JACKSON STATE UNIVERSITY'S
Information Security Plan
(In compliance with the Gramm Leach Bliley Act of 1999)

I. Information Security Plan Purpose

This document summarizes the Jackson State University's (the "University's") comprehensive written information security program (the "Program") mandated by the Federal Trade Commission's Safeguards Rule and the Gramm – Leach – Bliley Act ("GLBA"). In particular, this document an Information Security Program Plan describes the procedures for evaluating and addressing the electronic and physical methods of accessing, collecting, storing, using, transmitting and protecting customer information and elements pursuant to which the University intends to provide the proper safeguards to protect data, information, and resources: These safeguards include:

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

II. Definitions

A. ***Authorized user*** - any employee, contractor, agent, customer, or other person that is authorized to access any of JSU's information systems or data.
B. ***Customer information*** -any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of JSU or JSUs' affiliates.
C. ***Encryption*** -the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.
D. ***Financial institution***-any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C § 1843(k). An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.
E. ***Information security program*** -the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.
F. ***Information system*** -a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

G. ***Multi-factor authentication*** - authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; (2) Possession factors, such as a token; or (3) Inherence factors, such as biometric characteristics.

H. ***Nonpublic personal information*** - (i) Personally identifiable financial information; and (ii) Any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available.

I. ***Penetration testing*** - a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

J. ***Security event*** - an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

K. ***Service provider*** -means any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution that is subject to this part.

L. **Covered data-** means all information required to be protected under the Gramm-Leach-Bliley Act ("GLB Act"). "Covered data" also refers to financial information that the University, as a matter of policy, has included within the scope of this Information Security Program. Covered data includes information obtained from a student in the course of offering a financial product or service, or such information provided to the University from another institution. "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. Examples of student financial information relating to such products or services are addresses, phone numbers, bank and credit card account numbers, income and credit histories and social security numbers. "Covered data" consists of both paper and electronic records that are handled by the University or its affiliates.

III. Security Program Components

The GLB Act requires the University develop, implement and maintain a comprehensive information security program containing the administrative, technical and physical safeguards that are appropriate to the University's activities, size, and complexity. This Information Security Program has five components: (1) designating an employee or office responsible for coordinating the information security program; (2) conducting risk assessments to identify foreseeable security and privacy risks; (3) ensuring that safeguards are enforced and applied to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored; (4) overseeing service providers, and (5) maintaining and adjusting this Information Security Program based upon the results of testing and monitoring conducted as well as changes in operations or operating systems.

IV. Security Program Coordinator

A. Designation of Representatives: The University's Chief Information Security Officer (CISO) and Cybersecurity Officer is designated as the Program Officer(s) who shall be responsible for coordinating and overseeing the Program along with the University's Chief Information Officer and Chief Technology Officer. The Program Officer(s) may designate other representatives of the University to oversee and coordinate particular elements of the Program within relevant University offices and departments. Any questions regarding the implementation of the Program or the interpretation of this document should be directed to the Program Officer or his or her designees. Additional duties of the Program Officer(s) include:

- Consult with responsible department and offices to identify units and areas of the University with access to covered data
- Coordinate with responsible parties to ensure adequate training and education is developed and delivered for all employees with access to covered data
- Collaborate with the University's Department of Information Technology to assess procedures for monitoring potential information security threats associated with the University's network and software systems and for updating such systems
- Verify that existing policies, standards and guidelines that provide for the Security of covered data are reviewed and adequate
- Make recommendations for revisions to policy, or the development of new policy, as appropriate

B. Scope of Program: The Program applies to any record containing nonpublic financial information about a student or other third party who has a relationship with the University, whether in paper, electronic or other form, that is handled or maintained by or on behalf of the University or its affiliates. For these purposes, the term nonpublic financial information shall mean any information:

- A student or other third party provides in order to obtain a financial service from the University
- About a student or other third party resulting from any transaction with the University involving a financial service
- Otherwise obtained about a student or other third party in connection with providing a financial service to that person

The Coordinator(s) will consult with responsible offices to identify units and areas of the University with access to covered data that handle non-public, covered data as outline in the program scope. As part of this Information Security Program, the Coordinator(s) have identified units and areas of the University with access to covered data. These areas include but are not limited to:

- Admissions
- Bursars Office
- Financial Aid
- Career Services Center
- Registrar's Office
- Residence Life (Housing)
- Student Employment Center(Payroll)
- Student Health Center

The University recognizes that this list of identified units and area may change in accordance with the addition or disbanding of units, departments and areas that handle covered data. Therefore, additional Identification strategies will include surveys, or other reasonable measures, to confirm that all areas with covered information are included within the scope of this Information Security Program.

