PENSACOLA STATE COLLEGE
MANUAL OF PROCEDURES

Procedure Title:	Cyber Risk	Number 138
Related Policy:	Cyber Risk – 6Hx20.1.033	Page Page 1 of 11

Pensacola State College has established standards for the protection and security of information, and for the use of information and technology resources. Information is secure only when its integrity can be maintained, its availability ensured, and its confidentiality preserved. Security procedures protect information from unauthorized viewing, modification, dissemination, or destruction and provide recovery mechanisms from accidental loss. The security of information is the responsibility of all people who are authorized to access it. All employees are expected to abide by these standards.

I. Purpose

The procedure will provide details of standards for the use of information and resources. The College affirms that as part of its procedure it will protect customer confidentiality and employee privacy in accordance with applicable laws and personnel policies. Each person subject to this procedure will affirm that he or she has read, that he or she understands, and that he or she intends to comply with the provisions stated herein. The affirmation of this statement is a requirement for obtaining access to the organization’s data systems and networks.

II. Procedure

A. Scope and Application

1. The Information Technology Services (ITS) Department is responsible for establishing and maintaining organizational information security policies, standards, guidelines, and procedures. The focus of these activities is on information, regardless of its form, the technology used to manage it, where it resides, and which people possess it.
2. The procedure applies to employees, customers, volunteers, vendors, contractors, Board of Trustees members, affiliates, and any others who use College information resources or who have access to College information. The procedure applies equally to any information of the organization, including but not limited to electronic data, written or printed information and any other intellectual property of the organization. The information resources include hardware, software, manuals and office equipment. All individuals agree not to disclose or not to use information improperly or unethically for personal or professional gain.

B. Introduction

1. Critical Business Function

Reliable information and information systems are necessary for the performance of many of the essential activities of the College. If there were to be a serious security problem with College information or information systems, the College could suffer serious consequences, such as legal liability and degraded reputation. Accordingly, information security is a critical part of the College's business environment.

2. Supporting Business Objectives

This procedure has been prepared to ensure that Pensacola State College is able to support its educational mission. This document is also intended to support the integrity of the College's reputation. Because the prevention of security incidents is considerably less expensive than correction and recovery, adherence to this procedure may also reduce costs over time.

3. Consistent Compliance

A single unauthorized exception to security measures can jeopardize users, the entire organization, and external business partners. The interconnected nature of information systems requires that all users observe a minimum level of security. This document defines that minimum level of due care. In some cases these requirements will conflict with other objectives, such as improved efficiency and reduced costs. The College has examined these tradeoffs and concluded that the minimum requirements defined in this document are appropriate for all workers at the College. As a result, as a condition of continued employment, all workers (employees, contractors, consultants, temporaries, volunteers) must consistently observe the requirements set forth in this document.

4. Team Approach

Because information and information systems are distributed to desktop PCs and sometimes used in remote locations via laptops and tablets, the user performs an essential role involving information security. Information security is a team effort requiring the participation of every worker who comes in contact with the College and its information systems.

5. Shared Responsibility

Every user must understand College information security policies and procedures, and must agree to perform his or her work according to these policies and procedures. Responsibility for information security on a day-to-day basis is everyone's duty. Specific responsibility for information security is not solely vested in the ITS Department.

C. Information Security Responsibilities and Procedures

1. Information Owners

Administrators in College departments must be designated as the Owners of all types of information used for regular business activities. When information Owners are not clearly implied by organizational design the Chief Information Officer (CIO) will make the designation. Information Owners do not legally own the information in question, they are instead members of the College administrative team that make decisions on behalf of the organization.

