Missouri Western State University

Policy Name: Information Security and Cybersecurity Policy	**Date Effective:** July 1, 2026
Policy Category: Information Technology	**Date Last Revised:**
Approving Authority: Vice President for Finance and Administration	**Date Last Reviewed:**
Responsible Office: Technology Services	**Recommended Review Cycle:** 3 years

I. Purpose

The purpose of this Information Security and Cybersecurity Policy is to define the security measures and responsibilities for safeguarding the confidentiality, integrity, and availability of Missouri Western State University's information assets, including sensitive data, against cyber threats and vulnerabilities. This plan complements the university's Data Governance and Record Retention Policy by focusing specifically on cybersecurity protections and safeguards for sensitive data per regulatory requirements, including the Gramm-Leach-Bliley Act (GLBA), and best practices outlined in the NIST Cybersecurity Framework (CSF).

II. Applicability

This policy applies to all employees, students, third-party vendors, and any individuals or entities that have access to Missouri Western State University's information systems, networks, and data. This policy covers all systems, devices, software, and services used in the processing, storage, or transmission of sensitive information. This policy addresses all information, regardless of the form or format, that is created or used in support of the business activities of the University.

III. Definitions

Covered Data. Information contained in either University computer systems or in physical copy that is utilized for the purposes of conducting University business or learning. The terms "data" and "information" are used interchangeably throughout this policy.

Encryption. The transformation of data through an algorithmic process using a cryptographic key to render the information unintelligible during electronic transmission of the information.

NPI. - Non-public personal information (NPI) encompasses personally identifiable financial information collected by financial institutions in connection with providing financial products or services, excluding information that is publicly available. NPI includes Federal Tax Information (FTI), Financial Information, and Servicers.

Record. Any material upon which written, drawn, spoken, visual or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics that contain Sensitive Information. The term Record includes both paper and electronic material.

Sensitive Information. Any data, electronic or physical copy, of which the compromise with respect to confidentiality, integrity, and/or availability could have a material adverse effect on University interests, the conduct of University programs or the privacy to which individuals are entitled. Examples of such data would include that data protected by the Government Records Access and Management Act (GRAMA), Family Education Rights and Privacy Act (FERPA), Gramm-Leach-Bliley Act (GLBA) or other laws governing the use of data or data that has been deemed by the University as requiring protective measures.

IV. Policy

Missouri Western State University is committed to protecting employee and student data and our internal systems by adhering to the following principles:

- **Confidentiality:** Ensure that sensitive and nonpublic personal information (NPI) is protected from unauthorized access, disclosure, or use.
- **Integrity:** Ensure the accuracy and completeness of data and systems, preventing unauthorized modification or destruction.
- **Availability:** Ensure that systems, applications, and data are available and accessible as needed by authorized users.

The unauthorized addition, modification, deletion, or disclosure of Sensitive Information or NPI included in University data files is expressly forbidden.

V. Procedures/Policy Details

1. Plan Coordination

Security Coordinator (Responsible Authority)

Chief Information Officer (CIO)/Information Security Officer (ISO): The Chief Information Officer (CIO) is responsible for the overall administration of this policy, ensuring compliance with relevant laws and regulations, and overseeing the implementation of the university's cybersecurity initiatives.

2. Training of Staff

All employees will receive cybersecurity training at the time of hiring and annually thereafter. This training will cover topics such as:

- Identifying and preventing phishing attacks
- Protecting passwords and credentials
- Proper handling of sensitive information
- Reporting security incidents and suspicious activity

The training program will be continuously updated to reflect emerging threats and changes in regulatory requirements.

V. 3. Risk Management and Assessment

- Missouri Western State University will conduct regular risk assessments to identify, assess, and mitigate cybersecurity risks to information systems and sensitive data.
- Risk assessments will include evaluating the potential impact of cybersecurity threats, vulnerabilities, and potential consequences of a data breach or security incident.
- Based on risk assessments, appropriate security controls will be implemented to minimize risk and protect sensitive data.

VI. 4. Safeguards and Monitoring, Access Control

- Access to sensitive systems and data will be granted on a need-to-know basis. Users will be assigned roles with access privileges tailored to their job functions.
- User authentication will be enforced through strong password policies, multi-factor authentication (MFA), and identity management systems.

- Privileges will be reviewed periodically, and access rights will be revoked for users who no longer need access to specific systems or data.

