, or be stored in a locked cabinet or office. (If this information is stored by a third-party, the third-party must contractually abide by these rules.)
- Be destroyed in a manner consistent with that required by law or regulations.

Part 7. Personnel Security Policy

The Human Resources Information Security Program is intended to reduce the risks of human error, theft or misuse of SUNY Fredonia information and facilities. Security responsibilities must be defined and addressed at the employee hiring stage, included in contracts with third parties, and monitored by the employee's direct supervisor during an individual's employment.

Including Security in Job Responsibilities

Security roles and responsibilities as defined in this policy in the section titled 'Organizational and Functional Responsibilities' must be documented where appropriate. They will include any general responsibilities for implementing or maintaining the security policy as well as any specific responsibilities for the protection of particular assets, or for the execution of specific security processes.

Personnel Screening

SUNY Fredonia will follow the State guidelines with regard to pre-employment screening. SUNY Fredonia may perform, or have performed, additional screening for sensitive positions with State approval. These additional checks could include but are not limited to the following:

- Previous employment;
- Criminal records as authorized by Federal and State laws;
- A check (for completeness and accuracy) of the applicant's curriculum vitae;
- Confirmation of claimed academic and professional qualifications;
- Independent identity check (passport, visa or similar documents) consistent with Federal and State laws; and
- Licensing requirements for healthcare providers, etc.

User Training

An information security awareness program will be developed, implemented, and maintained to address security education for SUNY Fredonia employees. The awareness program will review information security policy, threats and concerns, and the proper use of information processing facilities (e.g. logon procedures and use of software packages) to minimize possible security risks. The program will additionally include the procedure to follow to report incidents (security breach, threat, weakness or malfunction) that might have an impact on the security of SUNY Fredonia information.

Reporting Security Weaknesses

Users of SUNY Fredonia Information Technology resources will be required to note and report any observed or suspected security weaknesses or threats to the appropriate manager/supervisor or the Director of Internal Control via information.security@fredonia.edu. They must report these weaknesses as soon as

possible. *Users must not attempt under any circumstances to prove a suspected weakness.* This is for their own protection, as testing weaknesses could be perceived as a potential misuse of the system.

Information Technologies established specifically to research Information Assurance as a legitimate academic pursuit are not restricted by this reporting policy.

Procedures must be established for reporting security software malfunctions. The following should be considered:

- The symptoms of the problem and any messages appearing on the screen should be noted;
- The computer must be isolated, if possible, and use of it stopped until the problem has been resolved;
- The matter should be reported immediately to the Director of Internal Control, Information Security Program Team, for appropriate investigation

Part 8. Physical and Environmental Security

Critical or sensitive SUNY Fredonia business information processing facilities must be housed in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls to protect from unauthorized access, damage and interference. Physical security perimeters should be established in SUNY Fredonia environments where servers are stored or operational in wiring closets for network and telephonic connections, where printers used for printing confidential or sensitive information, and any other location where critical or sensitive SUNY Fredonia computer equipment may be in use or stored. The purpose of the security perimeter is to prevent unauthorized access to the computer resource, or to prevent theft of the resource. The ITS designees of the information Security Team will perform periodic threat and risk analysis to determine the extent of the perimeter vulnerabilities.

Clean Desk and Clear Screen

Sensitive information must be removed from view and physically secured when not in use. Measures must be taken to insure that such information cannot be read or copied by unauthorized persons. Physical security for the machine when unattended is one approach. The use of computer screen savers or similar technology is required to ensure that sensitive information is not displayed after a specified period of inactivity. When unattended or physically unsecured for more than a few minutes, all computers **must be screen locked**.

Part 9. Communications and Network Management

A. SUNY Fredonia network monitoring follows best practice to the extent appropriate resources are available for staffing and monitoring tools.
B. Third party connections to any portion of the SUNY Fredonia network could compromise the integrity and confidentiality of data on the SUNY Fredonia network. Third party network connections are only allowed with prior approval by the Network Security Administrator to ensure that security measures are in place to maintain the current level of security on SUNY Fredonia networks.
C. See SUNY Fredonia's Computer and Network Usage policy at: http://www.fredonia.edu/helpdesk/Policies.asp for information on user responsibilities and policies on connecting computer systems to the SUNY Fredonia network and the temporary removal or blocking of vulnerable or compromised systems from the network.

Network Management

SUNY Fredonia implements a range of network controls to maintain security in its trusted, internal network, and to protect connected services and networks. The 'network' includes any device that is attached via a wired or wireless connection with an IP (Internet Protocol) address.

Host Scanning

ITS reserves the right to scan any device attached to the SUNY Fredonia network on a periodic and tiered basis to ensure optimal configuration to protect against known vulnerabilities and to advise Data Trustees/Steward of unencrypted storage of highly sensitive/confidential data (e.g. SS#). For example, a system integrity check, using an appropriate tool, may be run as frequently as current standards recommend checking for system integrity. Sensitive or critical systems will be scanned as frequently as current standards recommend. Due to the complex nature of various vulnerabilities, central scanning should be used where possible, and a notification mechanism developed to propagate vulnerability information to data trustees/owners and ITS staff for appropriate remediation.

Network Security Checking

A. Network vulnerability scans are conducted periodically on systems that are essential to supporting a process that is critical to SUNY Fredonia business and annually on all other systems. Appropriate tools to scan the network and to report vulnerabilities will be identified by ITS and will be updated periodically to ensure that recently discovered vulnerabilities are included in any scans.
B. The vulnerability scanning process is followed and tested at all times to minimize the possibility of disruption to SUNY Fredonia networks by such reviews. Reports of exposures to vulnerabilities will be forwarded to the ISec Program Team for review.
C. The use of network vulnerability scanning tools by anyone other than, or authorized by, ITS personnel is prohibited. Researchers and students performing vulnerability testing as a function of their research or coursework must receive ITS authorization and make arrangements to ensure that scans are limited to their own systems or systems that have been assigned to them. Any vulnerability scanning from the Internet must be conducted exclusively by appropriately authorized and trained organizations.

Penetration and Intrusion Testing

A. All production computing systems that provide campus information to external parties, either directly or through another service that provides information externally (such as the World Wide Web), may be subjected to penetration analysis and testing. It may be necessary for another campus organization, a suitably qualified State evaluation team or authorized third party to attempt a live test to validate potential vulnerabilities. Such analysis and testing will be used to determine if:
    - The application may be changed by anyone while in production;
    - An authorized user may access the application and cause it to perform unauthorized tasks;
    - An unauthorized user may access, destroy or change any data; or
    - An unauthorized user may access the application and cause it to take inappropriate action.

B. Only authorized administrators may perform penetration testing and the system owner or her/his designate must approve each test. Any other attempts to perform such tests or

to determine how a system may change or behaves under abnormal circumstances, whether successful or not, will be deemed an unauthorized access attempt and will result in disciplinary or legal action.

Internet and Electronic Mail Acceptable Use

All uses of the SUNY Fredonia network and of SUNY Fredonia electronic mail facilities must be within the bounds of SUNY Fredonia's Computer and Network Authorization and Use policy http://www.fredonia.edu/helpdesk/Policies.asp.

