SOUTH FLORIDA STATE COLLEGE
ADMINISTRATIVE PROCEDURES

PROCEDURE NO. 2155

TITLE: INFORMATION SYSTEMS SECURITY

BASED ON POLICY: 2.15 SAFEKEEPING, REPRODUCTION, AND DESTRUCTION OF RECORDS

OFFICE OF PRIMARY RESPONSIBILITY: VICE PRESIDENT FOR ADMINISTRATIVE SERVICES/ EXECUTIVE DIRECTOR, INSTITUTIONAL EFFECTIVENESS, PLANNING, AND TECHNOLOGY

I. Purpose:

To protect information assets from accidental or intentional but unauthorized disclosure, modification, or destruction or the inability to process that information

II. Procedure:

A. Security

1. Security objectives

a. Ensure the integrity and accuracy of the data

b. Provide for privacy of proprietary, personal, privileged, or otherwise sensitive data

c. Protect and conserve College information assets from natural and other hazards

d. Ensure the ability to survive hazards

e. Protect employees from fraudulent attempts to obtain sensitive or personally identifiable information

f. Protect employees from unnecessary temptation to default on their responsibilities

g. Protect innocent employees from suspicion in the event that another employee defaults on responsibilities

h. Protect management from charges of imprudence if any compromise of security occurs

2. Security policy

   Security must begin with the establishment of a collegewide policy by the highest levels of management in the organization. This policy will set the direction for security and give broad guidance. Guidelines and instructions on security will be covered in more detailed supporting documents.

3. Security staff

   The executive director, institutional effectiveness, planning, and technology will be designated with responsibility for directing and coordinating the implementation of the College's security policy. Responsibilities of the security manager are to:

   a. Maintain a current collegewide security policy
   b. Develop and implement a comprehensive security awareness program
   c. Publish detailed guidelines
   d. Assist department heads with implementation of the policy
   e. Coordinate security audits
   f. Recommend College employees to assist with the implementation of this procedure

4. Information asset management

   a. All information will be accounted for and properly protected by a custodian program.

   b. The fundamental principle of custodial management deals with the identification of the individual who is responsible for a given information asset

   c. The individual administrator or department head or his/her agent who has management responsibilities of the asset is designated as the custodian and is responsible for making recommendations to the security custodian with regard to:

      1) Who may use the asset
      2) The classification and level of protection given the asset
      3) Approving application controls and authorizing access to the asset
      4) Risk management, risk acceptance, and contingency planning with regard to the asset

5. Management responsibility

   All department heads and administrators must be intimately familiar with the College's policies and guidelines, and are responsible for ensuring that all employees are aware and abide by the established guidelines.

6. Employee awareness

   a. All employees must be alert to the need for security. This awareness must come from management's communication of the College's policy and guidelines to all personnel. A clear understanding and commitment on the part of all employees to abide by the policy is necessary.

   b. A collegewide security awareness program will be the most cost-effective action. It will be a part of the new employee orientation program. For existing employees, it will be instituted in a series of seminars and will be followed up with frequent reminders in College publications, on posters, and in newsletters.

   c. There will be both scheduled and impromptu audits. The program will:

      1) Emphasize the importance of security
      2) Identify security controls in terms of job and function for all employees
      3) Identify control practices to be followed
      4) Encourage participants to suggest improvements to the control practices
      5) Specify the consequences of non-compliance

   d. Security requirements and management's expectations of the employee will be included as a part of each employee's performance plan. Job appraisals and performance reviews should provide feedback to the employee in measuring up to the protection of the College's assets.

B. Hazards to information systems environment

   1. Hazards to the information system environment breaks down into two logical groupings:

      a. Natural hazards which include: fire, wind, rain, rising water, lightning, and others

      b. Manmade hazards which include: errors, omissions, mischief, vandalism, arson, riot, war, fraud, embezzlement, theft, eavesdropping, and others

2. It has been found that accidental events account for the major exposure to data loss. Intentional acts may have more serious consequences per event but occur less frequently.

C. Risk Analysis

For the purpose of risk analysis, the College will:

1. Specify a list of potential hazards (both natural and manmade)

2. Apply practical experience and management judgment to identifying the College’s vulnerabilities to these hazards

3. Assess and project the frequency of occurrence(s)

4. Quantify the resultant annualized loss exposure to the College on the basis of each type of hazard and expected frequency of occurrence

5. Prioritize the results on the basis of loss exposure

6. Identify protective measures to reduce the vulnerability to hazards or the resultant effect of hazardous events

7. Select protection on the basis of cost benefit tradeoffs

8. Implement protection on the basis of benefit to the College

9. Periodically, monitor all occurrences of hazardous events and evaluate the effectiveness of protective measures employed for reducing the College’s vulnerability to loss

D. Protective measures

Protective measures to reduce vulnerabilities and exposure to either accidental or intentional events are placed into three categories:

1. Physical security practices include:
    a. Providing a safe place to work
    b. Controlling access to sensitive resources
    c. Detecting and communicating emergencies
    d. Limiting the damage resulting from emergencies

2. Contingency planning addresses three key areas:

    a. Emergency plan: The goal of the emergency plan will be to contain the damage and preserve the mission of the College during a disaster. It addresses such issues as early detection of the incident, safety of personnel, evacuation, shelter, and containment of the incident to a minimal effect.

b. Backup plan: The goal of the backup plan is to provide a capability to carry out critical portions of the College's mission between the occurrence of an interruption and complete recovery. It addresses such issues as user responsibility, assessment of the criticality of various functional areas of the College, identification of alternate sources to run critical College applications, and testing procedures.

c. Recovery plan: The goal of the recovery plan is to provide a permanent restoration of the College's mission. It addresses such issues as the information system manager's responsibility, development of a strategy, resource identification, and testing procedures.

3. The contingency plan for each of these three areas will be documented and tested on a regular basis.

HISTORY: Last Revised: 4/27/20

Adopted: 10/29/86
Reviewed: 2/6/07
Revised: 12/4/01, 4/27/20