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 2025
Last Revised:
Last Reviewed:

2. Policy Purpose:

This Policy is established to implement, maintain and continually improve the Rivier University Information Security Program.

3. Scope and Application:

Information is a resource of great value to Rivier as are information systems, resources and processes that facilitate creation, collection, use, sharing, or storage of information over the course of business operations. It is therefore important to adequately preserve the confidentiality, integrity and availability of these important resources that the business relies upon to achieve strategic and operational objectives.

Information Security is the ongoing process of identifying, evaluating, and treating risks to the confidentiality, integrity and availability of information, information systems, and other business information processing resources and activities (collectively known as “Information Assets”). Rivier senior management is committed to implementing and continually improving Information Security controls, policies and practices that:

- Provide clear responsibilities for Information Security across the University.
- Implement safeguards to manage risk factors to help mitigate, transfer or avoid risks that may adversely impact the confidentiality, integrity, and availability of Information Assets
- Comply with applicable law, regulatory and industry requirements, and contractual obligations; and
- Provide assurance to Rivier stakeholders that Information Security risks are responsibly managed.

The above Rivier senior management objectives for Information Security will be primarily achieved through implementation of this Policy.

4. Definitions/Principles:

All components of the Information Security Program and requirements of this Policy focus on addressing risks to Information Assets. Risks to Information Assets shall be evaluated and managed according to the following fundamental security criteria, or principles:

Principles	
Confidentiality	Information Assets may have varying levels of sensitivity and therefore need to be protected from unauthorized access or exposure. By adhering to the principle of Confidentiality, Rivier makes Information Assets accessible to only those individuals or processes with a legitimate need and who are authorized to access them.
Integrity	Information Assets are relied upon to deliver value to customers or make business decisions. By adhering to the principle of Integrity, Rivier develops and maintains Information Assets to meet business objectives using methods that provide for accuracy and completeness.
Availability	Information Assets are expected to be accessible when needed to support business objectives. Adhering to the principle of Availability maintains access to Information Assets in a reliable and prompt fashion.

5. Policy Details:

Information Security Risk Management Framework

Rivier shall define and implement a framework for the identification and management of Information Security risks across the University. The Framework shall consist of the following components:

- A risk assessment process that is applied to information assets in order to identify, evaluate, treat, and report Information Security risks to applicable Risk Owners and Senior Management;
- Policies and implementation standards that outline mandatory Information Security control categories, objectives, and requirements that must be achieved across the University;
- An awareness program to make Rivier employees and relevant external parties aware of Information Security policies, standards and expected practices as well as the implications of non-compliance;
- A management process to oversee the performance of and evaluate the effectiveness of the Information Security Program across Rivier at regular intervals.

6. Policy Objectives

6.1. Information Security Policy

The objectives categorized and summarized below shall be established and relevant processes, practices and controls shall be implemented and monitored to manage Information Security risks across Rivier.

This Information Security Policy defines Senior Management's objectives and support for Information Security. This Policy shall:

- Be approved by management, published and communicated to employees and Third-Parties, as applicable; and
- Be reviewed at least annually, or at more frequent intervals if significant changes to the scope of the Information Security Program or business have occurred to evaluate the Policy's suitability, adequacy and effectiveness.

6.2. Personnel Security

Controls associated with Personnel Security shall be implemented to confirm that Rivier employees and Third-Parties understand and fulfill their Information Security responsibilities. Personnel Security includes the following control objectives:

- Screening of employees and Third-Parties;
- Communication to, and agreement by, employees and Third-Parties on their Information Security responsibilities prior to employment or prior to providing services to Rivier, including requirements for confidentiality and non-disclosure of Information;
- Information Security awareness, education or training of employees and relevant Third-Parties;
- Management responsibilities to confirm that employees and Third-Parties understand and perform their duties in accordance with Information Security policy;
- A disciplinary process to sanction employees or Third-Parties for failure to comply with Information Security policy; and
- A process for employee, contractor, and Third-Party off-boarding to manage revocation of access to, and recovery of, Information Assets.

6.3. Information Asset Management

Information Asset Management controls shall be implemented to identify, classify and assign responsibilities for protecting Information Assets, as practicable. Information Asset Management includes the following objectives:

- Identifying and maintaining an inventory of Information Assets and the Risk Owners responsible for their protection; excluding BYO devices;(We do allow end-users to access data on BYO devices). Talk through with IT team and senior team.
- Classifying Information Assets in a manner consistent with their value or business criticality; and - Note we assume everything has PII.
- Defined acceptable use, management, transfer, storage and disposal practices associated with Information Assets in accordance with an information classification scheme.
- IOT inventory as it pertains to PII. (Security cameras, door access controls, point of sales devices, etc.)

6.4. Access Control

The objective of Access Control is to restrict access to Information Assets or access to Information Systems. Only employees and Third-Parties with a legitimate business need and authorized by management shall have access to Information Assets or Information Systems. Access Control shall be achieved through implementation of the following:

- Processes for managing employee and Third-Party access to Information or Information Systems that include access provisioning, review of access rights at regular intervals, and modification or termination of access rights;
- Controls and mechanisms to authenticate employee and Third-Party access to Information Assets or Information Systems; and
- Controls to monitor and prevent unauthorized access to Information and Information Systems.

6.5. Physical & Environmental Security

Physical and Environmental Security controls shall be implemented to prevent unauthorized physical access, damage, loss, theft, or disruption to tangible Information Assets, encompassing Rivier office locations or facilities. Physical and Environmental Security objectives shall be achieved through implementation of the following:

- Maintaining secure perimeters and entry controls to protect and authorize physical access to Rivier office locations and facilities;
- Protecting supporting utilities and computer equipment from environmental threats, power failures, or other disruption, based on applicable risk factors;
- Protecting computer equipment and other tangible Information Assets from theft or unauthorized removal; and
- Processes to dispose of computer equipment or other tangible Information Assets to securely remove Information prior to re-use, or destroyed prior to final disposition.

6.6. Operations Security

Operations Security controls shall be implemented to protect and provide for the confidentiality, integrity and availability of Information and Information Systems. Operations Security controls shall include:

- Maintaining adequate documentation related to the design and operational performance of Information Systems;
- Maintaining a formal change management process to control planned and unplanned changes to Information Systems;
- Physical and/or logical separation of Information System development, test and production environments, or applicable controls to safeguard the use of Information in development, test and production environments;
- Security controls to detect threats, safeguard computing services, protect Information, or control access or changes to Information Systems;

- Protecting against Information loss by backing up Information and Information Systems and testing backups at regular intervals to allow Rivier to recover Information and Information Systems in timeframes sufficient to meet business requirements;
- Identifying and preventing against exploitation of technical vulnerabilities;
- Protecting against malware threats by employing solutions or processes to detect and recover from malware-based attacks; and
- Monitoring Information Systems to record and regularly review security events to identify unintended or unauthorized activity.
- Ensuring that information security is addressed in all project management efforts, regardless of the type of the project.

6.7. Communications Security

Communications Security controls shall be implemented to provide for the security of electronic communications networks and to protect Information Assets. Communications Security shall be achieved through implementation of the following controls:

- Network segmentation achieved by grouping Information Systems on segmented networks according to inherent risk factors;
- Controlling access between users and Information Systems on segmented networks;
- Deploying mechanisms to monitor for network security activity according to inherent risk factors; and
- Maintaining requirements for secure exchange and storage of electronic Information, including the use of encryption.

6.8. Information Systems Secure Development & Maintenance

Information Systems Secure Development and Maintenance controls are associated with integrating Information Security requirements across the entire Information System lifecycle. Security controls in this category should include:

- Analysis of Information Security requirements for modifications to existing or new Information Systems;
- Implementing protections for applications that transmit, process, or store Information to safeguard against unauthorized disclosure, modification, duplication, interference, replay, misrouting, or fraudulent activity;
- Applying secure software and systems engineering principles to Information System development and maintenance efforts;
- Maintaining a formal change management process to control planned and unplanned changes to software and applications;
- Securing development environments used for software engineering and systems integration activities;
- Security review and testing of Information Systems, including review and testing of software and applications; and
- Using carefully selected and protected data during software integration and quality assurance activities.

6.9. **Third-Party Security**

Controls shall be implemented to protect Information Assets that are shared with, accessible to, or stored by Third-Parties. Security controls shall include:

- A process to identify risks to Information Assets and incorporate Information Security and relevant risk treatment requirements into business agreements with Third-Parties. Specifically all prospective/new vendors must complete the EduCause Vendor Due Diligence spreadsheet;
- Processes to monitor Third-Party performance towards Information Security requirements.

6.10. **Information Security Incident Management**

Controls shall be implemented to provide for consistent and effective management of Information Security incidents. Information Security Incident Management controls shall include:

- A defined process for Information Security incident management that includes management responsibilities, requirements for reporting potential security incidents by staff, incident assessment or classification criteria, and documented response guidelines;
- Communication to and awareness by relevant individuals of their role in the Information Security incident management process;
- A requirement that appropriate contacts with relevant security authorities, special interest groups or other specialist security forums and professional associations be maintained; and
- A defined process to capture and apply knowledge gained from Information Security incidents to address and reduce the impact or likelihood of future occurrences.

6.11. Business Continuity Management

Controls shall be implemented to provide continued confidentiality, integrity and availability of Information Assets, as well as to provide for the continuity of applicable Information security controls or processes, during unplanned, adverse events. Business Continuity Management controls include:

A process to scope, document, and enact requirements for continuity of access to, availability, or recovery of, Rivier Information Assets; and

A process implemented at regular intervals to evaluate the effectiveness of business continuity activities.

6.12. Compliance & Audit

Compliance and Audit objectives are associated with the need to monitor business, legal, regulatory, or contractual requirements and confirm that Information Security controls and requirements are implemented consistently. Such security controls shall include:

- Monitoring, identification and review of applicable legal, regulatory, or contractual requirements as they relate to Information Security, including security and privacy of personal information;

- Auditing compliance with Information Security policies, standards, controls, processes or requirements at regular intervals;
- Rivier shall maintain a University-wide framework to manage its PCI-DSS compliance program and the protection of cardholder data; and
- A PCI-DSS compliance function shall be appointed by senior management assigning overall accountability for managing the program and periodically communicating the status of such program.

6. Responsibilities:

Position or Office	Responsibilities
Everyone at Rivier	University subsidiaries, full- and part-time employees, and Third-Parties – are responsible for supporting and complying with Information Security Program requirements outlined in this Policy. However, the following Information Security Program roles and responsibilities shall be allocated and maintained to contribute to and control the implementation of Information Security across the organization:
Senior Management	• Implementing and regularly improving the Information Security Program to be compatible with organizational strategy and operational objectives; • Providing adequate resources, and appropriately integrating the Information Security Program across Rivier business units and organizational processes; and • Promoting and supporting the Information Security Program by communicating with relevant stakeholders the importance of achieving and complying with Information Security Program objectives and requirements.
CIO/TD/ CISO	The CISO shall direct and manage implementation and continuous improvement of the Information Security Program, including: • Establishment of a process for identifying objectives for, and governance of, the Information Security

	Program that is scoped across relevant Rivier business units and organizational processes; • Maintenance of this Policy and its supporting framework of standards, procedures, and guidelines; • Design and implementation of an Information Security risk assessment process that identifies and evaluates Information Security risks against relevant risk criteria; • Design and implementation of an Information Security risk treatment process to drive formulation, implementation, and monitoring of Information Security risk treatment plans by relevant Risk Owners; • Providing for Rivier employee awareness and necessary competence to understand the implications of not complying with Information Security Program requirements and contributing to Information Security Program effectiveness; and • Monitoring and reporting on performance and effectiveness of the Information Security Program to relevant Rivier stakeholders.
Risk Owners	Risk owners are responsible for allocating or managing resources to address risk factors identified by the CISO or other relevant Information Security Program stakeholders that may adversely impact the confidentiality, integrity, and availability of Information Assets within their business function or span of organizational control.

7. Related Information:

Related Policies
Data Disposal Policy (needs to be modified)
Monthly Reporting Policy to the CA
Annual Cyber Security Risk Assessment Report to President
Data Center and Data Closet Access Policy

IT Personnel Security Policy
Information Asset tracking policy
Third Party Vendor Security Policy
IT Audit Policy
Incident Command Response Procedure
IT Backup and restore policy
Access Control Policy

8. Contacts:

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