External Internet and VPN Connections

SUNY Fredonia acts as an Internet Service Provider for its faculty, staff and students in support of its teaching, research and service missions. This mission is best served by minimizing controls on network traffic while ensuring that the network facilities are not abused.

A. VPN, wireless and open-port facilities attached to the general campus network must provide for authenticated access to insure proper use and the ability to attribute responsibility for actions. If a specific implementation does not allow for authentication, reasonable steps must be taken to ensure that access to the facility is controlled by other means.
B. All other permanent connections intended to route traffic from the SUNY Fredonia network to other networks must be approved by the SUNY Fredonia AVPITS in order to insure that they:
    1. Do not interfere with campus operations
    2. Address appropriate security concerns
    3. Insure proper use of SUNY Fredonia's resources (Examples of this kind include the Faculty Student Association and the Research Foundation).
    4. Transmission of sensitive data over the Internet must be done in such a manner that the data is not compromised in regard to privacy or integrity. Encryption of such data is required. This can be accomplished by encrypting the data prior to transmission or by using VPN technology to encrypt the data flow over the network.

Connections to Third Party Networks

A. Any permanent connection intended to route traffic from the SUNY Fredonia private network to a third party private network must have a business case documented and approved by the SUNY Fredonia AVPITS or designee. A risk analysis may be performed to ensure that the connection to the third party network will not compromise SUNY Fredonia's network. Controls, such as the establishment of firewalls and/or a DMZ (demilitarized zone), may be implemented between the third party and SUNY Fredonia to protect SUNY Fredonia's trusted networks. These connections may be periodically reviewed or tested by the SUNY Fredonia AVPITS or her/his designee to ensure:
    - The business case for the connection is still valid and the connection is still required;
    - The security controls in place (filters, rules, access control lists, etc.) are current and functioning correctly.
B. This policy requires that connection to the SUNY Fredonia network be done in a secure manner to preserve the integrity of the SUNY Fredonia network, data transmitted over that network, and the availability of the network. The security requirements for each connection will be assessed individually, and be driven by the business needs of the

parties involved. Only authorized Information Security or IT network staff will be permitted to use "sniffers" or similar technology on the network to monitor operational data and security events.

C. Third parties requesting permanent access to the SUNY Fredonia network must have an internal SUNY Fredonia sponsor develop a business case for the network connection. A SUNY Fredonia non-disclosure/non-access agreement must be signed by an authorized SUNY Fredonia representative and a duly appointed representative from the third party organization who is legally authorized to sign such an agreement. This document, describing the business case and network connection requirements, must be submitted to the SUNY Fredonia AVPITS and security staff. The SUNY Fredonia AVPITS or her/his designee has final approval authority. Failure to sign this document by either party will result in the connection being disapproved.

D. If a VPN connection is to be provided, refer to the section above, "External Internet and VPN Connections" for security requirements.

Security of Electronic Mail

Electronic mail is inherently not secure and should not be used to transmit highly sensitive/confidential information, due to the security risks which include but are not limited to:

- Vulnerability of messages to unauthorized access or modification or denial of service;
- Vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service;
- Impact of a change of communication media on business processes, e.g. the effect of increased speed of dispatch or the effect of sending formal messages from person to person rather than company to company;
- Legal considerations, such as the potential need for proof of origin, dispatch, delivery and acceptance;
- Implications of publishing externally accessible staff lists;
- Controlling remote user access to electronic mail accounts.

Messaging and Conferencing

When making use of commercial communications facilities or services, methods of authorization and encryption should be employed, when appropriate, to ensure that information is not disclosed to unauthorized individuals.

Portable Computing Devices and Information Media

A. Highly sensitive (confidential) data should never be in unencrypted format on portable computing devices and information media. Individuals requiring remote access to secure information should do so only via the VPN services provided by ITS with completion of VPN use agreement. http://www.fredonia.edu/its/documentation/vpn_employee_agreement.pdf Storage media used to backup and archive information must be secured to prevent compromise of confidentiality or integrity.

B. When using portable computing devices (e.g. laptops, smart phones, personal data assistants) to access information special care must be taken to ensure that device and information accessed by that device is not compromised (ie: unauthorized persons viewing information on the screen).When accessing databases containing confidential information the mobile device user must be careful to never save data to the local hard-drive or other mobile storage device.

Remote Access

Remote connection to SUNY Fredonia's networks is allowed only through a Virtual Private Network (VPN) maintained by ITS for administrative business use access when remote work-related business is an absolute necessity. The VPN application and terms of agreement require data trustee authorization and data steward agreement and understanding of their responsibility to: 1) protect university information by ensuring unauthorized users are not allowed access to SUNY Fredonia internal networks via the VPN; 2) maintain system security patches and anti-virus definitions; 3) secure the equipment used to access SUNY Fredonia information resources; 4) ensure no unencrypted highly sensitive (confidential) information resides on the device.

Modem Usage

Connecting dial-up modems to workstations that are stand-alone or simultaneously connected to SUNY Fredonia's local area network or to another internal communication network is prohibited.

Monitoring

SUNY Fredonia complies fully with Federal and State law. ITS may inspect, monitor or search SUNY Fredonia information systems to comply with subpoenas and search warrants issued by appropriate authorities. Network traffic may be monitored for indications of system compromise or attack.

Part 10. Operations Management

A. Responsibilities, processes and procedures should be established and documented for the management and operation of all information processing facilities. This includes the development of appropriate operating instructions and incident response procedures.
B. Operating procedures for all SUNY Fredonia administrative systems and applications should be documented and maintained. Operating procedures should be treated as formal documents with changes authorized by the supervisor. Documented procedures should also be prepared for housekeeping activities associated with information processing and communication facilities such as computer startup and shut down procedures, back-up, equipment maintenance, computer room management and safety.

Operational Change Control

Changes to SUNY Fredonia administrative information processing facilities and systems must be authorized and controlled through a change management process with appropriate checks and balances. Formal management responsibilities and procedures ensure satisfactory control of all changes to equipment, software or procedural documentation. Operational software will be subject to strict change control. When programs are changed, an audit log containing all the relevant information will be created and maintained. The change control process will consider the following activities:

- Identification and recording of significant changes;
- Assessment of the potential impact of the change;
- Formal approval process for proposed changes;
- Communication of changes to all affected people and organizations; and
- Procedures identifying responsibilities for aborting and recovering from unsuccessful changes.

Incident Management Procedures

An incident management process will be established to track the types, volumes and costs of security incidents and malfunctions. This information will be used to identify recurring or high impact incidents and to record lessons learned. This may indicate the need for additional controls to limit the frequency, damage and cost of future incidents, or to be taken into account in the policy review process.

A. All users of SUNY Fredonia systems should be made aware of the procedure for reporting security breaches, threats, weaknesses, or malfunctions that may have an impact on the security of SUNY Fredonia information. All SUNY Fredonia staff and contractors are required to report any observed or suspected incidents to local management as quickly as possible.
B. Incident management responsibilities and procedures will be clearly defined and documented to ensure a quick, effective and orderly response to security incidents. These procedures will address incidents such as:
   - Information system failures and loss of service;
   - Denial of service;
   - Errors resulting from incomplete or inaccurate business data;
   - Breaches of confidentiality;
   - Loss of integrity of the software or other system component.
C. In addition to normal contingency plans designed to recover systems or services, the incident response procedures will also cover:
   - Analysis and identification of the cause of the incident;
   - Planning and implementation of corrective actions to prevent reoccurrence;
   - Collection of audit log information;
   - Communication with those affected by or involved in the recovery from the incident.
D. SUNY Fredonia senior management will investigate significant security incidents and implement corrective actions to reduce the risk of reoccurrence.

