Applies to: *Faculty (including part-time and visiting faculty), staff and students (including graduate/undergraduate student workers and graduate assistants) employed by the University This policy continues to apply to individuals on sabbatical, other leaves or while visiting other institutions*

1. Policy:

Issued: June 2023
Last Revised: September 2023
Last Reviewed: June 2026
Owner: Chief Information Officer

2. Policy Purpose:

The purpose of this policy is to ensure the University's compliance with the **Gramm-Leach-Bliley Act (GLBA)** and the FTC Safeguards Rule, and to protect the security, confidentiality, and integrity of **customer information**, including student financial aid data and other sensitive personally identifiable information (PII).

3. Scope and Application:

This policy applies to all data users including employees, contractors, and third party service providers who access, process, store or transmit University data containing customer information or PII.

4. Definitions:

Definitions	
Customer Information	Any record containing nonpublic personal information about an individual, whether in paper, electronic, or other form, handled by or on behalf of the University, including information related to student financial aid (Title IV).
Personal Identifiable Information (PII)	II is defined as information: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., ..
Data Users	Data Users can view, copy or download institutional data as part of their assigned duties or in fulfillment of their role within the Rivier community. All Data Users have an obligation to understand the security responsibilities associated with their level of data access.
Data Stewards/ Managers	University officials who have planning and policy-level responsibilities for data in their functional areas are

	considered Data Managers. The Data Managers, as a group, are responsible for recommending policies, establishing procedures and guidelines for University--wide data administration activities, and training of Data Users on the proper handling of data. Data Managers, as individuals, have operational-level responsibility for information management activities related to the capture, maintenance, and dissemination of data. Data managers are responsible for developing and applying standards for the management of institutional data, and for ensuring that Data Users are appropriately informed of security obligations associated with their data access. For historical reasons – because data and the responsibility for data have traditionally been organized along functional or subject-area boundaries – the Data Managers are established according to this same subject-area organizing principle. The Data Group – Data Governance Committee (a group of data managers) meets on a regular basis.
Qualified Individual	The designated individual responsible for overseeing the University's Information Security Program, as required under GLBA.

5. Policy Details:

5.1 Information Security Policy

The University maintains a **Written Information Security Program (WISP)** designed to protect customer information. The program is risk-based and includes administrative, technical, and physical safeguards that are regularly reviewed and updated.

5.2 Governance and Oversight

The **Chief Information Officer (CIO)** is designated as the **Qualified Individual** and is responsible for:

- Overseeing the Information Security Program
- Ensuring compliance with GLBA requirements
- Coordinating security efforts across departments
- Reporting **at least annually** to senior leadership on:
    - Risk assessment results
    - Security incidents and response
    - Effectiveness of safeguards

- Recommendations for improvement

5.3 Risk Assessment

The University conducts **documented, periodic risk assessments** that:

- Identify internal and external threats to customer information
- Evaluate the likelihood and potential impact of risks
- Assess the adequacy of existing safeguards
- Inform security control decisions

Risk assessments are updated regularly and in response to significant changes in systems, processes, or threats.

5.4 Safeguards and Security Controls

The University implements safeguards appropriate to its risk profile, including:

Access Controls

- Role-based access to systems containing customer information
- Periodic review of user access rights

Authentication

- **Multi-factor authentication (MFA)** for systems containing sensitive data

Encryption

- Encryption of customer information **in transit and at rest**, where appropriate

Monitoring and Detection

- Continuous system monitoring and logging
- Use of endpoint detection and response tools (e.g., CrowdStrike)

Testing and Vulnerability Management

- Regular **vulnerability scanning and/or penetration testing**
- Timely remediation of identified risks

Secure Data Handling

- Secure storage, transmission, and disposal of customer information
- Data minimization practices to limit unnecessary collection and retention

5.5 Vendor and Service Provider Oversight

The University manages third-party risk by:

- Conducting **risk-based due diligence** prior to engagement
- Requiring contracts that include GLBA and data protection provisions
- Monitoring vendor compliance throughout the relationship

5.6 Training and Awareness

All workforce members receive **security awareness training**. Individuals with access to sensitive customer information receive **role-based training** appropriate to their responsibilities.

5.7 Incident Response

The University maintains a **written Incident Response Plan** that defines:

- Roles and responsibilities
- Detection, containment, and recovery procedures
- Communication and escalation protocols
- Post-incident review and corrective actions

5.8 Breach Notification and Regulatory Reporting

In the event of a security incident involving customer information, the University will:

- Notify affected individuals and applicable authorities as required by law
- **Report incidents affecting 500 or more individuals to the Federal Trade Commission (FTC)** in accordance with GLBA Safeguards Rule requirements

---

5.9 Recordkeeping

The University maintains records of its GLBA compliance efforts, including:

- Risk assessments
- Security policies and procedures
- Training records
- Incident response documentation
- Security testing and audit results

5.10 Enforcement

Any individual who violates this policy may be subject to disciplinary action, up to and including termination of employment, contract termination, or other appropriate measures.

Conclusion:

This GLBA policy is designed to protect the privacy of PII collected by the University and ensure compliance with applicable laws and regulations. The University is committed to maintaining the highest standards of PII protection and will regularly review and update this policy as necessary.

6. Procedures:

Procedures

7. Forms:

Forms

8. Responsibilities:

Position or Office	Responsibilities
CIO, Data Privacy Officer (Qualified Individual)	Implementing and maintaining policy
Data Stewarts	Implementing and maintaining policy

9. Related Information:

Related Policies

Data Governance Policy
Privacy Policy
Information Security Policy

10. Contacts:

Division/ Department	Position or Office	Contact Information
Information Technology	CIO	603-897-8630 / itsupport@rivier.edu