Ferris State University

Information Security Guidelines

General Information

This document outlines Ferris State University's Information Security Guidelines for safeguarding customer information according to the Gramm-Leach Bliley Act, Health Insurance Portability and Accountability Act (HIPAA), The Family Educational Rights and Privacy Act (FERPA) and the Payment Card Industry Data Security Standards (PCI-DSS), etc... These Acts spell out specific requirements regarding the security and privacy of customer personal information in whatever format, electronic or hard copy. In accordance with these Acts, the University is required to take steps to ensure the security and confidentiality of customer records (e.g., employees, students or third parties) such as names, addresses, phone number, bank and credit account information, income and credit histories and Social Security Numbers.

Specific objectives of the guidelines are to:

- Ensure the security and confidentiality of customer records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against the unauthorized access to or use of such records or information that could result in substantial harm or inconvenience of any customer.

Components of the Information Security Guideline

These Acts require the University to develop, implement and maintain a comprehensive Information Security Guideline consisting of administrative, technical and physical safeguards that are appropriate based on our size, programs, nature of activities and risk profiles. Outlined below are the five components required by the Acts to ensure implementation and completion of the Information Security Guideline:

- Designate an employee or employees responsible for coordinating the Guideline;

- Conduct risk assessments to help identify any possible security and privacy threats to customer information;

- Ensure safeguards (e.g., policies, standards, procedures and guidelines) are developed or modified to minimize or control the risks identified. Test and monitor the effectiveness of these safeguards, key controls, systems and procedures on regular basis;

- Oversee service providers;

- Maintain and adjust the Information Security Guideline using test and monitoring results to include consideration for any changes to operations or systems.

1. Information Security Coordinator

The Information Security Guideline Coordinator ("Coordinator") will be responsible for implementing this guideline. The Coordinator is presently the Data Security Administrator. The Data Security Administrator will work closely with Data Owners, units or offices (e.g., Colleges, General Counsel, Human Resources, Finance, etc.) to implement and complete these guidelines.

The Coordinator will:

- Consult with the Data Owners and responsible office employee(s) to identify units and areas of the University with access to covered data. A survey or other reasonable measures can be used by the Coordinator to help identify all areas with covered data. A list (or chart) will be developed and maintained by the Coordinator: 1) describing the covered data, 2) identifying the office or unit having access to covered data and 3) name of Data Owner or responsible employee(s).

- Ensure that risk assessments, safeguards and monitoring, are carried out for areas with access to covered data and safeguards are in place for the identified risks. If necessary, the Information Security Guideline can be augmented to include more in-depth security plans in cases where the access to covered data is considerable. Copies of these plans are to be submitted to the Coordinator. Also, the Coordinator may designate a responsible employee(s) for each office or unit to ensure implementation of the Information Security Guideline.

- Work with Data Owners and responsible employees to develop adequate training and help educate all employees with access to covered data. In conjunction with other University offices, the Coordinator will verify the existence and adequacy of policies, standards and guidelines related to the security, integrity and privacy of covered data. The Coordinator will make recommendations where policy changes are needed or help develop a new policy, if appropriate.

- Prepare a report on the status of the Information Security Guidelines and provide the results to the Chief Technology Officer. To provide reasonable assurance that the Information Security Guideline is implemented and maintained, the report may consist of:

    1. Copies of any unit-specific security plans;
    2. Current risk assessments for each unit with access to covered data;
    3. A statement on the controls in place to minimize risks and the effectiveness of such controls
    4. Summaries of monitoring activities to include actions taken or to be taken to correct any security, integrity or privacy issues identified and other information, as required.

- Update this Information Security Guideline and related documents as needed.

2. Risk Assessment

The Information Security Guideline will identify any possible foreseeable external and internal risks to the security, integrity and confidentiality of covered data that could result in an unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. A risk assessment will be conducted to determine if the safeguards in place are sufficient to control identified risks for each office or unit with access to covered data. Risk assessments may include evaluation of:

- Employee management and training;
- Information systems (both electronic and hardcopy form), including information storage, transmission, retrieval, and disposal;
- Systems for detecting, preventing and responding to attacks, intrusions or other system failures, and;
- Classification of information or covered data based on its sensitivity (e.g., evaluation of the value-added security system or other stand-alone systems and applications to ensure access is restricted to those employees based on job assignment and duties, customer, general public or third party accessibility).

The Coordinator will:

- Work with Data Owners, units, and responsible employees to carry out risk assessments considering the aforementioned factors or use other reasonable measures to identify risks to the security, integrity and confidentiality of covered data in each area of the University. Risk assessments will cover system-wide risks, as well as, risks associated with each office's or unit's covered data.
- Ensure that risk assessments are conducted at least annually or more frequently where necessary.
- Identify a responsible employee from Information Services and Telecommunications to conduct the system-wide risk assessment or if feasible, an external party may be used.
- Submit copies of the complete and current risk assessments for the system-wide and unit-specific risks along with the Coordinator's report on an annual basis.

3. Information Safeguards and Monitoring

The Information Security Guideline is designed to help verify that safeguards are in place to control the risks identified as part of the risk assessment. The Coordinator will ensure that sufficient safeguards and monitoring activities are completed for the offices or units with access to covered data. Such safeguards and monitoring may include the following:

a. Employee Training

Safeguards for security will include training of those individuals with authorized access to covered data. The University has adopted policies, standards and guidelines setting forth the procedures and recommendations for preserving the security and confidentiality of customer information to include covered data. These polices, standards and guidelines are listed in Section V below.

The Coordinator, along with other Data Owners, will identify categories of employees or others who have access to covered data and ensure that training is provided. For example, training will include education on relevant policies, standards, procedures, guidelines and other media (e.g., newsletters, pamphlets, notices, etc.) outlining security, integrity and privacy applicable to covered data. Acts that the University must comply with include:

- Family Educational Rights and Privacy Act (FERPA), 1974 which restricts and protects access to student information from disclosure to unauthorized parties. Communication of student information is restricted to only those parties authorized to have access in accordance with the provisions of FERPA.

- Health Insurance Portability and Accountability Act (HIPAA), 1996 which established national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also addresses the security and privacy of health data.
- Gramm-Leach-Bliley which addresses the security of personal, financial information.
- Payment Card Industry Data Security Standards (PCI-DSS) which includes specific security standards and requirements for security management, policies, procedures, network architecture, software design, and other critical protective measures. It applies to all aspects of storing, processing and/or transmitting cardholder data.

To strengthen security over covered data, other safeguards will be employed such as:

- Job-specific training on maintaining security, integrity and confidentiality of covered data;

- User-specific passwords;

- Restricted access to covered data by individuals with a valid business need;

- Signed certification of responsibilities prior to authorizing access to systems with covered data;

- Requiring signed releases for disclosure of covered data (FERPA and HIPAA), and;

- Establishing methods for prompt reporting of unauthorized disclosure (e.g., loss or theft) of covered data to include media or equipment used for storage.

b. Information Systems

Information systems include the transmission, storage, retrieval, and disposal of data. Network and software systems applications limit the risk of unauthorized access to covered data by maintaining appropriate screening programs to detect computer hackers, viruses and implementing security patches.

Safeguards and controls for information processing, storage, transmission, retrieval and disposal of covered data may include:

- Requiring electronic entry into a secure, password-protected system;
- Using secure servers and connections to transmit data;
- Storing of covered data on transportable media (e.g., floppy drive, 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 (e.g., hardcopy form) in a secure area and limiting access via key control;
- Protecting covered data and system 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
- Implementing other reasonable measures to secure covered data when in the possession or control the University.

c. Managing System Failures

The University information systems should include safeguards to help prevent, detect and respond to attacks, intrusions and other system failures. Such information systems may include maintaining and implementing of:

- anti-virus software;
- authentication software;
- operating systems patches to correct software vulnerabilities;
- use of appropriate filtering or firewall technologies;
- alerting those with access to covered data of threats to security;
- backing up data regularly and storing back up information off site; and
- other reasonable measures to protect the integrity and safety of information systems

d. Monitoring and Testing Systems

Periodical monitoring of systems will be completed to test the effectiveness of information security and controls. Testing and monitoring of information system security and controls will be completed to ensure safeguards are being followed and to help promptly detect and correct breakdowns in security. Monitoring may include sampling, system checks, review of access reports and logs to systems, audits and any other reasonable measures needed to verify that controls and procedures are working as intended.

e. Reporting of Status

The Coordinator will provide a report on the status of the Information Security Guideline’s safeguards, testing and monitoring results of covered data.

4. Service Providers

While conducting University business, covered data may be shared with third parties. Such activities may include collection activities, transmission of documents or data, destruction of documents, development of software, use of equipment or other similar services. This Information Security Guideline will ensure that reasonable steps are taken to select and retain service providers that are capable of implementing appropriate measures to safeguard covered data and to refrain from sharing any covered data with any other third party.

Through a survey or other means, the Coordinator will work with other offices or units (e.g., Purchasing Office and General Counsel) to identify service providers with access to covered data and make certain that service provider contracts contain appropriate language to protect the security of covered data.

5. Program Maintenance

The Coordinator, Data Owners, along with other responsible offices and units, will evaluate and revise the Information Security Guideline annually based on testing and monitoring results to include any significant changes to operations or business arrangements.

Roles and Responsibilities

Ferris Administrators: Administrators are responsible for managing employees with access to covered data; they will designate a responsible employee to work with the Coordinator to assist in the implementation of these guidelines. The responsible employee(s) will ensure that risk assessments are carried out for that office or unit and monitoring of identified risk are completed. The responsible employee(s) will report the status of the Information Security Guideline for accessible covered data of the unit to the Coordinator at least annually or more frequently, if necessary.

Employees with Access to Covered Data: Employees with access to covered data should comply with University policies and procedures related to covered data, as well as, any additional standards, guidelines and practices established by their office or unit manager. **University Archivist**: This individual is responsible for disposing and archiving personal and financial information in a manner that is acceptable under the various acts.

Data Security Administrator (Coordinator): This individual is responsible for implementing the requirements of this Information Security Guideline.

Data Owners: Because these individuals are the owners of the data within their modules, they will be responsible for helping to insure compliance and security.

Chief Technology Officer: The University's Chief Technology Officer will designate individuals who have the responsibility and authority for information technology resources and systems; 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 University information technology policies, procedures, standards and guidelines to the appropriate University offices (e.g., Office of General Counsel, Public Safety, etc.) for resolution or disciplinary action.

Related Policies, Standards and Guidelines

Policies and Procedures

Updates to the following may be found at http://www.ferris.edu/HTMLS/administration/buspolletter

- Computer Software Policy
- Computer Virus Policy
- Electronic Mail Policy and Electronic Mail Guidelines
- Ferris Website Policy
- Freedom of Information Act (FIOA) Policy and Procedures
- Network Operating Systems Policy
- Proper Use of Information Resources, Information Technology and Networks Policy
- Residential Network Support – Computer Systems and Information Misuse
- Residential Network Support – Computer Lab Rules
- Information Technology Policies – Community Standards on Computer Abuse: Student Responsibilities ***(source: FSU Student Handbook)***
- Information Technology Policies – Appropriate and Responsible Use
- Information Technology Policies - Ethical and Legal Use of Software: A Guide for Students, Faculty, and Staff at Ferris State University
- MichNet Acceptable Use Policy
- Credit Card Processing and Security Policy

Standards

- Network Standards http://www.ferris.edu/techsupport
- Netware Administration and Security Standard http://www.ferris.edu/techsupport

Contact Information

- Data security concerns can be emailed to DataSecurity@ferris.edu or via phone at (231)591-2132.
- The Chief Technology Officer can be reached at urbanicj@ferris.edu