COLLEGE of CENTRAL FLORIDA	**COLLEGE of CENTRAL FLORIDA** **ADMINISTRATIVE PROCEDURE**

Title: Security Incident Response	
Page 1 of 4	**Implementing Procedure for Policy #3.24 (See also; "Administrative Procedure – Information Security")**
Date Approved: 10/30/13	**Division: Administration and Finance/Information Technology**

Purpose

A security incident within Information Technology is defined as an adverse event that impacts or has the potential to impact the confidentiality, availability, or integrity of a computer system or network. This administrative procedure defines College of Central Florida's standards, responsibilities, and guidelines regarding security incident reporting and response. The intent is to contain and to repair damage from security incidents and to prevent similar incidents.

Examples of information security incidents include, but are not limited to:

- unauthorized disclosure, whether intentional or inadvertent, of confidential information
- unauthorized use, alteration, reproduction, or destruction of confidential information
- unauthorized use of user IDs, passwords or access codes
- failure to protect user IDs and passwords (i.e. sharing codes, posting at work station, etc.)
- unauthorized access to the Data Center, equipment closets, network or to a computer or workstation
- indications of a computer virus, excessive or disruptive use, suspicious activity
- theft of or tampering with computer equipment

Security Incident Response Team

The Security Incident Response Team is composed of IT security staff and reports to the Chief Information Officer. The team membership includes:

- Data Center Manager
- Network Engineer
- PC Specialist/Network Support
- Senior Technical Support Specialist
- Systems Programmer
- Systems Analyst

The Security Response Team is responsible for the management of security incidents, as follows:

- determining vulnerabilities of IT resources

- modifying access control policies and techniques when violations, incidents, and related risk assessments indicate that such changes are appropriate
- processing IT security complaints or incidents reported by others
- advising the President's staff, Human Resources, Marketing and possibly law enforcement and Florida DOE of incidents, progress, and results, particularly for security incidents that are determine to be medium or high severity
- implementing the appropriate course of action to resolve the incident
- reviewing the incident to determine if changes are needed to remove or reduce the vulnerability in the future
- adhering to strict confidentiality of all information collected surrounding the incident and disclosing information to only those parties that have a legitimate need to know
- maintaining for a minimum of two years, all Security Incident Reports and documentation pertaining to the investigations and corrective actions taken

Security Incident Report

College employees must report all suspected security incidents to the IT Help Desk immediately. A Security Incident Report form will be processed for each reported incident and will include:

- date and time when the incident occurred or was discovered
- identity of the person who discovered the incident
- date and time when the incident was reported
- identity of the person who reported the incident
- a description of the incident and any extenuating circumstances related to the incident

The Security Incident Report form will be given to the Security Incident Response Team. The team's responsibilities for each reported incident include:

1. contain the incident as quickly as possible
2. secure evidence
3. notify the appropriate constituents
4. investigate the details of the incident and the suspected vulnerabilities
5. determine the severity of the incident, based on:
    - data classification
    - legal issues
    - magnitude of service disruption
    - threat potential
    - public interest
6. determine the need for additional actions and discipline (If the incident involves a student, notify Student Affairs. If the incident involves an employee, notify the appropriate Vice President.) IT staff will not make disciplinary decisions unless they supervise the violator.
7. complete the report form, adding pertinent information, such as:
    - the names and times when other persons were consulted
    - a description of the course of action that was established

College of Central Florida may choose to report an incident to authorities outside of the college, if after investigation, the severity of the violation or parties involved warrants notification. Outside authorities may include local law enforcement, Internet Service Providers, or any other agency with a security interest. College of Central Florida may choose to prosecute based on the nature, repetition, or severity of damage caused by the incident.

Class 3: Highest Severity

If the answer is 'yes' to any of the following questions regarding an incident, then it is a Class 3 incident.

1. Data security - Is there a reasonable expectation that critical data was acquired by an unauthorized person as a result of this incident?

    a. Are data protected by privacy rules or legislation involved? For example:
        i. Non-directory student data as defined in FERPA
        ii. Social Security Number
        iii. Bank account, credit card or other private financial information
        iv. Driver license number
    b. Is intellectual property involved?
    c. Are other data security issues involved? For example:
        i. Passwords, risk assessments, or other security-related data
        ii. Data restricted by legal contracts, memorandums of understanding, or other agreements
    d. If the data is available to unauthorized users, will it cause harm to an individual, a group or the institution?

    If it is determined that a class 3 level breach of data security has occurred, the college will notify the affected parties based on the requirements established by Florida Statute Section 817.5681.

2. Legal issues - Does this incident involve any legal violation?

    a) Threat to persons or property
    b) Theft greater than $10,000
    c) Child pornography
    d) Copyright violations

3. Magnitude of service disruption - Does this incident impact mission critical services?
4. Threat - Are hosts involved in this incident actively attacking other hosts?
5. Public interest - Is there active public interest in this incident?

Class 2: Medium Severity

If the answer is 'no' to all of the Class 3 questions above, but 'yes' to any of the following questions, then it is a Class 2 incident.

1. Data Security - Is there a reasonable expectation that sensitive data was acquired by an unauthorized person as a result of this incident? For example:

    a) Infrastructure diagrams such as building and network
    b) Strategy documents
    c) Financial information
    d) Purchasing information
    e) Business recovery plans
    f) System configurations

2. Legal issues - Does this incident involve a legal violation? For example:

    a) Theft less than $10,000
    b) Harassment

3. Magnitude of service disruption - Is it likely that this incident will impact mission critical services?
4. Threat - Is an attack likely to occur from hosts involved in this incident?
5. Public interest - Is there likely to be public interest in this incident?

Class 1: Lowest Severity

If the answer is 'no' to all of the Class 2 and Class 3 questions above, then it is a Class 1 incident.