Information Owners, or their delegates, are required to make the following decisions and perform the following activities:

- a. Approve information-oriented access control privileges for specific job profiles.
- b. Approve information-oriented access control requests which do not fall within the purview of existing job profiles.
- c. Select a data retention period for their information, relying on legal advice.
- d. Designate a system-of-record (original source) for information from which all management reports will be derived.
- e. Select special controls needed to protect information (such as additional input validation checks or more frequent back-up procedures).
- f. Define acceptable limits on the quality of their information (accuracy, timeliness, time from capture to usage, etc.).
- g. Approve all new and different uses of their information.
- h. Approve all new or substantially enhanced application systems that use their information before these systems are moved into operational status.
- i. Review reports on system intrusions and other events relevant to their information.
- j. Review and correct reports that indicate the job profiles which currently have access to their information.
- k. Select a sensitivity classification category relevant to their information and review this classification periodically for possible modification.
- l. Select a criticality category relevant to their information so that appropriate contingency planning can be performed.
- m. Define procedures to assure information is being stored and handled in accordance with all relevant laws, regulations, and applicable professional standards.

2. Information Owners must designate a back-up person to act on their behalf if they are absent or unavailable. Owners may not delegate ownership responsibilities to third-party organizations (such as outsourced firms or consultants) or to any individual who is not a full-time employee of the College.
When both the Owner and the back-up Owner are unavailable, the CIO may make Owner decisions.
3. Supervisors
   - a. Owners do not approve ordinary access control requests. Instead, a user's immediate supervisor approves a request for system access based on existing job profiles. If a profile does not exist, the manager's responsibility is to request the profile and obtain the approval of relevant Owners who will inform the ITS Department.
   - b. Similarly, when a worker leaves the College or is transferred to another department, the worker's immediate supervisor is responsible for promptly informing the ITS Department that the privileges associated with the worker's user-ID must be revoked. User-IDs are specific to individuals and must not be reassigned to or used by others. Shortly after

separation from the College a worker's supervisor is additionally responsible for reassigning the involved duties and files to other workers.

4. Information Custodians
   a. Custodians are in physical or logical possession of information and/or information systems. Like Owners, Custodians are specifically designated for different types of information. In most cases the ITS Department will act as the Custodian. If a Custodian is not clear based on existing information systems operational arrangements, the CIO will designate a Custodian. Custodians follow the instructions of Owners, operate systems on behalf of Owners, but also serve users authorized by Owners.
   b. In cases in which the information being stored is paper-based and not electronic, the Information Custodian's responsibilities will logically fall to the department gathering the information. For such systems the ITS Department can offer guidance and suggestions but will not provide the custodian services.
   c. Custodians must define the technical options, such as information classification, and then allow Owners to select the appropriate options for their information. Custodians also define information systems architectures and provide technical consulting assistance to Owners so that information systems can be built and run to best meet business objectives. If requested, Custodians additionally provide reports to Owners about information system operations, information security problems, and the like. Custodians are furthermore responsible for safeguarding the information in their possession, including implementing access control systems to prevent inappropriate disclosure, as well as developing, documenting, and testing information contingency plans.
5. Information Users

   Users are not specifically designated but are broadly defined as any worker with access to internal information or internal information systems. Users are required to abide by all security requirements defined by Owners, implemented by Custodians, and established by ITS. Users are required to familiarize themselves with, and act in accordance with all College information security requirements. Users are also required to participate in information security training and awareness efforts. Users must request access from their immediate supervisor and report all suspicious activity and security problems. (See the section below entitled Reporting Problems.)
6. Information Security
   a. The ITS Department and, more particularly, the CIO or Information Security Manager (ISM), are the central points of contact for all information security matters at the College. Acting as internal technical consultants, this Department's responsibility is to create workable information security compromises that take into consideration the needs of various Users, Custodians, and Owners. Reflecting these compromises, this Department defines information security standards, procedures, policies, and other requirements applicable to the entire organization. ITS is responsible for handling all access to control

management activities, monitoring the security of College information systems, and providing information security training and awareness programs to College employees. The department is additionally responsible for periodically providing reports to management on the current state of information security.

b. The ITS Department must also provide technical consulting assistance related to emergency response procedures and disaster recovery. The ITS Department is responsible for organizing a formal Information Security Advisory Team (ISAT) to promptly respond to virus infections, hacker break-ins, system outages, and other security incidents. This ISAT shall consist of the following ITS staff members:

   i. Chief Information Officer (CIO);
   ii. Information Security Manager (ISM);
   iii. Director, Computer Services and Telecommunications;
   iv. Director, Management Information Systems Support;
   v. Director, Networking and Systems Support;
   vi. Director, Technology Support.

c. The ISAT is tasked with providing guidance, direction, and authority for information security planning, policies and procedures, threat mitigation, training, and incident response.

d. The ITS Department must provide the direction and technical expertise to ensure that the College information is properly protected. This includes consideration of the confidentiality, integrity, and availability of information and the systems that contain it. The ITS Department will act as liaison on information security matters between all College departments and must be the focal point for all information security activities throughout the organization. The department must perform risk assessments, prepare action plans, evaluate vendor products, assist with control implementations, investigate information security breaches, and perform other activities that are necessary to assure a secure information-handling environment.

e. The ITS Department has the authority to create and periodically modify technical standards and standard operating procedures (SOP) which support this information security policy document. These SOPs, when approved by appropriate the College administrators, have the same scope and authority as if they were included in this policy document. When a standard or procedure is intended to become an extension of this policy document, the standard or procedure will include these words: "This standard or procedure has been created by the authority described in the Pensacola State College Information Security Policy and must be complied with as though it were part of the Policy document."

D. Information Classification

1. College information is classified based upon its level of sensitivity, value, and the impact to the College should the information be altered, destroyed or disclosed

without authorization. All College faculty, staff and other entities who are affiliated with the College shall be responsible for protecting College information according to its classification.

2. Public Data

   Information is classified as Public when its disclosure, alteration, or destruction results in little or no risk to the College or its affiliates. Examples of Public data include course information, the College Catalog, press releases and other information intended for the general public. Basic security measures are necessary in order to ensure the integrity of Public data. Access to Public data is essentially unrestricted.

3. Sensitive Data

   Information is classified as operationally sensitive when its disclosure, alteration or destruction results in moderate risk to the College or its affiliates. Sensitive data includes information related to the regular business and administrative functions of the College not meant for the general public. Reasonable security controls must be implemented to ensure the integrity and availability of Sensitive information. Access to Sensitive data is restricted to faculty, staff, and affiliates of the College.

4. Confidential Data

   Information is classified as Confidential when its disclosure, alteration or destruction results in a high level of risk to the College or its affiliates. Information that is not specifically designated as Public or Sensitive shall be considered to be confidential. Examples of Confidential data include student records, certain personnel records, College donor information, etc. Security controls for confidential information are frequently required by law to ensure its confidentiality, integrity, and availability. Access to confidential data is restricted to faculty, staff, and affiliates of the College with approved access and signed confidentiality agreements.

E. ITS Department Responsibilities, Policies, and Procedures

1. The ITS Department must establish and maintain sufficient preventive and detective security measures to ensure that the College information is free from significant risk of undetected alteration.
2. Information Security Policy Document
   a. This Department is responsible for developing and maintaining this information security policy document.
   b. The policies and procedures in this document will be reviewed and evaluated on a regular basis.
   c. Management fully supports the development and enforcement of these information security policies and procedures.
3. Information Security Organization
   a. The CIO and Information Security Manager (ISM) will oversee and ensure compliance with policies and procedures within the entire organization.
   b. The ITS Department will occasionally test users to ensure that consistent compliance exists across the organization.

c. Third-party connection access requirements to the computer network are documented in contracts and agreements.

d. Information security requirements are fully specified in outsourcing contracts.

e. Any contract or agreement allowing access to the College's information assets must include the following language:

[Company Name] shall maintain in full force for the duration of this Agreement a Cyber Liability insurance policy with an aggregate minimum limit of $1,000,000.00, covering any loss by, or damages or injury to, the College for any unauthorized access, unauthorized use, virus transmission, denial of service, personal injury, advertising injury, failure to protect privacy, disclosure of protected information or intellectual property infringement arising from any act, omission or negligence on the part of [Company Name] or its officers, agents or employees in designing, developing, installing, hosting, operating, or maintaining the computer service, system, programming, support, software or Internet website that is the subject of this Agreement (collectively referred to hereafter as the "Work"). If the foregoing policy is written on a claims-made basis, [Company Name] warrants that any retroactive effective date for coverage under the policy shall precede the effective date of this Agreement; and that continuous coverage will be maintained for a period of four (4) years following the date that the Works is completed.

4. Asset Classification

a. A formal IT Asset Information Management System (IMS) is in place that tracks the movement of IT assets.

b. The IMS is detailed and covers the movement of hardware and software assets.

c. Information assets are classified appropriately.

d. Confidential information transmitted over insecure networks, such as the Internet, must be adequately encrypted.

5. Personnel Security

a. Positions with specific information security job responsibilities have been documented in job descriptions.

b. Applicants for positions that involve access to sensitive facilities receive a pre-employment background check and a thorough screening, including past criminal and credit checks.

c. Information security awareness is recognized as a significant risk management issue. New employees receive information security policies as part of their orientation, and as part of ongoing communication activities.

d. Information security breaches are logged and analyzed for patterns. A formal disciplinary process is in place for dealing with breaches.

6. Physical Security

a. There are ciphers or magnetic card locks on computer room doors, and codes/authorized cards are limited to authorized persons.

b. Computer rooms have installed fire suppression equipment. Maintenance is performed at least every six months.

c. All computer systems (including PBX and communication rooms housed separately from the main data center) are tied into the Uninterrupted Power Supply (UPS) system. The computer room is equipped with a backup generator that is tested on a periodic basis.

d. Computers and magnetic media are checked for sensitive information prior to disposal.

7. Computer and Network Security

a. All computer systems and applications have written documentation describing operational procedures. Documents are formally maintained and required for all applications. Vendor manuals exist for all purchased packages. It is the responsibility of the Management Information Systems (MIS) Department to ensure the accuracy of the system documentation, procedures, and manuals.

b. There is a documented change control process. Changes to most networks, operating systems or application systems (both legacy and client-server or web) are documented and approved.

c. A formal capacity and resource planning effort has been established. New applications and machines are periodically reviewed by a group of individuals from across the organization. There is regular tracking of utilization and bottlenecks and some planning for future requirements.

d. There is a documented virus policy and protection program. Virus detection software is installed on all file servers and personal computers. Virus signature updates are routinely posted. There are adequate preventative controls. Users have been instructed to check files, mail attachments and downloads of uncertain origin.

e. Appropriate, frequent backups of business systems are stored in remote, fireproof safes or hot sites. Thorough testing has proved that the processes work. Retention periods for all essential business information has been determined.

f. Operations staff maintain a work log (system start and finish times, system errors and corrective actions, confirmation of input and output). Systems logs are monitored for most systems, with critical systems given more attention.

g. A network monitoring package and a commercial firewall and/or proxy server is in place. Firewall configurations are based upon industry best practices or certified. Operating system and router settings are benchmarked on industry best practices, and kept up-to-date with patches/upgrades recommended by product vendors and other professional sources.

h. There are basic logs/lists of tapes to help trace or locate a backup tape. Media are physically secured and housed in locked rooms or cabinets.

i. Basic controls secure e-commerce activities, including general email policies, secure FTP, and web servers implemented with basic security controls. SSL encryption is in place where needed and security is guaranteed by a certificate authority.

8. System Access Control
    a. A formal system access request procedure exists. A written request/form must be completed in order to create, modify, or delete any user account. Approvals are required and usually obtained.
    b. All users are made aware of their responsibilities with respect to the selection and use of strong passwords. Passwords expire at least every 90 days. Stricter controls exist on sensitive systems or accounts. There are no shared or guest accounts.
    c. Only authorized users are able to gain access to networked systems from a remote location. There are adequate controls over the authentication of remote users using dial-back modems or at least two (2) levels of passwords. Network access is generally controlled through the use of firewalls at major access points.
    d. Unique user IDs (with names that do not indicated privileged users) and strong passwords are the rule in order to gain access at the operating system level on all systems. Logon processes are secure, and logon credentials are difficult to guess. There are no anonymous or shared accounts.
    e. All powerful system utilities are fully protected against unauthorized access. Most have been removed from the live systems and special access procedures are in place.
    f. Event logs are kept automatically for most systems showing unauthorized access attempts, privileged operations, major system events, and system failures. Logs are reviewed in response to problems. Logs from sensitive systems are taken offline and stored securely.
    g. Reasonable controls are provided to most laptops, such as access control software using one-time passwords or similar strong authentication, regular backups, virus prevention, and cable locks. Telecommuters must use approved security methods when accessing the corporate network, or access will not be granted.
9. System Development and Maintenance
    a. Policy requires that encryption be used for critical or sensitive systems, and for some mail or files transmitted over public networks. Adequate encryption and public key management techniques are used. Users are responsible for managing their own encryption products and public keys.
    b. Formal procedures have been established regarding the steps needed to update or upgrade operating systems and user applications. System administrators, testing personnel, and network management are involved in testing before any migration from test to production systems is permitted.
    c. There is a strict policy against modification of vendor-supplied packages, and they are only modified directly in-house as a last resort. The written consent of the vendor is always obtained, with potential impacts to future releases documented and understood.

10. Business Continuity Planning
    a. Management supports the development and maintenance of Business Continuity Plans (BCP) across the organization. It is the responsibility of the ITS Department for coordinating BCPs. BCPs are updated regularly, and are occasionally tested to determine effectiveness.
    b. BCPs address most of the following: outline of responsibilities, conditions for activating the plan, emergency procedures, contact lists, fall back and resumption, and a program for awareness, education, and testing.
    c. A comprehensive IT disaster recovery plan is an integral part of all applicable BCPs.
    d. All BCPs are tested at least annually, and testing is scheduled for specific departmental BCPs in response to modifications to affected application systems or computer systems. All connections with critical third-parties are tested.
11. Compliance
    a. There are strong management controls in place to monitor and ensure compliance. There is evidence of a comprehensive, control framework, designed in conjunction with legal advisors, and management responsibilities are clearly allocated. There are regular independent risk-based compliance reviews and management reporting. There is almost no risk of managers being prosecuted for non-compliance. Users who break laws or contractual obligations are considered for discipline and possible prosecution.
    b. All managers and staff are educated about their responsibilities through orientation, policy, and other awareness methods (e.g., newsletters, posters, flyers, etc.). Staff must demonstrate active compliance with the controls, and must re-affirm their understanding of policies by annual acknowledgement and review.
    c. Standards for secure configuration settings are comprehensive and regularly updated. A comprehensive program of regular reviews of compliance with secure configuration standards is scheduled, aided by automated technical security auditing tools.
    d. Information security audits are conducted based on risk analysis results.
    e. Audit, scan, or verification processes are documented; controls over access to audit materials have been established. Logging facilities are in places that have been designed for most application systems. Access to system audit tools and system audit facilities is strictly controlled.
12. Reporting Problems
    a. It is the responsibility of all faculty and staff to report suspicious activity and security issues regarding College information. All employees are expected to assist with maintaining the confidentiality, integrity, and availability of the data.
    b. Employees of the College should report information security related issues by contacting the CIO or ISM directly, or via the Help Desk at (484-1702).

Responsible Official	Chief Information Officer		
President's Signature: E Meadows		Date:	02/21/2017