Segregation of Duties

A. Segregation of duties is a method for reducing the risk of accidental or deliberate system misuse. Separating the management or execution of certain duties or areas of responsibility, in order to reduce opportunities for unauthorized modification or misuse of information or services, should be implemented wherever possible, especially in support of the University administrative systems.
B. Small organizations may find this method of control difficult to achieve, but the principle must be applied as far as possible and practicable. Whenever it is difficult to segregate, other controls such as monitoring of activities, audit trails and management supervision must be implemented. It is important that security audit remains independent.
C. Care must be taken that no single person can perpetrate fraud in areas of single responsibility without being detected. The initiation of an event must be separated from its authorization. The following controls must be considered:
   - It is important to segregate activities which require collusion in order to defraud, e.g. raising a purchase order and verifying that the goods have been received;
   - If there is a danger of collusion, then controls need to be devised so that two or more people need to be involved, thereby lowering the possibility of conspiracy.

Separation of Test and Operational Facilities

A. Where possible, separating development, test and operational facilities is important to achieve segregation of the roles involved. Rules for the transfer of software from development to operational status must be defined and documented.
B. Development and test activities can cause serious problems, e.g. unwanted modification of files or system environment, or of system failure. The level of separation that is necessary, between operational, test and development environments, to prevent operational problems must be considered to ensure adequate protection of the production environment. Where possible, a similar separation must also be implemented between development and test functions. In this case, there is a need to maintain a known and stable environment in which to perform meaningful testing and to prevent inappropriate developer access.
C. Where development and test staff have access to the operational system and its information, they may be able to introduce unauthorized and untested code or alter operational data. On some systems this capability could be misused to commit fraud, or introduce untested or malicious code. Untested or malicious code can cause serious operational problems. Developers and testers also pose a threat to the confidentiality of operational information.
D. Development and testing activities may cause unintended changes to software and information if they share the same computing environment. Separating development, test and operational facilities is therefore required to reduce the risk of accidental change or unauthorized access to operational software and business data. The following controls must be considered:
    - Development and operational software must, where possible, run on different computer processors, or in different domains or directories;
    - Development and testing activities must be separated as far as possible;
    - Compilers, editors and other system utilities must not be accessible from operational systems when not required;
    - Different log-on procedures are recommended for operational and test systems, to reduce the risk of error. Users will be encouraged to use different passwords for these systems, and menus should display appropriate identification messages;
    - In situations where separate development and production support staff exist, development staff will only have access to operational passwords where controls are in place for issuing passwords for the support of operational systems. Controls must ensure that such passwords are changed after use.

System Planning and Acceptance

A. Because system and data availability is a security concern, advance planning and preparation must be performed to ensure the availability of adequate capacity and resources. Requirements for new systems must be established, documented and tested prior to their acceptance and use.
B. Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing capability and storage are available. This information will be used to identify and avoid potential bottlenecks that might present a threat to system security or user services.
C. Acceptance criteria based on best practices for new information systems, upgrades and new versions of existing systems must be established. Suitable tests will be performed to ensure requirements have been met prior to formal system acceptance, ITS and senior management will ensure that the requirements and criteria for acceptance are clearly defined, agreed, documented and tested. New technologies are proposed as described at http://www.fredonia.edu/its/pmo/proposals.asp

Protection Against Code

Software and associated controls will be implemented across all SUNY Fredonia systems to prevent and detect the introduction of malicious software. The introduction of malicious software such as a computer virus, network worm programs and Trojan Horses can cause serious damage to networks, workstations and business data. User education will outline the dangers of unauthorized or malicious software. The types of controls and frequency of updating signature files, etc., is dependent on the value and sensitivity of the information that could be potentially at risk. For most SUNY Fredonia workstations, and all systems or servers, virus signature files are updated at least daily.

Information Back-up

Back-ups of critical SUNY Fredonia data and software are performed regularly. A threat and risk assessment is performed at least annually to determine the criticality of business systems, and the time frame required for recovery. Processes will be developed to back-up the data and software. Restoration of data is tested periodically. Formal disaster recovery plans for each critical SUNY Fredonia application will be developed, documented and tested periodically. Test results will inform changes to disaster recovery plans.

Inventory Requirements

An inventory will be maintained of all central IT hosts and servers, together with an assessment of the criticality of the services provided and the sensitivity of the information held on these systems.

System Security Checking

A. Systems and services that process or store non-public information or provide support for critical processes will undergo technical security reviews to ensure compliance with implementation standards and for vulnerabilities to subsequently discovered threats. Reviews of systems and services that are essential to supporting a critical SUNY Fredonia function must be conducted at least once every year. Reviews of a representative sample of all other systems and services must be conducted at least once every 24 months.
B. Any deviations from expected or required results that are detected by the security status review process must be reported to the SUNY Fredonia AVPITS and security staff and corrected immediately. In addition, SUNY Fredonia application owners should be advised of the deviations and must initiate investigation of the deviations (including the review of system activity log records if necessary).

Disposal of Media

Media such as tapes, diskettes, servers, mainframe and PC hard drives which contain sensitive data, must be disposed of in accordance with State Law. Sensitive information could be leaked to outside persons through careless disposal of media. Formal processes must be established to minimize this risk. Media containing sensitive SUNY Fredonia data must be destroyed by incineration, shredding, or electronic erasure of data before disposal consistent with record retention laws.

Part 11. Access Control

Philosophy

The value of data as a university resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its access. Furthermore, increased data access and use improves data integrity because discrepancies are identified and errors are subsequently corrected. As an educational institution with a mission to disseminate knowledge, SUNY Fredonia values ease of access to information, including administrative data. Permission to view or query data contained in the UEDB should be granted to all Data Users for all legitimate business purposes. Update access should be restricted as necessary, but granted to university employees at the location where data are initially received or originates whenever this is feasible. Information specifically protected by law or regulation must be rigorously protected from inappropriate access. Examples include student grades or personnel evaluations that are identifiable with a specific person. To preserve the qualities of integrity, confidentiality and availability, SUNY Fredonia's information assets will be protected by logical and physical access control mechanisms commensurate with the value, sensitivity, consequences of loss or compromise, legal requirements and ease of recovery of these assets.

Data Categorization

As part of the data definition process, Data Stewards assign each data element and each data view in the UEDB to one of three data access categories:

- Non-sensitive (Public data)
- Moderately sensitive (Internal Business use only data)
- Highly sensitive (Confidential data)

Except as noted below, all enterprise data are designated as ***university-internal*** *data for use within the university.* Data users have access to these data by authorization of the Data Trustees and Stewards and by authentication for use in the conduct of university business. These data, while available within the university, are not designated as open to the general public. Where appropriate, Data Stewards may identify elements or views of the UEDB that have no access restriction whatsoever. *Designated* ***Non-sensitive Public*** *data may be released to the general public*. Where necessary, Data Stewards may specify some data elements as limited-access. *Designated* ***Highly sensitive confidential*** *data includes those data for which Data Users must obtain individual authorization prior to access, or to which only* ***need based*** *access may be granted.* When data are designated as Highly sensitive, the Data Steward should provide the following to the ITS DBA unit:

1. Specific reference to the legal, ethical, or externally imposed constraint which requires the restriction.
2. Description of Data User categories that are typically given access to the data, under what conditions, or with what limitations.
3. Documentation of the process for approving and implementing access.
4. Documentation of the process for maintaining security controls.

