SOUTH FLORIDA STATE COLLEGE
ADMINISTRATIVE PROCEDURES

PROCEDURE NO. 2158

TITLE: INFORMATION SECURITY

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

OFFICE OF PRIMARY RESPONSIBILITY: PRESIDENT'S OFFICE

I. Purpose:

To continue to protect private information and data and to comply with new federal laws, South Florida State College (SFSC) has adopted this information security procedure for certain highly critical and private financial and related information. This procedure is established for the specific purpose of compliance with the Gramm-Leach Bliley Act (GLB Act). The procedure applies to customer financial information (covered data) that SFSC receives in the course of business as required by these new federal laws, as well as other confidential financial information SFSC has voluntarily chosen as a matter of policy or procedure to include within its scope. The procedure describes the activities SFSC currently undertakes, and will undertake, to maintain data protected by legal and college requirements. This information security procedure is designed to provide an outline of the safeguards that apply to this information, the practices that will be carried out and the impact on diverse areas of the college.

II. Procedure:

A. Definitions

Covered data - all information required to be protected under the Gramm-Leach-Bliley Act and to financial information that SFSC, as a matter of policy, has included within the scope of this information security procedure.

Such data shall include:

1. Information obtained from a student in the course of offering a financial product or service

2. Information provided to the college from another institution

3. Paper and electronic records that are handled by the college or its affiliates

Offering a financial product or service - includes offering student loans, receiving income tax information from a current or prospective student's parents as a part of a financial aid application, offering credit or interest

bearing loans and other miscellaneous financial services as defined in 12 CFR § 225.28. Such financial information includes:

1. Addresses

2. Phone numbers

3. Bank and credit card account numbers

4. Income and credit histories

5. Social security numbers

Service providers - all third parties who, in the ordinary course of college business, are provided access to covered data.

Service providers may include:

1. Businesses retained to transport and dispose of covered data

2. Collection agencies

3. Systems support providers

B. Security procedure components

This section of the procedure describes how the college will implement and maintain a comprehensive information security program that contains the administrative, technical, and physical safeguards that are based upon the college's size, complexity, and the nature of its activities. The five components of the procedure are as follows:

1. Designating an employee or office responsible for coordinating the program

2. Conducting risk assessments to identify reasonably foreseeable security and privacy risks

3. Ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored

4. Overseeing service providers

5. Maintaining and adjusting this information security procedure based upon the results of testing and monitoring conducted as well as changes in operations or operating systems.

C. Security procedure coordinator

The security program coordinator (coordinator) will be responsible for implementing this information security procedure. The coordinator is presently the college controller. The controller, or the controller's designee, will work closely with the IT Department, the Registrar, all Student Services Departments, Human Resources, and other necessary offices and units to implement this program. Specific duties of the coordinator shall be as follows:

1. Consult with responsible offices to identify units and areas of the college with access to covered data.

2. Conduct a survey, or utilize other reasonable measures, to confirm that all areas with covered information are included within the scope of this information security procedure.

3. Maintain a list of areas and units of the college with access to covered data.

4. Ensure that risk assessments and monitoring, as set forth in sections D and E below, are carried out for each unit or area that has covered data and that appropriate controls are in place for the identified risks.

5. May require units with substantial access to covered data to further develop and implement comprehensive security plans specific to those units and to provide copies of the plans.

6. May designate, as appropriate, responsible parties in each area or unit to carry out activities necessary to implement this information security procedure.

7. Work with responsible parties to ensure adequate training and education is developed and delivered to all employees with access to covered data.

8. Verify, in consultation with other college offices, that existing policies, standards, and guidelines that provide for the security of covered data are reviewed and adequate.

9. Make recommendations for revisions to policy, or the development of new policy, as appropriate.

10. Prepare an annual report on the status of the information security procedure and to provide that to the college president or designee.

11. Update this information security procedure, including this and related documents, from time to time.

12. Maintain a written security plan containing the elements set forth above in Section B at all times and make the plan available to the college community.

D. Risk assessment

This procedure identifies reasonably foreseeable external and internal risks to the security, confidentiality and integrity of covered data that could result in the unauthorized disclosure, misuse, alteration, destruction or otherwise compromise such information, and assess the sufficiency of any safeguards in place to control these risks. Risk assessments will include consideration of risks in each area that has access to covered information. Risk assessments shall include, but not be limited to, consideration of employee training and management; information systems, including network and software design, as well as information processing, storage, transmission and disposal; and systems for detecting, preventing, and responding to attacks, intrusions or other system failures.

The coordinator will work with all relevant areas to carry out comprehensive risk assessments. Risk assessments will include system-wide risks, as well as risks unique to each area with covered data. The coordinator will ensure that risk assessments are conducted at least annually and more frequently where required. The coordinator may identify a responsible party from the IT Department to conduct the system-wide risk assessment. The coordinator may identify a responsible party in each unit with access to covered data to conduct the risk assessment considering the factors set forth above, or employ other reasonable means to identify risks to the security, confidentiality and integrity of covered data in each area of the college with covered data.

E. Information safeguards and monitoring

This procedure shall ensure that information safeguards have been designed and implemented to control the risks identified in the risk assessment set forth above in Section D. The coordinator will ensure that reasonable safeguards and monitoring are implemented and cover each unit that has access to covered data. Such safeguards and monitoring will include the following:

1. Employee management and training

Safeguards for security will include management and training of those individuals with authorized access to covered data. The college has adopted comprehensive procedures for preserving the security of private information, included covered data. These are set for in Section E.