5. Data Protection and Encryption

- All sensitive data, including nonpublic personal information (NPI), will be protected through encryption both in transit and at rest using industry-standard encryption protocols (e.g., AES-256, TLS 1.2 or higher).
- Data classification standards will be applied to determine the sensitivity of information and apply appropriate safeguards.
- Sensitive data will be securely deleted when no longer required for business or legal purposes.

6. Incident Response and Breach Notification

- Missouri Western State University will maintain a formal incident response plan to detect, respond to, and recover from cybersecurity incidents.
- Employees, students, and contractors must report any suspicious activity, security incidents, or data breaches immediately to the Chief Information Officer (CIO).
- In the event of a data breach involving employee or student data, Missouri Western State University will notify affected customers as required by GLBA and other applicable data protection laws, including the timing and content of notifications.

7. Continuous Monitoring and Improvement

- Missouri Western State University will implement continuous monitoring tools to detect potential cybersecurity threats, including intrusion detection systems (IDS), security information and event management (SIEM) solutions, and vulnerability scanning tools.
- Security controls and practices will be regularly tested through penetration testing, vulnerability assessments, and internal audits.
- The organization will continuously evaluate the effectiveness of the cybersecurity program and adjust policies and procedures as needed to address new threats, vulnerabilities, and regulatory changes.

8. Third-Party Vendor Management

- All third-party vendors with access to sensitive customer data or critical systems will be required to comply with Missouri Western State University's cybersecurity requirements.
- Third-party agreements will include cybersecurity provisions, including requirements for data protection, access control, breach notification, and security audits.
- Vendors will be regularly assessed for their compliance with Missouri Western State University's security standards, including conducting risk assessments and security reviews before engagement and annually thereafter.

9. **Consequences for Policy Violations or Failure to Comply** with this and related policies is subject to disciplinary action, up to and including suspension without pay, or termination of employment or association with the University, in accordance with applicable (e.g., staff, faculty, student) disciplinary procedures.

VII. Compliance with Legal and Regulatory Requirements

Missouri Western State University will ensure compliance with all applicable laws and regulations related to cybersecurity and data protection, including but not limited to:

- Gramm-Leach-Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)G
- Family Educational Rights and Privacy Act (FERPA)
  State-specific data protection laws

Compliance will be verified through internal audits, third-party assessments, and by maintaining appropriate documentation.

VIII. Consequences for Policy Violation

Failure to comply with this and related policies is subject to disciplinary action, up to and including suspension without pay, or termination of employment or association with the University, in accordance with applicable (e.g. staff, faculty, student) disciplinary procedures.

IX. References

NIST Cybersecurity Framework: This framework, developed by the National Institute of Standards and Technology (NIST), is a widely recognized standard for developing and implementing cybersecurity programs. It provides a comprehensive approach to managing cybersecurity risk, from identifying vulnerabilities to implementing controls and monitoring effectiveness. The NIST Cybersecurity Framework is available at https://www.nist.gov/cyberframework.

HIPAA: The Health Insurance Portability and Accountability Act (HIPAA) sets standards for protecting sensitive patient health information. It requires healthcare organizations to implement robust security measures to safeguard electronic protected health information (ePHI) from unauthorized access, use, or disclosure. https://www.hhs.gov/hipaa/index.html

Federal Trade Commission (FTC) Safeguards Rule: This rule, issued under the GLBA, provides specific requirements for financial institutions to develop and implement information security programs to protect customer data. https://www.ftc.gov/legal-library/browse/rules/safeguards-rule

FERPA (Family Educational Rights and Privacy Act) plays a significant role in cybersecurity policies for educational institutions by mandating the protection of student data and requiring institutions to implement appropriate security measures to safeguard this information. https://studentprivacy.ed.gov/data-security-k-12-and-higher-education

X. Appendix A: Incident Reporting and Response Quick Reference

Step	Action	Responsible Party
Suspected incident identified	Stop work if possible; isolate device	Employee / Student / IT
Report incident immediately	Notify CIO / ISO via designated reporting channel	All Users
Initial investigation & triage	Assess scope and severity	CIO / IT Security Team
Containment & eradication	Shut down or patch systems as needed	IT Team

Step	Action	Responsible Party
Notification	Notify affected individuals if required by law	CIO / Legal / PR
Post-incident review	Document lessons learned, update procedures	IT / Risk Management / Legal