KANSAS WESLEYAN UNIVERSITY

POLICY ON INSTITUTIONAL FRAMEWORK

Administrative Division	**President's Office**
Policy Title	**Institutional Framework Policy**
Administrative Office	**President's and Provost's Office**
Effective Date of Policy	**April 27, 2026** **Amended: 09.30.26**

Purpose

To establish the framework for protecting institutional data, systems, and resources at Kansas Wesleyan University (KWU). This framework defines the expectations, safeguards, and responsibilities necessary to support a secure and compliant information-security environment.

Scope of Policy

This policy applies to all Kansas Wesleyan University (KWU) employees, students, contractors, and third-party service providers who access, manage, transmit, store, or otherwise interact with institutional information. It supports the operational and cultural foundations for information-security awareness and daily practice across the university.

The KWU Information Security Program (ISP) defines the specific administrative, technical, and physical safeguards required to protect institutional and regulated data, including FERPA-regulated information, GLBA-covered customer information, and other sensitive data.

Definitions

To ensure clarity and consistency, the following terms are used throughout this policy. For definitions related to Nonpublic Personal Information (NPI), Service Providers, and other regulated data categories, refer to the KWU Information Security Program (ISP), Section 2 ("Definitions and Scope").

- Access Control: Mechanisms that restrict access to systems and data based on user roles and permissions.
- Confidential Data: Information not intended for public release and which could cause operational or reputational harm if disclosed.
- Incident: Any event that threatens the confidentiality, integrity, or availability of KWU's information assets.
- Information Security: The practice of protecting information from unauthorized access, disclosure, alteration, and destruction.
- Public Data: Information intended for public disclosure that does not require protective measures.
- Restricted Data: Highly sensitive information protected by law, regulation, or contractual obligation; unauthorized disclosure could result in legal liability, financial loss, or significant harm.
- Sensitive Data: Information that, if compromised, could negatively impact KWU or individuals. This includes confidential and restricted data domains such as PII, financial data, and academic records.
- User: Any individual granted access to KWU systems or data, including employees, students, contractors, and affiliates.

Policy

Kansas Wesleyan University (KWU) is committed to protecting the confidentiality, integrity, and availability of institutional data and information systems. This Institutional Framework establishes the approach for managing information-security risks, ensuring compliance with applicable laws and regulations, and promoting a culture of security awareness across the university community.

Policy objectives include:

- Safeguarding sensitive, confidential, and restricted data from unauthorized access or disclosure.
- Ensuring reliable and secure access to university systems and services.
- Complying with legal and regulatory obligations (including FERPA, GLBA, and HIPAA).
- Promoting responsible and ethical use of university technology resources.
- Responding effectively to information-security incidents and breaches.

The policy is reviewed annually by the Compliance and Data Integrity Committee. Enforcement and operational oversight are supported by Information Systems, Human Resources, Department Heads, and Legal Affairs.

Procedures Referenced in ISP

The following summarizes university information-security practices aligned with and supported by the KWU Information Security Program (ISP). Operational procedures, system controls, testing schedules, and associated documentation are maintained within the ISP.

- Risk Assessment: Conducted as outlined in the ISP, including assessment of internal and external risks.
- Data Classification: Institutional data is categorized (Public, Confidential, Restricted) to ensure appropriate levels of protection.
- Access Controls: Role-based access with authentication standards such as MFA and password requirements.
- Incident Response: All information-security incidents are handled in accordance with the ISP's Incident Response Plan (IRP) and must be reported immediately to Information Systems.
- Training and Awareness: Users participate in annual training regarding information security, data handling, and phishing-prevention practices.
- Vendor and Third-Party Security: Vendors must meet ISP security requirements and sign agreements consistent with required oversight and security controls as necessary.

Compliance

Violations of this policy may result in disciplinary action, up to and including termination or expulsion, consistent with the Student Code of Conduct, Employee Handbook, Faculty Handbook, and applicable laws. Compliance with this policy supports and aligns with the requirements of the KWU Information Security Program (ISP). In cases of conflict or ambiguity, the ISP governs.

Training and Adherence Requirements

KWU ensures that all employees who access, manage, or store institutional information receive timely and role-appropriate training on the requirements and safeguards outlined in this policy and the ISP. Training is provided during onboarding and reinforced through:

- Annual information-security training
- Periodic security awareness communications
- Phishing-awareness exercises

- Targeted professional development coordinated by Information Systems, Compliance, and Human Resources

Employees must follow all institutional data-security policies as a condition of continued system access. This requirement also applies to contractors and third-party service providers acting on KWU's behalf.

Contractors must adhere to the ISP, this policy, and all applicable regulatory expectations. KWU enforces these requirements through:

- Contractual security and compliance obligations
- Documented onboarding and orientation to relevant policies
- Ongoing monitoring and review
- Verification of FERPA, GLBA, and institutional data-protection standards

Review Cycle

Generally, this policy shall be reviewed annually or when significant changes occur in technology, regulatory requirements, or institutional operations. Annual review ensures continued alignment with the KWU Information Security Program (ISP) and the Gramm–Leach–Bliley Act Safeguards Rule.