INFORMATION SECURITY PROGRAM POLICY

Northeastern State University

Approved by: Northeastern State University Executive Cabinet **Responsible Official:** Director of I.T. Infrastructure (918) 444-5887 **Forms:**	**History:** Adopted-May 14, 2024 **Revision:** August 18, 2025 **Related Policies:** **Additional References:** NIST 800-171 Resource, CMMC 2.0 Resourse

1. **OBJECTIVE**

The objective of Northeastern State University in developing, maintaining, and implementing this **Information Security Program** (ISP) is to create effective administrative, technical, and physical safeguards to protect the confidentiality, integrity, and availability of institutional data, including but not limited to:

- Personally Identifiable Information (PII)
- FERPA-protected records
- Research data
- Intellectual property
- Controlled Unclassified Information (CUI)
- Financial and operational data

This Information Security Program sets forth Northeastern State University's procedures for evaluating and addressing its methods of accessing, collecting, storing, using, transmitting, and protecting such data.

2. **PURPOSE**

The purpose of this Information Security Program is to better:

- Support Northeastern State University's teaching, research, and service mission by ensuring the security and proper management of institutional data.
- Ensure the security, confidentiality, integrity, and appropriate availability of institutional data.
- Protect against reasonably anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.

- Protect against unauthorized access to or use of Northeastern State University's maintained data in a manner that could result in substantial harm or inconvenience to any individual, partner, or the University.
- Ensure compliance with applicable regulatory frameworks and standards, including but not limited to:
    - Gramm-Leach-Bliley Act (GLBA)
    - Family Educational Rights and Privacy Act (FERPA)
    - Health Insurance Portability and Accountability Act (HIPAA)
    - Cybersecurity Maturity Model Certification (CMMC)
    - Payment Card Industry Data Security Standard (PCI DSS)

3. SCOPE

This Information Security Program applies to:

- All employees, staff, faculty, students, and affiliated entities of Northeastern State University.
- All third-party service providers, contractors, vendors, and hosted cloud services that create, process, store, transmit, or access institutional data on behalf of the University.
- All institutional data—regardless of format (electronic, paper, or otherwise)—that is created, collected, stored, transmitted, or maintained by Northeastern State University or by third parties on its behalf.
- Institutional data includes, but is not limited to:
    - Personally Identifiable Information (PII) (e.g., names, addresses, Social Security Numbers)
    - Student Records protected under FERPA
    - Financial data and payment information protected under GLBA and PCI DSS
    - Health-related information subject to HIPAA
    - Controlled Unclassified Information (CUI)
    - Research data, intellectual property, personnel and employment records

4. INFORMATION SECURITY COORDINATOR

The Director of IT Infrastructure serves as the Information Security Coordinator and is responsible for:

- Overseeing the development, implementation, and maintenance of the University's information security program.
- Managing and coordinating the periodic risk assessment process.
- Leading the development, review, and distribution of information security policies and procedures.
- Coordinating the University's incident response program.
- Overseeing the information security awareness and training program.
- Managing the third-party risk management program.
- Providing an annual report on the effectiveness of the information security program to University leadership.

5. RISK ASSESSMENT

Northeastern State University will conduct periodic, documented risk assessments:

- Annually.
- Prior to major system implementations or changes.
- After significant security incidents.
- In response to changes in applicable regulations or the threat landscape.

Risk assessments will consider:

- Emerging threats and vulnerabilities.
- Technology and business process changes.
- Third-party services and vendors.
- Results of audits, scans, and tests.
- Regulatory requirements.

6. INFORMATION SECURITY POLICIES AND PROCEDURES

Northeastern State University will implement and maintain policies and procedures that:

- Ensure personnel can enact the information security program in accordance with 16 CFR 314.4(e).
- Are reviewed and updated at least annually or as necessary to reflect lessons learned and changing risks.
- Address:
    - Roles and responsibilities.
    - Secure data handling and transmission.
    - User access management, encryption, Single Sign-On (SSO), Multi-Factor Authentication (MFA), and logging/monitoring.
    - Incident response.
    - Third-party risk management.
    - Security awareness and training.

