INTENT

The intent of this policy is to define the mechanisms by which data stored on Edinboro University-owned computing systems and utilized by University employees and students is secured from threats to its integrity and protected from unauthorized access.

SCOPE

This security policy applies to all computing platforms, local area networks, systems, and applications used to process Edinboro University of Pennsylvania administrative information. It also applies to the users of those systems and applications, including those who install, develop, maintain, and administer those systems and applications for the University. The policy also applies to all data extracts and reports derived from University data including those which might be stored on paper or other media.

All users of University-related technology facilities and resources must abide by all applicable University, State, and Federal guidelines, policies, regulations, statutes, and procedures pertaining to confidentiality and privacy, including, but not limited to the Family Educational Rights and Privacy Act of 1974 (FERPA) and the Graham-Leach-Bliley Act of 2000.

POLICY

Edinboro University of Pennsylvania administrative information resources are a valuable University asset and must be managed accordingly to ensure their integrity, security, and availability for appropriate educational and business activities. Of paramount importance in carrying out this mission is to establish basic information security policies and standards for managing Edinboro
University administrative information, while providing both access and security. Any person, group, or custodian accessing University information must recognize their responsibility to preserve the security and confidentiality of this information. Such information shall be used only for conducting University business or as appropriately authorized.

**Information Security Responsibilities**

The Chief Information Technology Officer (CITO), by providing leadership to University Technology and Communications functions, is responsible for ensuring that Edinboro University of Pennsylvania has adequate information security and that this policy is observed. To that end, the Information Security Officer, as designated by the CITO, has responsibility for developing and publicizing the information security policy and monitoring its compliance. The Information Security Officer coordinates the standards, procedures, and guidelines necessary to administer access to University information resources. The Information Security Officer works in conjunction with information resource owners, the University Data Administrator, and functional users to protect these resources.

All administrative information is the property of Edinboro University of Pennsylvania, unless otherwise stated in a contractual agreement. Following is a summary of responsibilities of those units and/or individuals using or supporting University administrative information.

**A. Enterprise-wide Security Administration**

The Enterprise Systems group within Technology and Communications is responsible for managing information security standards, procedures, and controls intended to minimize the risk of loss, damage, or misuse of Enterprise Systems-supported electronic data. Enterprise Systems is responsible for:

- Developing and maintaining an administrative information security policy
- Establishing and maintaining high-level standards and related procedures for access to University administrative information and systems
- Securing information managed by Enterprise Systems and implementing access as authorized by Data Custodians
- Assisting Data Custodians in identifying and evaluating information security risks
- Performing risk analysis for Enterprise Systems-developed projects
- Selecting, implementing, and administering controls and procedures to manage information security risks
- Distributing security report information in a timely manner to Unit Security Contacts, Data Custodians, and appropriate University administrators
- Serving as System Administrator(s) for all information residing on Enterprise Systems servers
B. Data Custodians
The Data Custodians function as trustees of a portion of the University's administrative information and are responsible for making decisions related to the development, maintenance, operation, and access to the application and data associated with that business unit. Examples include Records and Registration (student data), Finance (financial data), Bursar (accounts receivable data), and Financial Aid. A Unit Head may delegate custodial duties to an individual within that unit. Data Custodians:

- Maintain detailed knowledge of the data within their trust
- Interpret pertinent laws and University policies to classify data and define its level of sensitivity
- Define required levels of security
- Develop guidelines for requesting access
- Review and authorize requests for access to information
- Establish measures to ensure data integrity
- Provide data descriptions to inform data users about available shareable data, how to access the data, and what the data means
- Promote accurate interpretation of administrative data and publicize the rules and conditions that could affect the accurate presentation of that data
- Review usage information
- Assist with disaster recovery planning for their unit
- Define criteria for archiving data to satisfy retention requirements

C. System Administrators
System Administrators are generally responsible for the hardware and software environments used to store any administrative information. System Administrators are responsible for:

- Developing, maintaining, and documenting an internal security plan to include data integrity, user authentication, backup, recovery, and continuity of operations
- Ensuring that access to data and applications is secure as defined by the Data Custodians
- Providing adequate operational controls to ensure data protection
- Ensuring that access requests are authorized
- Communicating appropriate use, and consequences of misuse, to users who access the systems or data
- Modifying access when employees terminate or transfer
- Protecting sensitive files and access control files from unauthorized activity
- Maintaining access and audit records
- Creating, reviewing, and following up on security violation reports
Any unit maintaining electronic administrative systems, applications, or data is responsible for implementing a level of security consistent with this policy. This applies to all servers and workstations owned by and operated within any business unit.

For those systems under its control, Enterprise Systems is responsible for the operating system and application components, including production, system and test libraries, system and test data, and data dictionaries. For systems not managed by Enterprise Systems, system administration is the responsibility of the end user/business unit.

D. Unit Heads

All Unit Heads are responsible for ensuring that security policies are implemented within the unit. These duties may be delegated; however, it is the responsibility of the Unit Head to:

- Ensure that unit employees are trained and understand security policies, procedures, and responsibilities, including FERPA
- Approve appropriate data access, allowing staff to complete business-related assignments
- Review, evaluate, and respond to all security violations reported against staff, and take appropriate action
- Communicate to appropriate campus and University departments when employee departures, arrivals, and changes affect computer access
- Assign a liaison between the Data Custodians and System Administrators
- Ensure security procedures are in place to protect information assets under their control. Such procedures would include access control and virus protection for workstations, applications, local area networks, etc.

E. Information Usage and User Responsibilities

Anyone accessing University administrative data is personally responsible for proper use of the resulting available information.

University employees who access data are responsible for:

- Complying with University information security standards and procedures in the use, storage, dissemination, and disposal of data
- Protecting data from unauthorized access
- Reporting information security violations to their Unit Head
- Reporting data integrity errors to the appropriate management level
- Maintaining the accurate presentation of administrative data, and for the consequences of any intentional misrepresentation of that data

Students are responsible for safeguarding their account passwords and Personal Identification Numbers (PINs) that grant them access to their personal information.
While the University has discontinued using social security numbers as student identifiers, one of the largest security risks may be the possible non-standard practices concerning social security numbers, e.g. continued reliance by some University employees on the use of social security numbers. Social security numbers are considered protected information under both GLB and FERPA. By necessity, student social security numbers still remain in the University student information system. Their use should be on an exceptional or as-necessary basis.

Data Classification

The University categorizes the information it collects and maintains based on that information's sensitivity and importance to administrative operations. It should be noted that sensitivity is an attribute of the data itself, and not related to system or location. This classification system is used to determine adequate and appropriate protection controls.

A. General

Not all information resources can be, or must be equally protected. To ensure that University protection efforts are cost effective, all administrative information resources will be classified based on sensitivity and risk. Access control should be consistent with the classified value of the resources to be protected and the severity of the threat to them.

Administrative information maintained by Enterprise Systems will be classified in accordance with the security levels described in this document. Enterprise Systems will manage and coordinate this activity with the Data Custodians and will maintain authorization, access, and audit records. These classifications will be maintained throughout the University. The following guidelines apply:

- The appropriate Data Custodian must classify administrative data under their control
- The Unit Head is responsible for ensuring that the level of protection for administrative information used within the unit is consistent with standards established within this document
- The System Administrators are responsible for implementing these policies and standards

B. Categories

Different types of data require different levels of security. The University classifies data into three categories: Public, Proprietary, and Restricted. It is the Data Custodian's responsibility to establish authentication and authorization guidelines for custodial data. Please note that:
• Public data can generally be made available or distributed to the general public
• Proprietary data is for internal University use as deemed appropriate
• Restricted (moderately or highly sensitive) data is intended to be used only by individuals who require it in the course of performing their University responsibilities

Access Control

All users of University administrative data must be authorized to access the appropriate systems and their resources. Access is controlled and monitored in accordance with University policy. Copies of data, regardless of location, have the same data security and access control requirements as operational data. The elements involved in controlling and monitoring this access include identification, authentication, and authorization.

A. Protection Level
   Access control will be consistent with the assigned classification. The following generalizations apply:

   • Public data may not require an authentication, although authentication may be used to track resource usage.
   • Authentication is required for access to Proprietary data; however, it is possible that authorization may not be required.
   • Access to Restricted data requires both authentication and authorization. Depending on the sensitivity of the data, several authorizations may be required before access is granted.

B. Legally Restricted or Limited-access Data
   Access by University employees, or those in University-related entities, to proprietary or restricted data, either directly, or indirectly by requesting reports containing restricted data, requires approval of the appropriate Data Custodian(s).

C. Identification
   User identifiers (ID) are used to identify people, data, and resources for tracking access to the Administrative Information. All system users will be assigned a unique ID to use for accessing all systems, program products, and applications. User IDs are not to be shared. Users are responsible for maintaining the security of their IDs and all activity occurring under those IDs.

D. Authentication
   Authentication ensures an identity. Each ID requires a technique for validating identity such as a password or a Personal Identification Number (PIN).
E. Authorization
Only those users who have valid business reasons (as determined by the Data Custodians) for accessing administrative information will be granted access privileges appropriate to that user’s job function. Access is to be used only for the specific business purposes required for processing the data. Access is granted by means of a computer account and database account, which also serves as identification.

F. Security Monitoring

- Event Logging: All accesses that are denied by a network security system will be logged. Each denied access is considered a security "event," but not necessarily a security "violation." System administrators will produce a log of all security events from the prior activities. The logs will display events chronologically and by ID. System Administrators then conduct a review of each log for unusual security events and will further investigate unusual events.
- Violation Response: A security violation is any event which:
  - Fails to comply with data security standards.
  - Represents an apparent or real effort to undermine, override, or otherwise circumvent security standards or controls.

Data Transport Controls

Units supporting Internet, EDI, LANs, and WANs that access and use administrative information must observe appropriate data transport controls to ensure that the information is protected in a manner consistent with that prescribed by federal and state laws and University regulations. Proprietary or Restricted administrative information transmitted over any communication network must be encrypted and its access controlled, secured, and auditable, or at least be transmitted using Virtual Private Network links.

All University administrative information must reside on systems located behind firewalls.

Direct access to administrative databases must not be available through the firewall from locations outside the campus unless done over special Virtual Private Network links.

Servers supporting credit card services must not be visible or directly accessible by outside networks. These servers must accept transactions from only specific internal network addresses.
Operational Controls

System Administrators are responsible for implementing operational software and hardware security controls that provide the security required to protect administrative information.

A. Backup
All critical University administrative information whether located on centrally managed servers, or on systems located in user offices, must be backed up on a regular basis. The frequency established by each System Administrator is influenced by the frequency with which the data changes and the effort required to recreate information, if it is lost.

B. Recovery
All backups of critical data must be tested periodically to ensure that they still support full system recovery. System Administrators must document all restore procedures, and test them annually. Backup media must be retrievable within 24 hours, 365 days a year.

C. Off-site Storage
All backup copies destined for off-site storage should be moved within 24 hours of origination. Off-site is synonymous with "out of the building." The off-site storage location must provide evidence of adequate fire and theft protection and environmental controls.

D. Data Retention
Data Custodians are responsible for defining and documenting the length of time data must be retained. The retention period, legal requirement(s), responsible party(ies), and source of legal requirement should be specified. System Administrators are responsible for ensuring that these requirements are implemented.

E. Contingency and Disaster Planning
Each unit that maintains University administrative data must possess a documented and tested contingency and disaster recovery plan, which addresses the possibility of short- and long-term loss of computing services. Such a plan should include all procedures and information necessary to return computing systems to full operation in the event of a disaster.

F. Physical Security
Access to every office, computer room, and work area containing sensitive information must be physically restricted. All multi-user computing, and/or communications equipment, must be housed in locked rooms to prevent tampering and unauthorized access.
E. Separation of Duties
There shall be a distinct separation of job duties and responsibilities so that no one person has the authority and the ability to circumvent normal checks and balances. For applications containing mission-critical, financial, or confidential data, responsibility for maintaining the database and the system software will be separated.

F. Disposal of Equipment
All data on hard drives and associated peripherals is to be treated as confidential. This poses a threat if the equipment is being removed from service and the hard drive is recovered and falls into the wrong hands. Therefore all data must be cleansed from these devices as follows:

- All personal computers, laptops, servers, and other peripheral devices equipped with hard drives must have the hard drive erased or formatted to binary zeros before the unit is removed from its location.
- Hard drives must be physically removed from any unit designated as surplus or destined for recycling. The hard drive should be physically destroyed.

Violations
Violation of any provision of this policy may result in:

- limitation of an individual's access to some or all University systems;
- initiation of legal action by the University including, but not limited to, criminal prosecution under appropriate State and Federal laws;
- requirement of the violator to provide restitution for any improper use of service; or
- disciplinary sanctions in accordance with University policy

Policy Development and Maintenance
This section describes the process for developing, maintaining, and implementing policy and procedures for accessing, storing and using administrative information.

A. Security Advisory Council
Enterprise Systems is responsible for administering this policy with the advice of the Technology and Communications Advisory Council and the Enterprise Resource Planning Team which includes representatives from all University divisions.
B. Changes to Policy and Standards
All requests to change policies and standards must be received in writing and contain brief, factual comments describing the problem, recommendations, and benefits of the proposed change.

C. Exceptions to Policy and Standards
If an exception is required, a written request including a description of and justification for the exception is sent to Technology and Communications, who will forward it to the Enterprise Resource Planning Team for review. All exceptions require the approval of all affected Data Custodians and the Enterprise Resource Planning Team. Technology and Communications retains all such requests for audit purposes.