GRAMBLING
STATE UNIVERSITY
GRAMBLING, LOUISIANA

Policy #

INFORMATION SECURITY PROGRAM POLICY

Effective Date: February 21, 2018
Responsible Office: Information Technology Center
Division: Finance

I. PURPOSE/OBJECTIVE

The federal Gramm-Leach-Bliley Act (GLB Act) requires financial institutions to take steps to ensure the security and confidentiality of customer records and information. Colleges and universities, defined as financial institutions for purposes of the GLB Act, are not subject to the privacy provisions of the GLB Act provided they are in compliance with the Family Educational Rights and Privacy Act (FERPA). However, higher education institutions are subject to the provisions of the GLB Act related to the administrative, technical, and physical safeguarding of customer records and information as specified in the Federal Trade Commission's (FTC) Standards for Safeguarding Customer Information ruling, known as the Safeguards Rule, which requires all covered financial institutions to have in place a comprehensive, written information security program. This policy has been formulated to facilitate Grambling State University's implementation of the requirements of the GLB Act.

II. STATEMENT OF POLICIES

Grambling State University complies with the requirements of the Gramm-Leach-Bliley Act. The requirements of the Act are as follows:

1. Each covered financial institution is to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information at issue. Safeguards are to be reasonably designed to achieve the following objectives:
    a. To insure the security and confidentiality of customer information;
    b. To protect against any anticipated threats or hazards to the security or integrity of such information; and
    c. To protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

2. In developing, implementing, and maintaining the information security program, each covered institution is to:
    a. Designate an employee or employees to coordinate the program.
    b. Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information; and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment is to include consideration of risks in each relevant area of an institution's operations, including:

        i. Employee training and management;
        ii. Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
        iii. Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

    c. Design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.
    d. Oversee service providers by:

        i. Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
        ii. Requiring service providers by contract to implement and maintain such safeguards.

    e. Evaluate and adjust the information security program in light of the results of the testing and monitoring required by paragraph 2.c.; any material changes to operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on the information security program.

A. INFORMATION SECURITY PROGRAM

As required by the GLB Act, Grambling State University has developed, implemented, and maintained a comprehensive information security program as outlined below:

Risk Assessment Committee: The Risk Assessment Committee (Committee) is responsible for implementing and maintaining the Information Security Program.

a. The Committee is comprised of the AVP for Information Technology, the Director of Network Services, and the Security Administrator. In implementing this Program, the Committee works closely with relevant academic and administrative organizational units across campus.
b. The responsibilities of the Committee include, but are not limited to:
    i. Consulting with responsible offices to identify organizational units with access to covered data, ensure all such units are included within the scope of this Program, and maintain a current listing of these units.
    ii. Working with all relevant organizational units to identify potential and actual risks to the security and privacy of covered data; evaluate the effectiveness of current safeguards for controlling these risks; design and implement additional required safeguards; and regularly monitor and test the Program;
    iii. Working with appropriate organizational units to ensure adequate training and education programs are developed and provided to all employees with access to covered data; ensure existing policies and procedures that provide for the security of covered data are reviewed and adequate; and make recommendations for revisions to policy, or the development of new policy, as appropriate.
    iv. Consulting with responsible organizational units to identify service providers with access to covered data; ensure all such service providers are included within the scope of this Program; and maintain a current listing of these service providers.
    v. Reviewing the Information Security Program, including this and related documents, annually, and making adjustments as needed.
    vi. Maintaining a current, written Program, that is available to the University community.
c. In carrying out these responsibilities, the Committee may require organizational units with substantial access to covered data to review security reports specific to those units, to provide the Committee with security changes,

and to designate responsible individuals to carry out activities necessary to implement this Information Security Program.

2. **Risk Identification and Assessment**: Under the guidance of the Committee, organizational units with access to covered data identify and assess internal and external risks to the security, confidentiality, and integrity of that data.

    a. At a minimum, this process considers the risks to covered data, and the safeguards currently in place to manage those risks, in each relevant area of University operations including:
        i. Employee management and training;
        ii. Information systems, including network and software design, as well as information processing, storage, transmission, and disposal for both paper and electronic records; and
        iii. Security management, including the prevention, detection, and response to attacks, intrusions, or other systems failures.

    b. The Committee establishes procedures for identifying and assessing risks in each relevant area of the University's operations outlined above.

    c. Each affected organizational unit, in consultation with the Committee, performs the risk identification and assessment and identifies a responsible individual to serve as that unit's contact person with the Committee.

    d. Risk assessments include system-wide risks, as well as risks unique to each area with covered data. The Committee ensures risk assessments are conducted annually and more frequently where required.

3. **Information Safeguards and Monitoring**: The Committee verifies that organizational units with access to covered data design, implement, and regularly monitor safeguards to control identified risks to the security, confidentiality, and integrity of that data. Such safeguards and monitoring include:

    a. ***Employee Management and Training***: Safeguards for information security include the management and training of those individuals with authorized access to covered data.
        i. In consultation with other responsible organizational units, the Committee identifies categories of employees and others with access to covered data.
        ii. The Committee works with the Information Technology Training Center and other responsible organizational units to develop appropriate training and education programs for all current and new affected employees.

1. These programs may be developed as part of the University's existing employee training program and/or as a component of the new employee orientation program.
2. Training and education may also include brochures, web sites, and other means of increasing awareness of the importance of preserving the confidentiality and security of covered data.

b. ***Information Systems***: Information systems include network and software design, as well as information processing, storage, transmission, and disposal. Safeguards are designed and implemented in accordance with the nature and scope of the unit’s activities and the sensitivity of the covered data to which it has access.

i. Each affected organizational unit implements and maintains in writing administrative, technical, and physical safeguards to control the risks to information systems, as identified through the unit's risk assessment process.

ii. The Committee works on the design and implementation of safeguards. Safeguards may include:

1. Creating and implementing access limitations;
2. Using secure, password-protected systems and encrypted transmissions within and outside the University for covered data;
3. Regularly installing patches to correct software vulnerabilities;
4. Prohibiting the storage of covered data on transportable media;
5. Permanently removing covered data from computers, hard drives, or other electronic media prior to disposal;
6. Storing physical records in a secure area with limited access;
7. Protecting covered data and systems from physical hazards such as fire or water damage;
8. Disposing outdated records under the records retention policy; and

Other reasonable measures to secure covered data during the course of its life cycle while in the University's possession or control.

c. ***Security Management***: The Committee develops and implements effective procedures for preventing, detecting, and responding to actual and attempted attacks, intrusions, and other systems failures.
   i. The Committee implements the appropriate security management procedures.
   ii. Such procedures may include implementing and maintaining current anti-virus software; maintaining appropriate filtering or firewall technologies; regularly obtaining and installing patches to correct software vulnerabilities; imaging documents and shredding paper records; regularly backing up data; implementing incident response plans; and other reasonable measures.
   iii. The Committee may elect to delegate to an appropriate individual in Information Technology the responsibility for monitoring and disseminating information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the University.

d. ***Monitoring and Testing***: In consultation with other responsible organizational units, the Committee develops and implements procedures to test and monitor the effectiveness of information security safeguards.
   i. Monitoring levels are to be appropriate to the probability and potential impact of the risks identified, as well as the sensitivity of the information involved.
   ii. Monitoring may include sampling, systems checks, systems access reports, and any other reasonable measures adequate to verify that Information Security Program safeguards, controls, and procedures are effective.

4. **Service Providers and Contract Assurances**: The Committee, by survey or other reasonable means, identifies service providers with access to covered data and the organizational units that provide this access. Working with these units, the Committee ensures reasonable steps are taken:
   a. To select and retain service providers capable of maintaining appropriate safeguards for covered data;
   b. To require service providers, by contract, to implement and maintain such safeguards; and
   c. To require service providers, by contract, to grant the University assurances of GLB Act compliance.

5. **Periodic Review and Adjustment of Program**: The Committee, working with other responsible organizational units, annually evaluates and revises the Information Security Program to:
   a. Ensure compliance with the GLB Act, the FTC Safeguards Rule, and any related federal and state laws and regulations;
   b. Ensure effectiveness of the Program in light of testing and monitoring results and any material changes to operational or business arrangements, including but not limited to changes in technology, sensitivity of covered data, and the nature of internal and external threats to information security.

B. COMMUNICATION

This information is communicated through the Information Technology Center and the Information Technology Center's Web Page.