Rivier University
IT Personnel Security Practice Policy

Applies to: *Information Technology professionals employed or contracted 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: May 2026
Last Reviewed:

2. Policy Purpose:

This policy establishes security practices and responsibilities for all IT personnel to protect the confidentiality, integrity, and availability of the organization's information systems and data.

3. Scope and Application:

This policy applies to all employees, contractors, consultants, and third-party service providers who have access to the organization's IT systems, infrastructure, or data.

4. Definitions:

Definitions	

5. Policy Details:

Access Control

- Access to systems and data must be granted based on the principle of least privilege.
- Role-based access controls (RBAC) must be implemented and reviewed quarterly.
- All access must be logged and monitored.

Authentication and Password Management

- Multi-factor authentication (MFA) is required for all administrative access.
- Passwords must meet complexity requirements and be changed every 90 days.
- Default passwords must be changed immediately upon deployment.

Device and Endpoint Security

- All IT-managed devices must have up-to-date antivirus and endpoint protection.
- Devices must be encrypted and locked when unattended.
- Remote access must be secured via VPN and monitored.

Change Management

- All changes to systems must follow a documented change management process.
- Changes must be tested, approved, and logged before implementation.

Incident Response

- IT personnel must report security incidents immediately to the CIO
- Incident response procedures must be followed, including documentation and root cause analysis.

Training and Awareness

- IT personnel must complete annual security awareness training.
- Specialized training must be provided for roles with elevated privileges.

Termination and Role Change

- Access rights must be revoked immediately upon termination or role change.
- Exit procedures must include return of all IT assets and credentials.

Compliance and Auditing

- Regular audits will be conducted to ensure compliance with this policy.
- Non-compliance may result in disciplinary action, up to and including termination.

Confidential Information

Scope of Confidential Information

Confidential or protected information may include, but is not limited to:

- Student information, including education records protected under FERPA
- Employee information, including HR, payroll, benefits, performance, or medical data
- Admissions, financial aid, and student accounts data
- Academic records, advising notes, grading information, or academic progress data
- Institutional financial information
- System credentials, passwords, access tokens, security configurations, or logs

- Research data, when access is restricted or regulated
- Forms, documents, or records not intended for public access

Confidentiality applies regardless of how the information is encountered or stored.

6. Responsibilities:

Position or Office	Responsibilities
All IT Personnel	must adhere to this policy and report any security incidents or policy violations.
CIO	is responsible for enforcing this policy and conducting regular audits
	must ensure that all IT personnel are aware of and trained on this policy.

7. Related Information:

Related Policies
Information Security Policy
Information Security Confidentiality and Appropriate Access Acknowledgement

8. Contacts:

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