Note that a data view can possibly have more open access than that of the underlying data elements that comprise it. For example, removal of person-identifying data elements from a view may result in a view that contains some otherwise-restricted data elements but that the Data Steward may now designate as public or university-internal. The appropriate Data Steward in collaboration with ITS is responsible for determining and documenting data access procedures that are unique to a specific information resource, view, or set of data elements.

Data Access Control

Data Trustees and Stewards are responsible for determining who should have access to protected resources within their jurisdiction, and what those access privileges will be (read,

update, etc.).

Any Data User may request that a Data Steward review the restrictions placed on a data element or data view, or review a decision to deny access to limited-access data. The appropriate Data Trustee makes the final determination about restrictions and access rights for enterprise data.

Data Stewards and the ITS DBAs share security administration responsibilities (i.e., the functions of specifying, implementing, and managing system and data access control). To the extent possible, the Data Stewards work together and with the DBAs to define a single set of university procedures for requesting and authorizing access to limited-access data elements in the UEDB. Data Stewards and DBAs are jointly responsible for documenting these access request and authorization procedures. Data Stewards, with the assistance of ITS, are responsible for monitoring and annually reviewing security implementation and authorized access. All Data Users who are cleared for the highly sensitive category of UEDB data must acknowledge (by signed statement or other documented means) that they understand the level of access provided and accept responsibility to both protect their access privileges and to maintain the confidentiality of the data they access. Data Stewards are responsible for defining and implementing procedures to assure that data are backed up and recoverable in response to events that could compromise data integrity. ITS or other university organizations may assist in this effort. Data Stewards may delegate specific security administration activities to operational staff. The Information Security Program Team is responsible for maintaining a plan for security policies and practices and for keeping abreast of security related issues internally within the university community and externally throughout the information technology marketplace.

University enterprise data may be stored on a variety of computing hardware platforms, and is considered part of the UEDB. Every data storage platform must have a defined ***System Administration*** function with a designated system administrator whose responsibilities include:

- Physical site security
- Administration of security and authorization systems
- Backup, recovery, and system restart procedures
- Data archiving
- Capacity planning
- Performance monitoring

User Registration and Management

A. A process will be established to outline and identify all functions of user management, to include the generation, distribution, modification and deletion of user accounts for access to resources. The purpose of this process is to ensure that only authorized individuals or other entities have access to SUNY Fredonia applications and information and that these users only have access to the resources required for authorized purposes.
B. The User Management Process should include the following sub-processes:
    - Enrolling new users;
    - Removing user IDs;
    - Granting privileges to a user;
    - Removing privileges from a user;
    - Periodic reviewing of privileges of users;
    - Periodic reviewing of users enrolled to any system; and
    - Assigning a new authentication token (e.g. password reset processing).

C. The appropriate data trustee or steward or other authorized officer will make requests for the registration, granting, and revocation of access rights for all authorized users.
D. For applications that interact with individuals that are not employed, registered, or appointed by SUNY Fredonia, the information owner is responsible for ensuring an appropriate user management process is implemented where limitation of access is appropriate. Standards for the registration of such external users must be defined, to include the credentials that must be provided to prove the identity of the user requesting registration, validation of the request and the scope of access that may be provided.

Privilege Management

The issuance and use of privileged accounts will be restricted and controlled. Inappropriate use of system privileges is often found to be a major contributing factor to the failure of systems that have been breached. Processes must be developed to ensure that use of privileged accounts is monitored, and any suspected misuse of these accounts is promptly investigated.

User Password Management

Passwords are a common means of authenticating a user's identity to access an information system or service. Password standards are implemented and communicated to ensure all authorized individuals accessing SUNY Fredonia resources follow proven password management practices. These password rules must be mandated by automated system controls whenever possible. See Information Security Program Appendix H for detailed password management information. http://www.fredonia.edu/helpdesk/Policies.asp

Network Access Control

Access to SUNY Fredonia's trusted internal network must require all authorized users to authenticate themselves through use of an assigned user ID and an authentication mechanism, e.g., password, token or smart card, and/or digital certificate.

User Authentication for External Connections (Remote Access Control)

A. Individual accountability is required and must be maintained when SUNY Fredonia's resources are being accessed remotely. Identification and authentication of the entity or person attempting access must be performed across an encrypted connection using such technology as HTTPS and/or a secure VPN tool. Users who need a password reset must be authenticated before the request is granted.
B. For a vendor to access SUNY Fredonia computers or software, individual accountability is also required. For those systems (hardware or software) for which there is a built-in user ID for the vendor to perform maintenance, the account must be disabled until vendor access is required. The activity performed while this vendor user ID is in use must be logged. When the vendor has completed their work, the vendor user ID should be disabled, or the password changed to prevent unauthorized use of this privileged account.
C. Authentication of a user can be accomplished using three techniques: by providing something only the user knows; by providing something the user has; or by identifying the user by a physical characteristic of the user. "Strong authentication," refers to the use of two out of three of these methods to authenticate a user (i.e. password or PIN plus a token card).

D. To maintain information security, SUNY Fredonia requires that individual accountability be maintained at all times, including during remote access where sensitive information is exchanged. For example, remote access to generally available web content on SUNY Fredonia servers does not necessarily require individual accountability. For the purposes of this policy, "remote access" is defined as any access coming into SUNY Fredonia's network from off SUNY Fredonia's private, trusted network. This includes, but is not limited to:
    - Connecting a third party network to the SUNY Fredonia network;
    - VPN access (refer to Part 9, Communications and Network Management, External Internet and VPN Connections).

Segregation of Networks

When the SUNY Fredonia network is connected to another network, or becomes a segment on a larger network, (e.g., the State's SUNYNet network), controls are in place to prevent users from other connected networks from unauthorized access to sensitive areas of SUNY Fredonia's private network. Routers or other technologies are implemented to control access to secured resources on the trusted SUNY Fredonia network.

Operating System Access Control

A. Access to operating system code, services and commands must be restricted to only those individuals who need access in the normal performance of their University roles. Where possible, individuals will have a unique user ID for their use so that activities can be traced to the responsible person. Where avoidable, user IDs should not give any indication of the user's privilege level, e.g., supervisor, manager, administrator.
B. In certain circumstances, where there is a clear business requirement or system limitation, the use of a shared user ID for a group of users or a specific job can be used. Approval by management should be documented in these cases. Additional compensatory controls must be implemented to ensure accountability is maintained.

Application Access Control

Access to SUNY Fredonia applications must be restricted to those individuals who have a business need to access those applications or systems in the performance of their job responsibilities. Access to source code for applications and systems must be restricted. This access should be further restricted so that authorized SUNY Fredonia staff and contractors can access only those applications and systems they directly support.

