COLLEGE of CENTRAL FLORIDA

ADMINISTRATIVE PROCEDURE

Title: Information Security	
Page 1 of 7	**Implementing Procedure For Policy # 3.24**
Date Approved/Revised: 2/23/05	**Division: Administration and Finance/Information Technology**

Purpose

This set of procedures has been created by the authority described in the College of Central Florida Information Security Policy. This document details the procedures necessary to implement the policies set forth in the College's Information Security Policy. As stated in Policies 3.21 and 3.24, these procedures provide details about standards for the protection and use of information and technology resources. The College will protect confidentiality and privacy in accordance with applicable laws and our personnel policies. Each person subject to the Policy will sign a statement annually affirming that they have read, that they understand, and that they intend to comply with the provisions of the Policy and the Procedures stated herein. The signing of this statement is a requirement for obtaining access to the organization's data systems and networks.

Critical Business Function

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

Supporting Business Objectives

This procedure has been implemented to ensure that the College of Central Florida is able to support our educational mission. This document is also intended to support our reputation for integrity. Because the prevention of security problems is considerably less expensive than correction and recovery, this document may also reduce costs over time.

Consistent Compliance

A single unauthorized exception to security measures can jeopardize other 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 minimum requirements defined in this document are appropriate for all employees at the College of Central Florida and should have a minimal impact on efficiency and costs. Indeed, there may be cost avoidance in some cases by close adherence to these procedures. 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.

College of Central Florida offers equal access and opportunity in employment, admissions and educational activities. The college will not discriminate on the basis of race, color, ethnicity, religion, sex, age, marital status, national origin, genetic information, veteran status or disability status and any other factors prohibited under applicable federal, state, and local civil rights laws and regulations in its employment practices or in the admission and treatment of students. Recognizing that sexual harassment constitutes discrimination on the basis of sex and violates this policy statement, the college will not tolerate such conduct. The Title IX Coordinator has been designated to handle inquiries regarding nondiscrimination policies and can be contacted at the Ocala Campus, 3001 S.W. College Road, at 352-291-4410 or Compliance@cf.edu.

Team Approach

Although the tools now available in the information security field are becoming more sophisticated, users still play the most important role in information security. Because information and information systems are distributed to desktop PC's, and sometimes used in remote locations via laptop, the user's role is an essential part of information security. Information is not the exclusive domain of the Information Technology Department - information security is a team effort requiring the participation of every employee who comes in contact with the College of Central Florida and its information systems.

Information Security Responsibilities and Procedures

Information Owners: Administrators in user departments are 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 Information Systems Officer will make the designation. Information Owners do not legally own the information in question; they are instead members of the College of Central Florida administrative team that makes decisions on behalf of the organization. Information Owners, or their delegates, are required to make the following decisions and perform the following activities:

a) Designate a system-of-record (original source) for information from which all management reports will be derived.
b) Select special controls needed to protect information (such as additional input validation checks or more frequent back-up procedures)
c) Define acceptable limits on the quality of their information (accuracy, timeliness, time from capture to usage, etc.)
d) Approve all new and different uses of their information
e) Approve all new or substantially enhanced application systems that use their information before these systems are moved into operational status
f) Review reports about system intrusions and other events relevant to their information
g) Review and correct reports that indicate the people who currently have access to their information
h) Define procedures to assure information is being stored and handled in accordance with all relevant laws, regulations, and applicable professional standards

Information Owners must designate a back-up person to act if they are absent or unavailable. Owners may not delegate ownership responsibilities to third party organizations (such as outsourcing firms or consultants) or to any individual who is not a full-time employee. When both the Owner and the back-up Owner are unavailable, the Information Systems Officer may make Owner decisions.

Supervisors: Owners do not approve access requests. Instead, a user's Vice President approves a request for system access and sends the request to Information Technology.

Similarly, when an employee leaves the College of Central Florida, the employee's immediate supervisor, in the case of a part-time employee, and the HR Department, in the case of a full-time employee, are responsible for promptly informing the Information Technology Department that the privileges associated with the worker's user-ID must be revoked. User-ID's are specific to individuals, and must not be reassigned to, or used by, others. Shortly after separation from the College of Central Florida, an employee's supervisor is additionally responsible for reassigning the involved duties and files to other employees.

Terminated employee e-mail is maintained for supervisor review for 90 days after which it is backed up to electronic media and deleted from on-line disk space.

Information Custodians: 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 Information Technology Department will act as the Custodian. If a Custodian is not clear based on existing information systems operational arrangements, the Information Systems Officer will designate a Custodian. Custodians follow the instructions of Owners, operate systems on behalf of Owners, but also serve users authorized by Owners.

In cases in which the information being stored is paper-based, and not electronic, the Information Custodian responsibilities will logically fall to the department gathering the information. For such systems, the Information Technology Department can offer guidance and suggestions, but will not provide the custodian services.

Custodians must define the technical security options, such information criticality categories, 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.

Information Users: Users are not specifically designated, but are broadly defined as any employee 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/or established by the Information Technology Department. Users are required to familiarize themselves with, and act in accordance with all College of Central Florida 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.