V. Risk Assessment

A. Risk Identification and Assessment. The University intends, as part of the Program, to undertake a risk assessment to identify and assess external and internal risks to the security, confidentiality, and integrity of nonpublic financial information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information. The following is a list of threats to customer financial information that will be mitigated through the implementation of this program:

- Unauthorized access to data through software applications
- Unauthorized use of another user's account and password
- Unauthorized viewing of printed or computer displayed financial data
- Improper storage of printed financial data
- Unprotected documentation usable by intruders to access data
- Improper destruction of paper documents and electronic data

In implementing the Program, the Program Officer(s) will establish procedures for identifying and assessing such risks in each relevant area of the University's operations. Risk assessments will 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.

VI. Information Safeguards and Monitoring

The Information Security Program will verify that information safeguards as required by the GLBA, and FERPA Acts are designed and applied to control the risks identified in the risk assessments set forth above in Section V. The Program Officer(s) and relevant department, units and areas 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:

A. Employee Management and Training

Safeguards for security will include management and training of those individuals with authorized access to covered data. The Information Security Program Coordinator(s) will, work with the responsible departments, offices and units to identify categories of employees, students and others who have access to covered data. Each department head, manager, director, supervisor and the Information Security Program Coordinator will ensure that the appropriate awareness training and education is provided to all employees who have access to covered data. Such training will include education on relevant policies and procedures as outlined by Jackson State University's Division of Information Technology and the GLBA and FERPA safeguards put in place to protect covered data.

Existing, New, and Student Employee Training:

- Training for **new JSU Employees** will include an explanation of the purpose of GLBA and FERPA and how to avoid violating the required safeguards. They will also be informed about where, how and to whom to report potential risks, data breaches and cyber incidents. Each employee will sign into CANVAS to complete GLBA and FERPA Training along with submitting electronic acknowledgement statements that verify that the employee has 1) Reviewed the training materials for each ACT 2) that he/she understands the content presented in the trainings and 3) that he/she acknowledges that they have taken the training and are aware of their responsibilities under GLBA and FERPA. Acknowledgement statements must be submitted in the training modules before the training are considered complete.
- **Existing employees** will receive the same training as new employees and be reminded each year of their responsibilities under the GLBA and FERPA Acts by their supervisor and the program officer.
- **Students** who work in department that handles covered data and must use this information to perform his/her job duties will undergo the same training as the University's employees by their supervisor and will be reminded of their obligations after they stop working for the department. An electronic acknowledgement statement will be required before the trainings are accepted as a complete.

B. Information Systems

Information systems include network and software design, as well as information processing, storage, transmission, retrieval, and disposal. The Program Officer(s) will coordinate with the Chief Information Office and the Chief Technology Officer and additional relevant departments to assess the risks to nonpublic financial information associated with the University's information systems, including network and software design, information processing, and the storage, transmission and disposal of nonpublic financial information. This evaluation will include assessing the University's current policies and procedures relating to Acceptable Use of the University's network and network security, document retention and destruction (Refer to Acceptable Use Policy 50000.003). The Program Officer(s) will also coordinate with the University's Division of Information Technology to assess procedures for monitoring potential information security threats associated with software systems and for updating such systems, by implementing security patches or other software fixes designed to deal with known security flaws.

C. Managing System Failures

The Program Officer(s) will coordinate with the University's Division of Information Technology and other relevant units to evaluate procedures for and methods of detecting, preventing and responding to attacks or other system failures and existing network access and security policies and procedures, as well as procedures for coordinating responses to network attacks and developing incident response teams and policies. In this regard, the Program Officer(s) may collaborate with a member of the cyber security incident response team representative of the Division of Information Technology to conduct monitoring and participating in the dissemination of information related to the reporting of known security attacks and other threats to the integrity of networks utilized by the University.

Designing and Implementing Safeguards- The risk assessment and analysis described above shall apply to all methods of handling or disposing of nonpublic financial information, whether in electronic, paper or other form. The Program Officer(s) will, on a regular basis, implement safeguards to control the risks identified through such assessments and to regularly test or otherwise monitor the effectiveness of such safeguards. Such testing and monitoring may be accomplished through existing network monitoring and problem escalation procedures. Safeguards for information processing, storage, transmission, retrieval and disposal may include:

Electronic Data Security and Safeguards:

- Requiring electronic covered data to be entered or accessed from a secure, password-protected system with ***Multi-Factor/Dual Factor Authentication*** is enabled for an additional layer of security;
- Using secure VPN connections to transmit data outside the University; using secure servers;
- Ensuring covered data is not stored on transportable media (floppy drives, zip drives, etc);
- Properly erasing and disposing of covered data from computers, diskettes, magnetic tapes, hard drives, or other electronic media disposal
- Encrypting covered data when sending emails to internal or external requestors

Physical Security and Safeguards

The University has addressed the physical security of covered data, information, and resources by limiting access to only those employees who have a business reason to know such information. For example, personal customer information, accounts, balances, and transactional information are available only to University employees with an appropriate business need for such information.

- Storing physical records in a secure area and limiting access to only authorized employees
- 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
- Covered data on paper documents is required to be kept in file cabinets, rooms, or areas that can be locked each day

D. Monitoring and Testing

Monitoring of the University's systems, safeguards and policies 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 system checks, reports of access to systems, reviews of logs, audits, and other reasonable measures adequate to verify that Information Security Program's controls, systems and procedures are working.

E. Reporting

The Information Security Program Coordinator will provide a report on the status of the information safeguards and monitoring implemented for covered data as described in Section VI. C of this document.

VII. Service Providers

This Information Security Program will ensure that reasonable steps are taken to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue and requiring service providers by contract to implement and maintain such safeguards.

The Chief Information Security Officer, and Cyber Security Officer, Chief Information Officer and Chief Technology Officer shall coordinate with those responsible for the third party service procurement activities and other affected departments to raise awareness of, and to institute methods for, selecting and retaining only those service providers that are capable of maintaining appropriate safeguards for nonpublic financial information of students and other third parties to which they will have access. In addition, the Program Officer(s) will work with the University's General Counsel Division or other designated University officials to develop and incorporate standard, contractual protections applicable to third party service providers, which will require such providers to implement and maintain appropriate safeguards. The Coordinator, by survey or other reasonable means, will identify service providers who are provided access to covered data.

VIII. Program Maintenance

The Program Officer(s)is responsible for evaluating and adjusting the Program based on the risk identification and assessment activities undertaken pursuant to the Program, as well as any material changes to the University's operations or other circumstances that may have a material impact on the Program.

IX. Roles and Responsibilities

University Deans, Directors, Department Heads, Supervisors and other Managers.

The University's Deans, Directors, Department Heads, Supervisors and other Managers in the relevant identified units are responsible for managing employees with access to "covered data" under the Information Security Program. Each of these employees by default will serve as the responsible contact to ensure safeguards are being applied. However, they may designate an alternate responsible contact to work with the Coordinator to assist in implementing this program from there unit, department, or office in the event that they are not available to serve as the responsible contact. 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 Program for covered data accessible in that unit to the Coordinator at least annually, and more frequently where appropriate.

Employees with Access to Covered Data. Employees with access to covered data must adhere to the University's policies and procedures governing covered data, as well as any additional practices or procedures established by their unit heads or directors. Additional roles and responsibilities include reporting cyber incidents, participating in work place data assessment risk surveys, enrolling in Information Security Program Trainings created by the Information Security Program Officer and complete each training with a status of satisfactory and ensuring that ***Multi-Factor/Dual Factor Authentication*** is used to access covered data in their area/department.

Security Program Coordinator. The designated Security Program Coordinator is responsible for implementing the provisions of this Information Security Program Plan. Additional duties include those as outlined in IV of this document.

Chief Information Officer and Chief Technology Officer. The University's Chief Information Officer and Chief Technology Officer will designate an Information Security officer to implement the University's Information Security Program Plan. They will also coordinate with the Program Officer to ensure that enforceable rules regarding access to and acceptable use of information technology resources and reasonable security policies and measures to protect data and systems are established and followed. The University's Chief Information Officer and Chief Technology Officer will also monitor the application of required safeguards and the reports on the status of the application of these safeguards; collaborate with the University's Program Officer to investigate problems and alleged violations of University information technology policies; and refer violations to appropriate University offices such as the University's Division of the General Counsel and the or other reporting entities for resolution or disciplinary action.

X. Policies, Standards and Guidelines

The University has adopted comprehensive policies, standards, and guidelines relating to information security. They are incorporated by reference into this Information Security Plan, and include:

Policies: Acceptable Use Policy 50000.003

XI. References

[1] https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-acty Rule?
[2] https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer-information