Monitoring System Access and Use

Sensitive systems and applications are monitored to detect deviation from the access control policy and record events to provide evidence and reconstruct lost or damaged data. Depending on the nature of the events continuous and/or periodic monitoring may be appropriate. Audit logs recording exceptions and other security-relevant events that represent security incidents/deviations from policy are produced and kept to assist in future investigations and access control monitoring. Audit logs will include where technically feasible:

- User IDs;
- Dates and times for logon and logoff;
- Terminal identity or location if possible;
- Records of rejected system access attempts; and

- Records of rejected data and other resource access attempts.

Part 12. Systems Development and Maintenance

A. Software applications are developed or acquired to support SUNY Fredonia in achievement of its mission. These applications generally store, manipulate, retrieve and display information used to conduct SUNY Fredonia activities. SUNY Fredonia departments and customers become dependent on these applications, and it is essential the data processed by these applications be accurate, and readily available for authorized use. It is also critical that the software that performs these activities be protected from unauthorized access or tampering.
B. To ensure that appropriate security is built into all SUNY Fredonia information systems, all security requirements, including the need for rollback arrangements, must be identified during the requirements phase of a project and justified, agreed to and documented as part of the overall business case for a SUNY Fredonia information system.
C. Security requirements and controls must reflect the value of the information assets involved, and the potential damage that might result from a failure or absence of security measures. This is especially critical for Web and other online applications. The framework for analyzing the security requirements and identifying controls to meet them is associated with threat assessment and risk management which must be performed by the information owner and technical support staff.
D. A process must be established and implemented for critical applications to:
    - Understand the business risks and develop a profile of the data to help to understand the risks;
    - Select security measures based on the risk profile and protection requirements;
    - Select and implement specific controls based on security requirements and technical architecture;
    - Provide a method to test the effectiveness of the security controls;
    - Develop processes and standards to support changes, ongoing management and to measure compliance.
E. Controls in systems and applications can be placed in many places and serve a variety of purposes. The specific control mechanisms must be documented at the application level. At a minimum, the security measures that are implemented must be based on the threat and risk assessments of the information being processed.

Input Data Validation

- Data input must be validated. Checks will be applied to the input of business transactions, static data (names, addresses, employee numbers, etc.) and parameter tables. Where feasible the applications should apply the controls as part of the system to ensure consistent, complete, and accurate implementation of the controls in the most efficient manner. The following controls must be considered:
- Dual input or other input checks to detect the following errors:
    1. Out-of-range values;
    2. Invalid characters in data fields;
    3. Missing or incomplete data;
    4. Exceeding upper and lower data volume limits;
    5. Unauthorized or inconsistent control data.
- Validation of the input's compliance with SUNY Fredonia policy, procedures and business rules.
- Periodic review of the content of key fields or data files to confirm their validity and integrity;

- Inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents should be authorized);
- Procedures for responding to validation errors;
- Procedures for testing the plausibility of the input data;
- Defining the responsibilities of all personnel involved in the data input process.

Control of Internal Processing

Data that has been correctly entered can be corrupted by processing errors or through deliberate acts. Validation checks and business rules must be incorporated into systems and automated where possible. The design of applications must ensure that restrictions are implemented to minimize the risk of processing failures leading to a loss of data or system integrity. Specific areas to consider include:

- The use and location in programs of add and delete functions to implement change to data;
- The procedures to prevent programs running in the wrong order or running after failure of prior processing;
- The use of correction programs to recover from failures to ensure the correct processing of data.
- Use of automated checking on the database (triggers) to ensure key validation rules are applied at the database level.

Cryptographic Controls

Use of cryptography for protection of high-risk information must be considered when other controls do not provide adequate protection. Encryption is a technique that can be used to protect the confidentiality of information. It must be considered for the protection of sensitive or critical information. Based on a risk assessment, the required level of protection will be identified taking into account the type and quality of the encryption algorithm used and the length of cryptographic keys employed. To the extent possible, consideration must also be given to the regulations and national restrictions that may apply to the use of cryptographic techniques in different parts of the world. In addition, and to the extent possible, consideration must be given to controls that apply to the export and import of cryptographic technology.

Key Management

Protection of cryptographic keys is essential if cryptographic techniques are going to be used. A secured environment must be established to protect the cryptographic keys used to encrypt and decrypt information. Access to these keys must be tightly controlled to only those individuals who have a business need to access the keys. Loss of confidentiality of a cryptographic key would cause all information encrypted with that key to be considered compromised.

Protection of System Test Data

Test data must be protected and controlled. Live operational data must never be connected to a testing environment. Acceptance testing usually requires large volumes of test data that closely resembles operational data. The use of test data populated from operational databases containing sensitive information requires that those performing the tests are authorized by the appropriate data custodians to access such information.

Change Control Procedures

A. To minimize the possibility of corruption of administrative information systems, strict controls over changes to information systems must be implemented. Formal change control procedures must be enforced. They must ensure that security and control procedures are not compromised, that support programmers are given access only to those parts of a system necessary to perform their jobs, and that formal agreement and approval processes for changes are implemented. These change control procedures will apply to SUNY Fredonia applications as well as systems software used to maintain operating systems, network software, hardware, etc.
B. In addition, access to source code libraries for both SUNY Fredonia applications and operating systems must be restricted to ensure that only authorized individuals have access to these libraries and where practical that access is logged to ensure all activity can be monitored.

Part 13. Business Continuity Planning

A. The scope of this policy is limited to the IT infrastructure, and the data and applications of the local SUNY Fredonia environment. To ensure interruptions to normal SUNY Fredonia business operations are minimized, and critical University business applications and processes are protected from the effects of major failures or disasters, each SUNY Fredonia business unit, in cooperation with the SUNY Fredonia IT organization, must develop, implement and periodically test a local business continuity plan that can meet the recovery requirements of all critical business processes and applications. These interruptions could be caused by natural disasters, accidents, equipment failures, or deliberate actions.
B. The consequences of an extended interruption due to a disaster or security failure must be analyzed to determine the impact on SUNY Fredonia's business, and to determine the recovery time necessary to restore normal business operations. Business continuity management must include controls to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.
C. Business continuity management begins with a business impact analysis and a threat analysis that identifies events that could cause an interruption of business operations and processes. Following the threat identification, a risk assessment must be performed to determine the impact of the threat on the business, likelihood of occurrence, and recovery time necessary for essential SUNY Fredonia business applications and processes. This assessment will consider only those business processes that are information technology related. These activities must be performed with the full involvement of the owners of the business data and business processes.
D. A business continuity plan must be developed by each SUNY Fredonia business unit that addresses each of the following key elements:
    - Understanding the risks SUNY Fredonia is facing in terms of their likelihood and impact on the business, including identification and prioritization of business processes and supporting applications;

- Understanding the impact the interruptions are likely to have on SUNY Fredonia, and establishing the business objectives of information processing facilities;
- Formulating and documenting a business continuity strategy and plans that are consistent with SUNY Fredonia's business objectives and priorities;
- Regular testing and updating of the business continuity plans and processes that have been put in place;
- Ensuring that the management of business continuity is built into SUNY Fredonia's processes and structure. Responsibility for coordinating the business continuity management process should be assigned to appropriate individuals.