Information Security: The Network Engineer in the Information Technology Department is the central point of contact for all information security matters at the College of Central Florida. Acting as internal technical consultants, the Information Technology Department's responsibility is to create workable information security that takes 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. The Information Technology Department is responsible for handling all access to control management activities, monitoring the security of the College of Central Florida information systems, and providing information security training and awareness programs to the College of Central Florida employees. The department is additionally responsible for periodically providing management with reports about the current state of information security.

The Information Technology Department must also provide technical consulting assistance related to emergency response procedures and disaster recovery. The Information Technology Department is responsible for organizing responses to promptly respond to virus infection, hacker break-ins, system outages, and similar security problems. Guidance, direction, and authority for information security activities are centralized for the entire organization in the Information Technology Department.

The Information Technology Department provides the direction and technical expertise to ensure that the College of Central Florida's information is properly protected. This includes consideration of the confidentiality, integrity, and availability of both information and the systems that handle it. The Department will act as a liaison on information security matters between all 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.

Information Technology Department Responsibilities, Policies and Procedures

The Information Technology Department must establish and maintain sufficient preventive and detective security measures to ensure that the College of Central Florida information is free from significant risk of undetected alteration.

- **Information Security Procedure Document**
    - This Department is responsible for developing and maintaining this information security procedure document.
    - The procedures in this document will be reviewed and evaluated on a regular basis.
    - Management fully supports the development and enforcement of these information security policies and procedures.

- **Information Security Organization**
    - The Information Systems Officer is the person who will oversee and ensure compliance with policies and procedures within the organization.
    - The Information Technology Department will occasionally test users to ensure that consistent compliance exists across the organization.
    - Third Party connection access requirements to the computer network are documented in contracts and agreements.
    - Information security requirements are fully specified in outsourcing contracts.

- **Asset Classification**
    - A formal information technology asset management system (ITAMS) is in place that tracks the movement of information technology assets.
    - The ITAMS is detailed and covers the movement of hardware and software assets.
    - Sensitive information assets are classified as Confidential.

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

- **Personnel Security**
  - Positions with specific information security job responsibilities have been documented in job descriptions.
  - 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.
  - Information security awareness is recognized as a significant risk management issue. New employees receive training on information security policies and procedures as part of their orientation, and as part of ongoing communication activities.
  - Where appropriate and reasonable, information security breaches are logged and analyzed for patterns. A formal disciplinary process is in place for dealing with breaches.

- **Physical Security**
  - There are cipher or magnetic card locks on computer room doors, and codes / authorized cards are limited to authorized persons.
  - Computer rooms have installed fire suppression equipment. Maintenance is performed at least every six months.
  - All computer systems (including communication and technology equipment rooms housed separately from the main data center) are protected by Uninterrupted Power Supplies (UPS). The computer room is equipped with a backup generator that is tested on a periodic basis.
  - Computers and magnetic media are checked for sensitive information prior to disposal.

- **Computer and Network Security**
  - 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 Information Technology Department responsibility to ensure the accuracy of the system documentation, procedures, and manuals.
  - 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.
  - 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.
  - Appropriate, frequent backups of business systems are stored in remote, fireproof safes or hotsites. Thorough testing has proved that the processes work.
  - Information Technology staff maintain a log of system errors and corrective actions.
  - A network monitoring package and a commercial firewall and/or proxy server is in place. Firewall configurations are based upon industry best practices or are 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/or other professional sources.
  - There are basic logs/lists of tapes to help trace or locate a backup tape. Media is physically secured and housed in locked rooms or cabinets.
  - Basic controls secure e-commerce activities, including general e-mail policies, secure FTP, and web servers implemented with basic security controls and SSL encryption.

- **System Access Control**
  - A formal system access request procedure exists. A request / form must be submitted in order to create, modify, or delete any user account. Approvals are required.
  - All users are made aware of their responsibilities with respect to the selection of strong passwords, their use, protection and need for frequent change. There are no shared or guest accounts.
  - 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. Network access is generally controlled through the use of firewalls at major access points.
  - Unique user IDs (with names that do not indicate 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 it would be difficult to guess. There are no anonymous or shared accounts.
  - 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.
  - Sensitive systems are protected from unauthorized access through the “freezing” of the account after a 3rd successive log in attempt.
  - Reasonable controls are provided to most laptops, such as access control software using one-time passwords or similar strong authentication, regular backups, virus prevention, cable locks. Telecommuters must use approved security methods when accessing the corporate network, or access will not be granted.

- **System Development and Maintenance**
  - Procedure 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.
  - 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.

- **Business Continuity Planning**
  - Management supports the development and maintenance of Business Continuity Plans (BCP) across the organization. The Information Technology Department is designated as responsible for coordinating BCP's. BCP’s are updated regularly, and are occasionally tested to determine effectiveness.
  - BCP's 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.
  - A comprehensive IT disaster recovery plan is an integral part of all applicable BCP’s.
  - All BCP’s are tested at least annually, and testing is scheduled for specific departmental BCP’s in response to modifications to affected application systems or computer systems. All connections with critical third parties are tested.

- **Compliance**
  - There are strong management controls in place to monitor and ensure compliance. Users who break laws or contractual obligations are considered for discipline and possible prosecution.
  - 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.
  - 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.
  - Information security audits are conducted on a regular basis, based on risk analysis results. Automated audit/security scanning and assessment utilities and tools are frequently used.
  - 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.

Vice President, Administration & Finance		Date:
Approved by President		Date: