Rivier University
Vendor Security Policy

Applies to: *Third party vendors who provide managed services or software to the University This policy continues to apply to individuals on sabbatical, other leaves or while visiting other institutions*

1. Policy:

Issued: 5/29/2025
Last Revised:
Last Reviewed:

2. Policy Purpose:

This policy outlines the cybersecurity requirements for third-party vendors who provide services to the University. The goal is to ensure that all vendors adhere to the University's cybersecurity standards to protect sensitive data and systems.

3. Scope and Application:

This policy applies to all third-party vendors, contractors, consultants, and service providers who access, process, store, or transmit university data or who provide technology services that integrate with the university's systems. It encompasses all forms of data, including but not limited to personally identifiable information (PII), protected health information (PHI), financial records, academic records, and any other sensitive or confidential information. The policy is applicable throughout the entire vendor lifecycle—from initial engagement and onboarding through contract termination—and is designed to ensure that all external partners maintain cybersecurity practices that align with the university's standards and regulatory obligations.

4. Definitions:

Definitions	
Data Encryption:	Securing data by converting it into a coded format during storage (at rest) and transmission (in transit).
Access Controls	Mechanisms to restrict data access to authorized individuals.
Role-Based Access:	Granting access based on job roles and the principle of least privilege.

5. Policy Details:

Vendor Risk Assessment

All third-party vendors must undergo a thorough risk assessment before engaging in any contractual agreements. The risk assessment will evaluate the vendor's security posture, including their policies, procedures, and technical controls.

The risk assessment process includes the following steps:

1. Initial Screening: Evaluate the vendor's security policies and practices.
2. Security Questionnaire: The vendor must complete a detailed security questionnaire.
3. Onsite Assessment: If necessary, conduct an onsite assessment of the vendor's security controls.
4. Risk Rating: Assign a risk rating based on the assessment results.
5. Approval: Obtain approval from the university's cybersecurity team before engaging the vendor.

Data Protection Requirements

Vendors must implement appropriate data protection measures to safeguard the university's sensitive information. These measures include, but are not limited to:

1. Data Encryption: Encrypt all sensitive data at rest and in transit.
2. Access Controls: Implement strict access controls to limit data access to authorized personnel only.
3. Data Backup: Regularly back up data and ensure backups are securely stored.
4. Data Disposal: Securely dispose of data that is no longer needed.

Access Controls

Vendors must implement robust access controls to ensure that only authorized personnel have access to the university's systems and data. Access controls should include:

1. User Authentication: Implement strong user authentication mechanisms, such as multi-factor authentication (MFA).
2. Role-Based Access: Assign access rights based on the principle of least privilege.
3. Access Reviews: Conduct regular access reviews to ensure access rights are up to date.
4. Logging and Monitoring: Implement logging and monitoring to detect and respond to unauthorized access attempts.

Incident Response

Vendors must have an incident response plan in place to address cybersecurity incidents. The incident response plan should include:

1. Incident Detection: Implement mechanisms to detect security incidents.
2. Incident Reporting: Report security incidents to the university's cybersecurity team within 24 hours.
3. Incident Containment: Take immediate steps to contain and mitigate the impact of the incident.

4. Incident Investigation: Conduct a thorough investigation to determine the cause and impact of the incident.
5. Incident Recovery: Restore affected systems and data to normal operation.
6. Incident Documentation: Document all incidents and the actions taken to address them.

Compliance with Regulations

Vendors must comply with all applicable regulations and standards, including but not limited to:

1. FERPA: Family Educational Rights and Privacy Act.
2. HIPAA: Health Insurance Portability and Accountability Act
3. GDPR: General Data Protection Regulation (if applicable)
4. PCI-DSS: Payment Card Industry Data Security Standard (if applicable).
5. Rivier University Information Security Policy
6. Rivier University Acceptable Use Policy

Ongoing Monitoring

The university will conduct ongoing monitoring of vendors to ensure compliance with this policy. Ongoing monitoring activities include:

1. Regular Audits: Conduct regular security audits of the vendor's systems and practices.
2. Performance Reviews: Review the vendor's performance and security posture on a regular basis.
3. Continuous Improvement: Work with vendors to continuously improve their security practices.

6. Responsibilities:

Position or Office	Responsibilities
CIO/CISO	Responsible for maintain and update the policy
Directors and managers	Responsible for ensuring vendors are aware of the policy and training their employees with Rivier tools when appropriate.

7. Related Information:

Related Policies
Information Security Policy
Data Governance Policy
Acceptable Use Policy

Vendor Due Diligence Policy

8. Contacts:

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