Gramm-Leach-Bliley Act (GLBA) Information Security Standard

September 2023

Purpose:

The Gramm-Leach-Bliley Act (GLBA) requires financial institutions, including educational organizations, that provide financial services or products to protect the security, confidentiality, and integrity of customer financial records ("Covered Data"). The Standards for Safeguarding Customer Information ("Safeguards Rule") establishes appropriate administrative, technical, and physical safeguards that must be implemented by financial institutions and is enforced by the Federal Trade Commission (FTC). This standard summarizes James Madison University's operating requirements as mandated by the GLBA and the Safeguards Rule and in accordance with University Policy 2010 - Gramm-Leach-Bliley Act (GLBA) Information Security Policy and is subject to periodic review and adjustment.

Definitions:

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 when offering a financial aid package, and engaging in debt collection activities.

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

Standard:

1. Coordination and Responsibility

The Director of IT Policy and Compliance serves as the GLBA Program Coordinator and is responsible for the development, implementation, and oversight of the University's compliance with the policies and procedures required by the GLBA Safeguards Rule. The GLBA Program Coordinator designates a GLBA Committee representing units and areas with access to Covered Data. Represented units and areas include the Office of Financial Aid and Scholarships, University Business Office, School of Professional and Continuing Education, Office of the Registrar, Audit and Management Services, and Information Technology. Committee members are responsible for the implementation of activities required under the GLBA for their respective units or areas. This includes ensuring required training is completed by all personnel who handle or are involved in the management of Covered Data.

The University's Information Security Officer (ISO) serves as the Qualified Individual responsible for the implementation and supervision of the University's Information Security and Incident Response Plans. The Qualified Individual also acts as a member of the GLBA Committee.

2. Scope

The University has determined units and activities that are in scope for GLBA. Identified departments include the Office of Financial Aid and Scholarships, University Business Office, School of Professional and Continuing Education, Office of the Registrar, and Information Technology. Not all activities performed by these units are in scope for the GLBA; only the activities and data associated with Covered Data are in scope and must comply with this standard.

Colleges and universities that are deemed compliant with the privacy provisions and regulations of the Family Education Rights and Privacy Act (FERPA) are also considered to be compliant with the privacy provisions and regulations of the GLBA for those student records which are subject to FERPA. See University Policy 2112 – Student Privacy.

Questions regarding interpretations and applicability of the GLBA should be directed to the GLBA Program Coordinator.

3. Risk Assessment and Safeguards

The GLBA Program Coordinator and Qualified Individual works with the GLBA Committee to identify and assess potential risks to the security, confidentiality, and integrity of Covered Data. Departments are required to assess the safeguards they have in place to protect not only Covered Data, but also all university data in accordance with University Policy 1205 - Data Stewardship. In addition, departments are required to complete a System Management Plan for systems and services that fall under the GLBA. System Management Plans are provided to Information Technology annually for review by the GLBA Program Coordinator and Qualified Individual.

Specific safeguarding practices that departments should implement in their respective areas include:

- **Access to Covered Data:** Access to Covered Data is limited to those employees with a legitimate business need that requires access to carry out their assigned job duties.
- **Clean Desk Standard:** Identified units and areas should implement a clean desk standard for the handling and management of Covered Data where possible. The standard should include, at a minimum, the following:

  - Employees must lock their computers when leaving their workstations unattended.
  - Employees must ensure that Covered Data is removed from their desk/work area and kept secure in a locked drawer or cabinet at the end of each day and when they are expected to be away from their desk/work area for an extended period of time.
  - File cabinets containing Covered Data must be kept closed and locked when not in use or left unattended.
  - Shred bins containing Covered Data should be kept secure. Personal shred bins located at workstations should be emptied at the end of each day.
  - Printouts containing Covered Data should be immediately removed from printers/copiers/fax machines.
  - Fax machines should be configured so the hard drive does not store Covered Data.
- **Data Encryption:** Covered Data should be encrypted in transit and at rest. If it is not feasible to use encryption, Covered Data must be secured by using effective alternative controls approved in writing by the Qualified Individual.
- **Data Inventory:** Departments should provide to the GLBA Program Coordinator, upon request, a written inventory of Covered Data, noting where it is collected, stored, and/or transmitted. An accurate list of all systems, devices, platforms, and personnel that process Covered Data should be maintained by the department.
- **Multi-Factor Authentication:** Two-factor authentication must be used, at a minimum, for anyone accessing Covered Data. The Qualified Individual may approve in writing the use of another equivalent form of secure access controls.
- **Physical Security:** Rooms and file cabinets where Covered Data is stored should be locked with access restricted to employees that require access to carry out their assigned job duties. Documents with Covered Data should not be left unattended at printers or copiers. Fax machines should not be in public spaces (even inside an office suite), but housed in a room that can be locked during non-business hours.
- **Storage and Retention:** Covered Data may be stored electronically and in paper form in accordance with the Guidelines for Data Storage and Collaboration. Data retention requirements should be formally documented by the unit or area and based upon either a legal requirement or a legitimate business need. Processes should be developed and implemented to regularly review all stored Covered Data to ensure the retention period is not exceeded. Covered Data should be securely destroyed when no longer needed in accordance with the Virginia Public Records Act and University Policy 1109 – Records Management.
- **Continued Assessment:** Department heads and university personnel who handle or are involved in the management of Covered Data must continually assess the vulnerabilities of their electronic as well as paper-based systems. Information Technology and Audit and Management Services are available to assist in assessing the efficacy of existing safeguards and to propose improvements if needed.

4. Employee Training and Education

All university personnel are required to complete security awareness training when hired and every ninety (90) days thereafter. In addition, all university personnel who handle or are involved in the management of Covered Data must receive training specific to the GLBA and the safeguarding of Covered Data when hired and annually thereafter. Current employees that do not complete the training by the required deadline will have their access removed and must complete the training before access is restored.

5. Oversight of Service Providers and Contracts

The University uses several third-party service providers to handle some aspects of its data processing environment. Reasonable steps should be taken to select and retain service providers who maintain appropriate safeguards for Covered Data. All third-party service providers that process Covered Data on behalf of the University must have policies and procedures in place to ensure the security and confidentiality of the Covered Data. The documented responsibilities and compliance status of the University's service providers must be reviewed annually by Information Technology and the respective department.

Information Technology works with Procurement Services to develop and incorporate standard contractual provisions that require service providers to implement and maintain appropriate safeguards to ensure Covered Data is kept confidential and only used for the purposes set forth in the contract.

6. Information Security and Incident Response Plans

Information Technology maintains a written Information Security Plan to ensure the security, confidentiality, and integrity of University Data, which includes Covered Data. In addition, a written Incident Response Plan is also maintained and outlines procedures for responding to actual or attempted unauthorized access to University Data. The Qualified Individual oversees both plans, which are reviewed annually and updated as necessary.

7. Reporting

The Qualified Individual must report in writing to the University's Board of Visitors annually. The report must include an overall assessment of the University's compliance with its information security program. In addition, it must cover specific topics related to the program, such as risk assessment, risk management and control decisions, service provider arrangements, test results, security events and how management responded, and recommendations for changes to the information security program.

8. References

The following policies, standards, and guidelines supplement this standard to help to create a comprehensive information security program to ensure compliance with the GLBA and are hereby incorporated by reference.

- University Policy 2010 - Gramm-Leach-Bliley Act (GLBA) Information Security Policy
- University Policy 2112 – Student Privacy
- University Policy 1201 – Information Technology Resource Management
- University Policy 1204 – Information Security
- University Policy 1205 – Data Stewardship
- University Policy 1206 – Contingency Management for Technology-based Information Systems
- University Policy 1207 – Appropriate Use of Information Technology Resources
- University Policy 1109 – Records Management
- Data Stewardship Standard
- Guidelines for Data Storage and Collaboration