E. For all instances where SUNY Fredonia is reliant upon the services of a third party for providing information services, SUNY Fredonia will define the requirements for information availability and recovery. These requirements must be made part of the agreement with the party providing services.
F. Although information security roles and responsibilities may be outsourced to third parties, it is the overall responsibility of each SUNY Fredonia business unit to maintain control of the security of the information assets that it owns.
G. The disaster recovery requirements for the Information Technology (IT) components are based on the business impact analysis performed by SUNY Fredonia business units and academic departments.

Part 14. Compliance

To avoid breaches of any criminal and civil law, statutory or State regulatory or contractual obligations, and security requirements, the design, operation, use and management of information systems may be subject to statutory, regulatory and contractual security requirements. Advice on specific legal or SUNY Fredonia requirements will be provided by SUNY System Administration Legal Counsel.

Intellectual Property Rights

A. Appropriate procedures must be implemented to ensure compliance with legal restrictions on the use of copyrighted material, or material that may have design rights or trademarks. Proprietary software products are generally supplied with license agreements that limit the use of the product to a specific machine or number of users. Controls must be implemented to ensure all aspects of license agreements are met and can be audited. Copyright infringement can lead to legal action which may involve criminal proceedings.
B. For software or other intellectual property that SUNY Fredonia may create that it wants to protect, security measures and copyright procedures must be implemented to protect the State's intellectual property from unauthorized access and/or use.

Safeguarding of SUNY Fredonia Records

A. SUNY Fredonia records must be protected from loss, destruction or unauthorized modification. Some records may need to be retained in a secure manner for extended periods to meet State and Federal legal retention requirements, as well as to support essential business operations. Records and information must be categorized into record types, e.g., accounting records, database records, transaction logs, audit logs, and operational procedures, each with details of retention periods and types of storage media.
B. The *General Retention and Disposition for New York State Government Records* contains guidelines for complying with legal, fiscal, and administrative requirements for records

retention and provides advice on management of records commonly found in state entities. State entities may not dispose of any records without disposition authorization from New York *State Archives and Records Administration* (SARA) consistent with provisions of Section 5705 of Arts and Cultural Affairs Law. SARA issues general schedules to authorize the retention and disposition of records common to some or all state entities.

http://iarchives.nysed.gov/Publications/pubOrderServlet?category=ServicesGovRecs#SGS04

Prevention of Misuse of Information Technology Resources

The information technology resources and the data processed by these resources are provided for SUNY Fredonia business purposes. Management should authorize their use. Any use of ITS facilities for non-business or unauthorized purposes, without management's consent, should be considered a misuse of SUNY Fredonia facilities. Controls must be implemented to detect and report such activity to the appropriate responsible officer.

Compliance with Security Policy

SUNY Fredonia supervisors will ensure that all security processes and procedures within their areas or responsibility are followed. In addition, all business units within SUNY Fredonia will be subject to regular reviews to ensure compliance with security policies and standards.

Part 15. Other Related SUNY Fredonia Policies

- www.fredonia.edu/humanresources/policies.asp
- www.fredonia.edu/helpdesk/policies.asp

Part 16. References

Data Administration Guidelines for Institutional Data, Indiana University
Administrative Data Access Policy, University of Virginia
Standards, Practices, and Procedures, University of Arizona
Data Administration Mission, University of Maryland
Data Classification Policy, Columbia University

Part 17. Policy Change Management and Approval

The original policy was adopted with permission from University of Buffalo and from Virginia Polytechnic Institute and edited for SUNY Fredonia.

Approved by authority of the President's Cabinet March 2010

Payment Card Industry - Data Security Standards

Background

Since the State University of New York at Fredonia ("Fredonia") and related affiliates currently accept credit cards as a reliable and secure means of payment for services and products, Fredonia is required to obtain and maintain PCI-DSS compliance for each credit card processing entity ("merchant") across campus. The Payment Card Industry Data Security Standards (PCI - DSS) is a mandated information security standard for organizations that store, process, access or transmit cardholder data (CHD or credit card numbers) in any format (e.g. electronic, paper-based, etc). A data security breach that stems from a gap in PCI compliance is, by definition, a breach of the contract between the merchant and the card brands. Consequences for having a breach of cardholder data include substantial fines up to $500,000 (per card brand) as well as forensic costs and reparation for the fraudulent transactions.

Purpose

This standard is intended to prevent the loss or disclosure of customer information including credit card numbers. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the unit and Fredonia.

Standard

It is Fredonia's standard to allow acceptance of credit cards as a form of payment for goods and services. Fredonia requires all departments that accept credit cards to do so only in compliance with credit card industry standards and in accordance with the procedures outlined in this document and other established requirements.

Roles and Responsibilities

The path to obtaining and retaining PCI-DSS compliance is complex and can not effectively be achieved without a strong partnership between all parties responsible for the various activities and components. Although the Division of Finance and Administration together with Academic Affairs - Information Technology Services (ITS) take a joint role and joint responsibility in leading Fredonia's PCI-DSS compliance effort, all campus entities are responsible for adhering to all aspects of PCI-DSS compliance .

Academic Affairs - Information Technology and Services (ITS) responsibilities include:

- Recommend, install, and maintain all information technology systems and services used in the storage, processing, transmission of, and access to credit card information. This includes all networks, card swipe devices, computer systems, network segments, firewalls, etc. used in the processing of credit cards.
- Develop and implement a service offering that includes the technology and support to achieve and maintain PCI-DSS compliance while minimizing PCI-DSS scope and associated costs.
- Investigate new, more secure, and less intrusive technologies used in the processing of credit card transactions and make recommendations to Finance and Administration and other Business Partners when said technologies exist and may be adoptable by Fredonia.

Finance and Administration's responsibilities include:

- Draft and follow documented business practices and procedures outlining how credit cards are taken and processed at Fredonia.
- Set PCI-DSS processing standards including who is allowed to take credit cards as a form of payment at Fredonia and outline how such processes will be constructed.
- Enforce best practices on how credit cards are processed and who has the authority to take credit cards as a form of payment at Fredonia.

Finance and Administration and ITS joint responsibilities include:

- Co-chair the campus effort of drafting the PCI-DSS compliance project plan that defines the steps required to ensure the University becomes and maintains PCI-DSS compliance.
- Devise training schedules, review training materials, assist in the delivery of training sessions (via Fredonia staff or assisting with coordinating with external consultant).
- Develop strategies for achieving and maintaining PCI-DSS compliance for on-campus merchants who have complex business processes.
- Monitor, support, and communicate with merchant areas to ensure any and all corrective actions are properly applied in a timely manner.
- Attend conferences and workshops as to maintain a modern, working knowledge of PCI-DSS compliance efforts throughout higher education.

Merchant Department Responsible Person (MDRP) responsibilities include:

- Comply with the Fredonia Payment Card Industry - Data Security Standards (PCI-DSS).
- Attend the required PCI-DSS Merchant Annual Training.
- Report any security incidents to the Information Security Office.

- Communicate on an on-going basis of any changes within their departmental procedures and practices as they relate to PCI-DSS compliance.

Information Security Committee:

- The Information Security Committee co-chairs are responsible for the enforcement of this standard and related procedures.
- The Information Security Committee co-chairs will have the Cabinet level authority to prohibit credit card processing for campus community and University departments in the event they are found to be non-compliant.

PCI-DSS Sub-Committee:

- The PCI-DSS sub-committee will be responsible for the on-going compliance reviews, projects and initiatives required for Fredonia (and related affiliates) to maintain PCI-DSS compliance.
- The PCI-DSS sub-committee will report to the Information Security Committee and be co-chaired by the Vice President of Finance and Administration's designee and the Information Security Officer.
- The PCI-DSS sub-committee will provide updates and make recommendations to the Information Security Committee as to the status of compliance efforts.
- Campus community merchants representing other Fredonia divisions and affiliates (e.g. Research Foundation, etc.) will be requested to attend committee meetings and trainings as needed.

Sub-Committee Membership:

Title	**Division or Affiliate**
Information Security Officer	Academic Affairs - Information Technology Services
Director of Information Technology	Faculty Student Association
Associate Vice President of Information Technology & Chief Information Officer	Academic Affairs - Information Technology Services
Director of Student Accounts	Finance and Administration
Director of Internal Control	Finance and Administration

Scope

The Fredonia Payment Card Industry-Data Security Standards (PCI-DSS) apply to all faculty, staff, students, organizations, third-party vendors, individuals, systems and networks involved with credit card handling. This includes transmission, storage and/or processing of credit card numbers, in any form (electronic or paper), on behalf of Fredonia or a Fredonia affiliate.

Authority

The President's Cabinet has delegated their authority to enforce this standard to the Co-Chairs of the Information Security Committee.

Glossary

Term	Definition
Payment Card Industry Data Security Standards (PCI-DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the 5 major Credit Card Brands: Visa, MasterCard, American Express, Discover, JCB
Card Brands	Visa, MasterCard, American Express, Discover, JCB
Cardholder	Someone who owns and benefits from the use of a membership card, particularly a credit card.
Card Holder Data (CHD)	Those elements of credit card information that are required to be protected. These elements include Primary Account Number (PAN), Cardholder Name, Expiration Date and the Service Code.
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or credit card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.
Cardholder Name	The name of the Cardholder to whom the card has been issued.

Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of credit card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
CAV2, CVC2, CID, or CVV2 data	The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Disposal	CHD must be disposed of in a certain manner that renders all data un-recoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, USB storage devices,(Before disposal or repurposing, computer drives should be sanitized in accordance with applicable Fredonia policies. The approved disposal methods include the following: Cross-cut shredding, Incineration, Approved shredding or an

	approved (physical or electronic) contracted disposal service.
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by the (institution) to accept credit cards and has been assigned a Merchant identification number.
Merchant Department Responsible Person (MDRP)	An individual within the department who has primary authority and responsibility within that department for credit card transactions. This individual is typically the department Director or Chairperson.
Database	A structured electronic format for organizing and maintaining information that is accessible in various ways. Simple examples of databases are tables or spreadsheets.

Administration and Department Payment Card Standard Operating Procedures

Payment Card Industry
Data Security Standard (PCI DSS)
PCI DSS Version 3.2

Rev. 090117

Contents

Purpose

This document and additional supporting documents represents the State University of New York at Fredonia's ("Fredonia") Standard Operating Procedures (SOP) to prevent loss or disclosure of sensitive customer information including payment card data. Failure to protect customer information may result in financial loss for customers, suspension of credit card processing privileges, and fines imposed on and damage to the reputation of the department and the institution.

PCI DSS

The Payment Card Industry Data Security Standards (PCI DSS) is a mandated set of requirements agreed upon by the five major credit card companies: VISA, MasterCard, Discover, American Express and JCB. These security requirements apply to all payment card transactions and the merchants/organizations that accept these cards as forms of payment. Further details about PCI can be found at the PCI Security Standards Council website (https://www.pcisecuritystandards.org).

In order to accept payment card transactions, Fredonia must prove and maintain compliance with the Payment Card Industry Data Security Standards. The Fredonia Payment Card Industry Data Security Standards and additional supporting documents define the requirements for compliant processing, transmitting, storage, and disposal of cardholder data during payment card transactions. These are required in order to reduce the institutional risk associated with the administration of card payments by all departments and to ensure proper internal control and compliance with the PCI DSS.

Visa Cardholder Information Security Plan (CISP)

Visa Inc. instituted the Cardholder Information Security Program (CISP) in June 2001, CISP is intended to protect Visa cardholder data - wherever it resides - ensuring that members, merchants, and service providers maintain the highest information security standard. In 2004, the CISP requirements were incorporated into the Payment Card Industry Data Security Standard (PCI DSS).

MasterCard Site Data Protection Program (SDP)

The MasterCard Site Data Protection Program, similar to the above Visa CISP, was the original compliance program defining the data security and compliance validation requirements to protect MasterCard payment account data. This program was also incorporated into the PCI DSS when that program was original created.

Scope/Applicability

The Fredonia Payment Card Industry Administration and Department SOP apply to all faculty, staff, students, organizations, affiliates, third-party vendors, individuals, systems, and networks involved with payment card handling. This includes transmission, storage, and/or processing of payment card data, in any form (electronic or paper), on behalf of Fredonia. Purchasing Card (aka P-card) data does not fall under the PCI DSS requirements, but shall be protected in a similar manner, particularly as it relates to storage and disposal of cardholder data.

Authority

As a part of that management, the Fredonia PCI DSS Sub-Committee will direct the development and implementation of Fredonia's policies and procedures. The Chairs of the Fredonia Information Security Committee are responsible for enforcement of these procedures as designated by the President.

Standard Operating Procedures

In the course of doing business at Fredonia, including affiliated organizations, it may be necessary for a department or other unit to accept payment cards. Fredonia requires all departments that accept payment cards to do so only in accordance with the Fredonia Payment Card Industry Data Security Standards and the following procedures.

1. Card Acceptance and Handling

The opening of a new merchant account for the purpose of accepting and processing payment cards is done on a case by case basis. Any fees associated with the acceptance of the payment card in that department will be charged to the individual merchant. NOTE: Departments may only use the services of vendors (Third Party Service Providers) which have been approved by PCI DSS Sub-Committee to process payment card transactions regardless of whether the transaction is point of sale (POS), mail/telephone order, or internet-based.

1.1. Interested departments or merchants should contact the PCI DSS Sub-Committee to begin the process of accepting payment cards. Steps include:
   1.1.1. Completion of an "Application to become a Merchant Department" and designating a "Merchant Department Responsible Person". Any department accepting payment cards on behalf of the institution or related foundation must designate an individual (Merchant Department Responsible Person) within the department who will have primary authority and responsibility within that department for payment card transactions. The department should also specify a back-up, or person of secondary responsibility, should matters arise when the primary is unavailable.
   1.1.2. Completion of Fredonia PCI DSS Merchant training.
   1.1.3. Review and acknowledgement of the "Fredonia Payment Card Industry Data Security Standards", including proof of ongoing compliance with all requirements of the policy.

1.2. Specific details regarding processing and reconciliation will depend on the method of payment card acceptance and type of merchant account. Merchants are responsible for the reconciliation of any associated accounts on an ongoing basis.

