Policy 2010
Gramm-Leach Bliley Act (GLBA) Information Security Policy

Date of Current Revision: January 2024

Responsible Officers: Associate Vice President for Information Technology and Associate Vice President for Finance

1. PURPOSE

The Federal Trade Commission's Safeguards Rule, which implements the security provisions of the Gramm-Leach-Bliley Act (GLBA)/Program, went into effect on May 23, 2003. The Safeguards Rule requires financial institutions, which includes colleges and universities that are significantly engaged in providing financial services, to protect the security, confidentiality, and integrity of customer financial records, including non-public personally identifiable financial information. To ensure this protection, the GLBA Safeguards Rule mandates that all covered financial institutions establish appropriate administrative, technical, and physical safeguards (16 CFR § 314.1(a)). Therefore, any JMU Academic Unit, office or department that collects, stores or processes Covered Data must implement data protection standards to ensure compliance. This is in addition to any other University policies and procedures that may be required pursuant to federal and state laws and regulations, including the Family Educational Rights and Privacy Act (FERPA).

2. AUTHORITY

The Board of Visitors has been authorized by the Commonwealth of Virginia to govern James Madison University. See Code of Virginia § 23.1-1600; § 23.1-1301. The Board has delegated the authority to manage the university to the president.

STATE OR FEDERAL STATUTE AND/OR REGULATION
The GLBA Safeguards Rule mandates that all covered financial institutions establish appropriate administrative, technical, and physical safeguards (16 CFR § 314).

The Family Educational Rights and Privacy Act of 1974 ("FERPA," 20 USC 1232g et. seq.) is the federal law that addresses access to and confidentiality of student education records.

3. DEFINITIONS

Academic Unit
An academic department, school or the functional equivalent, as determined by the Provost. For the purposes of this policy, it refers collectively to academic institutes, centers, departments, and schools within the Division of Academic Affairs.

Covered Data
Non-public personal financial information about a Customer and any list, description, or other grouping of Customers (and publicly available information pertaining to them) that is derived using any non-public personal financial information. Examples of Covered Data include bank and credit card account numbers, income and credit histories, tax returns and social security numbers and lists of public information such as names, addresses and telephone numbers derived in whole or in part from personally identifiable financial information (e.g., names of

students with outstanding loans). Covered Data is subject to the protections of the GLBA, even if the Customer ultimately is not awarded any financial aid or provided with a credit extension. Covered Data includes such information in any form, including paper and electronic records.

Customer
Any individual (student, parent, faculty, staff, or other third party with whom the University interacts) who receives a Financial Service from the University for personal, family or household reasons that results in a continuing relationship with the University.

Financial Service
Includes offering or servicing student and employee loans, receiving income tax information from a student or a student's parent, guardian, or other person responsible for the student account when offering a financial aid package, and engaging in debt collection activities.

Related Entities
The following types of entities and their subsidiaries, if legally separate from the University and unless otherwise indicated: auxiliary enterprise corporations, college associations, student services corporations, childcare centers, etc.

Service Provider
Any person or entity that receives, maintains, processes, or otherwise is permitted access to Covered Data information through its direct provision of services to the University.

4. APPLICABILITY

This policy applies to any individual or department that has access to Covered Data including but not limited to the following (GLBA Relevant Departments):

- Office of Financial Aid & Scholarships
- University Business Office
- Office of the Registrar
- School of Professional and Continuing Education
- Information Technology

This policy also applies to any Related Entity that provides a Financial Service or assists the University or a College with the administration of a Financial Service as follows:

- Related Entities that maintain or distribute Covered Data relating to a Financial Service on or through a University server or other technology under university control, or which assist the University or an academic unit with the administration of a Financial Service shall be deemed to be part of their supported academic unit, solely for purposes of compliance with this policy.

- Related Entities that are subject to GLBA but maintain and/or distribute Covered Data relating to a Financial Service independent of any University-controlled technology and do not assist the University or an academic unit with the administration of a Financial Service, shall adopt their own policy(ies) consistent with the requirements of GLBA and this policy, including without limitation regarding information system security, the training of employees, and safeguarding of information.

5. POLICY

It is the policy of the university to comply with the GLBA Safeguards Rule and establish appropriate administrative, technical, and physical safeguards for Covered Data. Any JMU Academic Unit, office or department that collects, stores or processes Covered Data must implement data protection standards in order to ensure compliance. This is in addition to any other University policies and procedures that may be required pursuant to federal and state laws and regulations, including the Family Educational Rights and Privacy Act (FERPA).

6. PROCEDURES

6.1 Designation of the GLBA Program Coordinator and Qualified Individual

The Director of IT Policy and Compliance shall serve as the GLBA Program Coordinator, who will administer JMU's GLBA Security Program and also serve as the primary University resource and liaison with the administrative and academic units for addressing issues related to the GLBA Safeguards Rule and disseminating relevant information and updates. The GLBA Program Coordinator shall designate a GLBA Committee representing units and areas with access to Covered Data across the campus to oversee implementation of JMU's campus-wide GLBA policy (i.e., IT, Audit, Registrar's Office, Financial Services, and Financial Aid).

The University's Information Security Officer (ISO) shall serve as the Qualified Individual responsible for the implementation and supervision of the university's Information Security and Incident Response Plans.

6.2 Identification of Risks and Risk Assessment

JMU recognizes that there are both internal and external risks associated with the protection of Covered Data. The GLBA program coordinator will conduct a periodic written risk assessment that examines the reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of Covered Data that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguard in place to control these risks. JMU's system owners and data custodians will actively seek to identify and address all potential security risks associated with Covered Data and communicate them to the GLBA program coordinator.

Audit and Management Services shall incorporate identification of GLBA related security risks and controls into its Annual IT Risk Assessment/Internal Control Review process. The risk assessments may include system-wide risks as well as risks unique to each area with covered data.

6.3 Design and Implementation of a Safeguarding Program

- Safeguarding Data
  Policy 1205 – Data Stewardship Policy - establishes a framework of uniform data management practices for ensuring the availability and protection of university data. The policy applies to all university data collected, stored, or maintained by administrative, academic or other units, employees or agents of the university regardless of its source or where it resides. Institutional policy as well as state and federal law prohibit individuals from using university data for purposes other than approved university business.

Policy 2112 – Student Privacy - is specific to privacy of student records and student information and responsibilities for compliance with the Family Educational Rights and Privacy Act of 1974 (FERPA).

At all times, Covered Data shall be maintained in a manner consistent with university policies and procedures, as detailed in JMU's Data Stewardship and Information Security Framework. In particular, Covered Data will be protected by encryption when transmitted over external networks and at rest, or secured by effective alternative compensating controls approved in writing by the Qualified Individual. Any individual accessing any information system with Covered Data should use multi-factor authentication unless the Qualified Individual has approved in writing the use of reasonable equivalent or more security access controls.

Access to Covered Data shall be limited to those employees who have a business reason to have such information. Whether this information is stored in hard copy form or electronically, employees must exercise appropriate care for its safekeeping by following the guidelines outlined in the Gramm-Leach-Bliley Act (GLBA) Information Security Standard.

- Periodic Control Assessment
  The GLBA program coordinator is responsible for periodically assessing the controls designed to mitigate the risks identified in the risk assessment as noted in 6.2.

- Periodic Inventory
  The GLBA program coordinator will identify the data, personnel, devices, system, and facilities that enable JMU to achieve business purposes associated with Covered Data.

6.4 Testing and monitoring effectiveness of safeguards

The GLBA Program Coordinator shall ensure that the safeguards, key controls, system and procedures are regularly tested and monitored. This shall include continuous monitoring or periodic penetration testing and vulnerability assessments.

6.5 Ensuring personnel have adequate knowledge and training

The GLBA Program Coordinator will work with administrative and academic units to arrange for training of the various groups impacted by the GLBA Safeguards Rule throughout the University, as needed, on an ongoing basis. Such training will include education on relevant policies and procedures and other safeguards in place or developed to protect covered data. Job-specific training on maintaining security and confidentiality will be included as required or appropriate.

Students will undergo the same training as the staff when they are employed in areas that deal with Covered Data, such as the University Business Office, Office of Financial Aid and Scholarships, Office of the Registrar, and Information Technology.

6.6 Oversight of Service Providers and Contracts

The GLBA Safeguards Rule requires that the University take reasonable steps to select and retain Service Providers who will maintain safeguards to protect Covered Data. Appropriate steps shall be taken to ensure that all contracts for service providers with access to Covered Data comply with GLBA.

6.7 Evaluation of the information security program

The University's Information Security Plan must be evaluated and adjusted as a result of testing and monitoring, any material changes to the environment, or other circumstances.

6.8 Maintenance of a written incident response plan

The GLBA Program Coordinator in coordination with the Information Security Officer shall ensure that the written incident response plan is updated regularly. The University takes every precaution to secure and protect university systems and data. Immediate steps should be taken to correct any security breach or exposure of sensitive data. Anyone who has reason to suspect a deliberate or significant breach of established security policy or procedure should promptly report it to the appropriate Dean, Director, or Department Head. Report any violation of security or appropriate use to abuse@jmu.edu or it-security@jmu.edu to the university's information security officer. Report suspected possible fraudulent transactions involving university information technology resources to Audit and Management Services (see Policy 1603 – Fraud, Waste and Abuse Reporting).

6.9 Reporting

The Qualified Individual shall report at least annually to the Board of Visitors in writing regarding the overall status of the program and any other material matters related to the information security program.

7. RESPONSIBILITIES

The GLBA Program Coordinator will administer the GLBA security program and designate a GLBA Committee representing units and areas with access to Covered Data across the campus, to oversee implementation of this policy.

The University's Information Security Officer (ISO) shall serve as the Qualified Individual responsible for the implementation and supervision of the University's Information Security and Incident Response Plans.

Information Technology is responsible for the security of computing assets.

All departments, offices and employees that generate, receive, or maintain public records under the terms of this policy are also responsible for compliance with Policy 1109 – Records Management.

8. SANCTIONS

Sanctions will be commensurate with the severity and/or frequency of the offense and may include termination of employment.

9. EXCLUSIONS

None.

10. INTERPRETATION

The authority to interpret this policy rests with the president and is generally delegated to the associate vice president for information technology and associate vice president for finance.

Previous version: n/a

Approved by the president: January 2024