The coordinator will, working with other responsible offices and units, identify categories of employees or others who have access to covered data. The coordinator will ensure that appropriate training and education is provided to all employees who have access to covered

data. Such training will include education on relevant policies and procedures and other safeguards in place or developed to protect covered data. Training and education may also include newsletters, promotions or other programs to increase awareness of the importance preserving the confidentiality and security of confidential data.

Other safeguards will also be used, as appropriate, including job specific training on maintaining security and confidentiality, requiring use-specific passwords and required periodic changes to those passwords, limiting access to covered data to those with a business need for access to information, requiring signed certification of responsibilities prior to authorizing access to systems with covered data, requiring signed releases for disclosure of covered data, establishing methods for prompt reporting of loss or theft of covered data or media upon which covered data may be stored, and other measures that provide reasonable safeguards based upon the risks identified.

2. Information systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal.

Network and software systems will be reasonably designed to limit the risk of unauthorized access to covered data. This may include designing limitations to access, and maintaining appropriate screening programs to detect computer hackers and viruses and implementing security patches.

Safeguards for information processing, storage, transmission, retrieval and disposal may include: requiring electronic covered data be entered into a secure, password-protected system; using secure connections to transmit data outside the college; using secure servers; ensuring covered data is not stored on transportable media (floppy drives, zip drives, zip drives, etc); permanently erasing covered data from computers, diskettes, magnetic tapes, hard drives or other electronic media before re-selling, transferring, recycling or disposing of them; storing physical records in a secure area and limiting access to that area; providing safeguards to protect covered data and systems from physical hazards such as fire or water damage; disposing of outdated records under a document disposal policy; shredding confidential paper records before disposal; maintaining an inventory of servers or computers with covered data; and other reasonable measures to secure covered data during its life cycle in the college's possession or control.

3. Managing system failures

The college will maintain effective systems to prevent, detect and respond to attacks, intrusions and other system failures. Such systems may include maintaining and implementing current anti-virus software; checking with software vendors and others to regularly obtain and installing patches to correct software vulnerabilities; maintaining

appropriate filtering or firewall technologies; alerting those with access to covered data of threats to security; imaging documents and shredding paper copies, backing up data regularly and storing back-up information off site, as well as other reasonable measures to protect the integrity and safety of information systems.

4. Monitoring and testing

   Monitoring systems will be implemented to regularly test and monitor the effectiveness of information security safeguards. Monitoring will be conducted to reasonably ensure that safeguards are being followed, and to swiftly detect and correct breakdowns in security. The level of monitoring will be appropriate based upon the potential impact and probability of the risks identified, as well as the sensitivity of the information provided. Monitoring may include sampling, system checks, reports of access to systems, reviews of logs, audits and any other reasonable measures adequate to verify that information security program's controls, systems and procedures are working.

5. Reporting

   The coordinator will provide a report on the status of the information safeguards and monitoring implemented for covered data as described in Section D.

F. Service providers

In the course of business, the college may from time-to-time appropriately share covered date with third parties. Such activities may include collection activities, transmission of documents, destruction of documents or equipment, or other similar services. This procedure will ensure that reasonable steps have been taken to select and retain service providers that are capable of maintain appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.

The coordinator, by survey or other reasonable means, will identify service providers who are provided access to covered data. The coordinator will work with the Office of the President, and other offices as appropriate, to make certain that service provider contracts contain appropriate terms to protect the security of covered data.

G. Program maintenance

The coordinator, working with other responsible units and offices, will evaluate and may revise the procedure in light of the results of testing and monitoring described in Section F, as well as any material changes to operations or business arrangements, and any other circumstances which may reasonably have an impact on the information security procedure.

This procedure will be reviewed at least annually by the coordinator and the college president or designee.

H. Roles and responsibilities

Deans, directors, department heads and other managers

The dean, department head, director, or other manager responsible for managing employees with access to covered data will designate a responsible contact to work with the coordinator to assist in implementing this program. The designated contact will ensure that risk assessments are carried out for that unit and that monitoring based upon those risks takes place. The designated responsible contact will report the status of the information security procedure for covered data accessible in that unit to the coordinator at least annually and more frequently when appropriate.

Employees with access to covered data

Employees with access to covered data must abide by college policies and procedures governing covered data, as well as any additional practices or procedures established by their department chairs, directors and/or deans.

Office of the Vice President for Administrative Services

The vice president shall be responsible for the provisions of all information technology security policies, procedures and guidelines. The vice presidents shall designate a college member as the college's information technology security administrator.

Information technology (IT) security administrator

The IT security administrator shall perform as the college's security procedure coordinator and will be responsible for assisting the vice president for administrative services in implementing the provisions of all information security policies, procedures, and guidelines. The IT security administrator will designate individuals who have the responsibility and authority for information technology resources; establish and disseminate enforceable rules regarding access to and acceptable use of information technology resources; establish reasonable security policies and, measures to protect data and systems; monitor and manage system resource usage; investigate problems and alleged violations of college information technology policies; and refer violations to the vice president for administrative services.

HISTORY: Last Reviewed: 8/31/06

Adopted: 8/25/03
Reviewed: 8/31/06
Revised: -