1.3. All service providers and third party vendors providing payment card services must be PCI DSS compliant. Departments who contract with third-party service providers must maintain a list that documents all service providers and:
   1.3.1. Ensure contracts include language stating that the service provider or third party vendor is PCI compliant and will protect all cardholder data.
   1.3.2. Annually audit and obtain an Attestation of PCI Compliance (AoC) from all service providers and third-party vendors. A lapse in PCI compliance could result in the termination of the relationship.

2. Payment Card Data Security

All departments authorized to accept payment card transactions must have their card handling procedures documented and made available for periodic review. Departments must have in place the following components in their procedures and ensure that these components are maintained on an ongoing basis.

PROCESSING AND COLLECTION

1.1. Access to cardholder data (CHD) is restricted to only those users who need the data to perform their jobs. Each merchant department must maintain a current list of employees with access to CHD and review the list periodically to ensure that the list reflects the most current access needed and granted.

1.2. Equipment used to collect cardholder data is secured against unauthorized use or tampering in accordance with the PCI DSS. This includes the following:

1.2.1. Maintaining an inventory/list of devices and their location;

1.2.2. Periodically inspecting the devices to check for tampering or substitution;

1.2.3. Training for all personnel to be aware of suspicious behavior and reporting procedures in the event of suspected tampering or substitution.

1.3. Email must never be used to transmit payment card or personal payment information, nor should it be accepted as a method to supply such information. In the event that it does occur, disposal as outlined below is critical. If payment card data is received in an email then:

1.3.1. The email should be replied to immediately with the payment card number deleted stating that "Fredonia does not accept payment card data via email as it is not a secure method of transmitting cardholder data".

1.3.2. Provide a list of the alternate, compliant option(s) for payment.

1.3.3. Delete the email from your inbox and also delete it from your email Trash.

1.4. The use of fax machines to transmit payment card information to a merchant department is strictly prohibited.

STORAGE AND DESTRUCTION

1.5. Cardholder data, whether collected on paper or electronically, is protected against unauthorized access.

1.6. Physical security controls are in place to prevent unauthorized individuals from gaining access to the buildings, rooms, or cabinets that store the equipment, documents, or electronic files containing cardholder data.

1.7. No database, electronic file, or other electronic repository of information will store the full contents of any track from the magnetic stripe, or the card validation code.

1.8. Portable electronic media devices should not be used to store cardholder data. These devices include, but are not limited to, the following: laptops, compact disks, floppy disks, USB flash drives, personal digital assistants, and portable external hard drives.

1.9. Merchants must refrain from retaining Cardholder data. CHD must be destroyed immediately using a PCI DSS-approved method of destruction. A regular schedule of deleting or destroying data should be established in the merchant department to ensure that no cardholder data is kept..

3. Risk Assessment

Implement a formal risk assessment process in which current threats and vulnerabilities to the institution's network and processing environment, including staff, are analyzed. Risk assessments must be conducted annually. Information Technology should conduct the risk assessment of the infrastructure and threats; departments that accept payment cards should also conduct an assessment of their physical environments and assess risks to the payment environment. Address all threats with mitigation tasks, timelines and/or acceptance statements. Prepare and maintain documented output from the risk assessment exercise(s).

4. Incident Response

In the event of a breach or suspected breach of security, the department or unit must immediately execute the Fredonia Payment Card Incident Response Plan. The plan must include notifications, staff requirements, and handling procedures. If the suspected activity involves computers (hacking, unauthorized access, etc.), immediately notify the Information Security Office at (716) 673-4725. The Incident Response Plan should be reviewed and tested at least annually.

5. Policy and Training

Ensure policy and procedure documentation governing cardholder data exists and that it covers the entirety of the PCI DSS. Document users' acknowledgement of understanding and compliance with all policies and procedures annually. Ensure training on the PCI DSS and overall information security is provided to all staff members with access to cardholder data and/or the processing environment upon hire, and at least annually thereafter.

6. Sanctions

Failure to meet the requirements outlined in the Fredonia Payment Card Industry Standard and this procedure will result in suspension of the physical and, if appropriate, electronic payment capability for the affected merchant(s). In the event of a breach or a PCI violation the payment card brands may assess penalties to the Merchant's bank which will likely then be passed on to Fredonia. Any fines and assessments imposed will be the responsibility of the impacted division. A one-time penalty of up to $500,000 per card brand per breach can be assessed as well as on-going monthly penalties.

Persons in violation of this policy and procedure are subject to sanctions, including the potential loss of computer or network access privileges, disciplinary action, suspension and termination of employment, as well as legal action. Some violations may constitute criminal offenses under local, state, or federal laws. The Fredonia PCI DSS Sub-Committee will carry out its responsibility to report such violations to the appropriate authorities.

Interpretations

The authority to interpret these procedures rests with the State University of New York at Fredonia President and the President's Cabinet.

Glossary

Term	Definition
Cardholder	Non-consumer or consumer customer to whom a payment card is issued to or any individual authorized to use the payment card.
Cardholder Data (CHD)	At a minimum, cardholder data consists of the full PAN. Cardholder data may also appear in the form of the full PAN plus any of the following: cardholder name, expiration date and/or service code.
Cardholder Data Environment (CDE)	The people, processes and technology that store, process, or transmit cardholder data or sensitive authentication data.
CAV2, CVC2, CID, or CVV2 data	The three- or four-digit value printed on or to the right of the signature panel or on the face of a payment card used to verify card- not-present transactions.
Disposal	CHD must be disposed of in a certain manner that renders all data unrecoverable. This includes paper documents and any electronic media including computers, hard drives, magnetic tapes, and USB storage devices. Before disposal or repurposing, computer drives should be sanitized in accordance with Information Management and Cyber Security Policy. The approved disposal methods are: ● Cross-cut shredding, Incineration, Approved shredding or disposal service
Expiration Date	The date on which a card expires and is no longer valid. The expiration date is embossed, encoded or printed on the card.
Magnetic Stripe (i.e., track) data	Data encoded in the magnetic stripe or equivalent data on a chip used for authorization during a card-present transaction. Entities may not retain full magnetic-stripe data after transaction authorization.
Merchant Department	Any department or unit (can be a group of departments or a subset of a department) which has been approved by Fredonia to accept payment cards and has been assigned a Merchant identification number.
Payment Card Industry Data Security Standards (PCI DSS)	The security requirements defined by the Payment Card Industry Security Standards Council and the five major payment card brands: ● Visa, MasterCard, American Express, Discover, JCB
Primary Account Number (PAN)	Number code of 14 or 16 digits embossed on a bank or payment card and encoded in the card's magnetic strip. PAN identifies the issuer of the card and the account, and includes a check digit as an authentication device.

PIN/PIN block	Personal Identification Number entered by cardholder during a card-present transaction, and/or encrypted PIN block present within the transaction message.
Service Code	The service code that permits where the card is used and for what.
Sensitive Authentication Data	Additional elements of payment card information that are also required to be protected but never stored. These include Magnetic Stripe (i.e., track) data, CAV2, CVC2, CID, or CVV2 data and PIN/PIN block.
Affiliate	Any entity that utilizes the State University of New York at Fredonia's electronic services or computing infrastructure with a legitimate business purpose to process credit card payments.