7. SAFEGUARDS

Northeastern State University will:

- Implement and periodically review role-based access controls.
- Conduct periodic inventory of institutional data and document data flows.
- Encrypt institutional data at rest and in transit.
- Require MFA for systems handling sensitive data.
- Dispose of data in accordance with NIST SP 800-88 guidelines.
- Evaluate and document security impacts of system and network changes.
- Maintain centralized logging and automated monitoring of key systems.
- Assess applications for common vulnerabilities (OWASP Top 10) before deployment.
- Provide ongoing training to employees, students, contractors, and vendors.

- Conduct formal security and compliance evaluations of third-party applications from service providers.
- Maintain a formal change management process to ensure that modifications to systems, applications, and networks are properly documented, reviewed, tested, and approved.

8. SERVICE PROVIDER OVERSIGHT

Northeastern State University will:

- Require service providers that process or store institutional data to provide a HECVAT or equivalent and penetration test reports upon request.
- Require contractual provisions for:
    - Prompt notification of security incidents or data breaches.
    - Subcontractor compliance with equivalent standards.
    - Monitor and periodically reassess service provider performance.
    - Require secure data return or disposal upon contract termination.
- Conduct formal security and compliance evaluations of third-party applications from service providers. The institution reserves the right to approve or deny the use of such applications based on risk assessments, regulatory requirements (e.g., FERPA, GLBA, HIPAA), and alignment with institutional security policies.

9. MONITORING

Northeastern State University will:

- Maintain centralized logging of key systems and automated alerting.
- Conduct periodic vulnerability scanning and penetration testing.
- Track and remediate identified vulnerabilities.
- Report on monitoring metrics to leadership and as part of annual reviews.

10. INCIDENT RESPONSE

Northeastern State University's Incident Response Plan will include:

- Defined roles and responsibilities.
- Notification procedures (internal, external, legal).
- Containment, eradication, and recovery procedures.
- Evidence preservation guidelines.
- Post-incident reporting and lessons learned.
- Annual testing of the incident response plan through exercises or simulations.

11. ENFORCEMENT

Violations may result in disciplinary action or termination of relationships, in accordance with University policies and applicable laws.

12. PROGRAM REVIEW & CHANGE MANAGEMENT

Northeastern State University will review this ISP:

- Annually.
- After significant incidents.
- Following changes in technology, business practices, or regulations.
- Based on the results of risk assessments, audits, and monitoring.

Information Security Program reviews will result in action plans to address gaps and opportunities for improvement.

PROGRAM GLOSSARY

Term	Definition
Access Controls	Mechanisms to ensure that only authorized users can access specific systems or data.
Change Management	Structured process for managing changes to IT systems and networks.
Controlled Unclassified Information (CUI)	Information requiring safeguarding under applicable regulations.
Cybersecurity Maturity Model Certification (CMMC)	A framework for assessing cybersecurity maturity and compliance.
Encryption	Encoding data to protect it from unauthorized access.
Higher Education Community Vendor Assessment Tool (HECVAT)	A security questionnaire for evaluating vendor security practices.
Incident Response (IR)	Processes to detect, contain, and recover from cybersecurity incidents.
Logging and Monitoring	Recording and analyzing system and user activity.
Multi-Factor Authentication (MFA)	Requiring multiple methods of authentication to verify user identity.

National Institute of Standards and Technology (NIST)	U.S. federal agency that develops cybersecurity standards and best practices.
Penetration Testing	Simulated attacks to identify system vulnerabilities.
Personally Identifiable Information (PII)	Information that can identify an individual.
Risk Assessment	Identifying and evaluating risks to institutional data.
Safeguards	Controls and procedures to protect institutional data.
Security Incident	An event that may indicate that systems or data have been compromised.
Service Provider	A vendor, contractor, or third-party entity processing institutional data.
Single Sign-On (SSO)	Allows users to access multiple applications or systems using a single set of login credentials, streamlining authentication and enhancing security
Vulnerability Scanning	Automated process to identify system vulnerabilities.
Information Security Program (ISP)	NSU's formal program for protecting institutional data.