WRITTEN INFORMATION SECURITY PROGRAM POLICY

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

1. OBJECTIVE

The objective of Northeastern State University in the development, maintenance and implementation of this comprehensive written information security program ("WISP") is to create effective administrative, technical, and physical safeguards for the protection of personally identifiable information (PII) of our employees, students, and affiliated entities. This WISP sets forth Northeastern State University's procedure for evaluating and addressing its electronic and physical methods of accessing, collecting, storing, using, transmitting, and protecting PII.

2. PURPOSE

The purpose of this WISP is to better:

- Ensure the security, confidentiality, integrity, and appropriate availability of PII Northeastern State University collects, creates, uses, and maintains;
- Protect against any 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 PII in a manner that could result in substantial harm or inconvenience to any customer or employee; and
- Define an information security program that is appropriate to Northeastern State University's size, scope, and business its available resources; and the amount of PII that NSU owns or maintains on behalf of others, while recognizing the need to protect both customer and employee information.

3. SCOPE

This WISP applies to all employees, students, and affiliated entities of Northeastern State University. It applies to any records that contain PII in any format and on any media, whether electronic or paper form.

For purposes of this WISP, "personally identifiable information" means either a first and last name or first initial and last name in combination with any one or more of the following data elements, or any of the following data elements standing alone or in combination, if such data elements could be used to commit identity theft against the individual:

- Social Security number;
- Banner ID;
- Driver's license number, other government-issued identification number, including passport number or tribal identification number;
- Account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password that would permit access to the individual's financial account.
- Health insurance identification number, subscriber identification number, or other unique identifier used by a health insurer.
- Email address with any required security code, access code, or password that would permit access to an individual's personal, medical, insurance, or financial account.
- PII does not include lawfully obtained information that is available to the general public, including publicly available information from federal or local government records.

4. INFORMATION SECURITY COORDINATOR

NSU has designated the Director of Infrastructure as the qualified individual to implement, coordinate, and maintain this WISP.

5. RISK ASSESSMENT

As a part of developing and implementing this WISP, Northeastern State University will conduct a periodic, documented risk assessment on a regular basis, and at least annually or whenever there is a material change in University business practices that may implicate the security, confidentiality, integrity, or availability of records containing personally identifiable information. (NIST 800-171 3.11.1/CMMC 2.0)

6. INFORMATION SECURITY POLICIES AND PROCEDURES

As part of this WISP, Northeastern State University will develop, maintain, and distribute information security policies and procedures in accordance with applicable laws and standards to relevant employees, students, and affiliated entities that will establish policies and procedures appropriate for the effective protection and security of the University.

7. SAFEGUARDS

Northeastern State University will develop, implement, and maintain reasonable administrative, technical, and physical safeguards in accordance with applicable laws and standards to protect the security, confidentiality, integrity, and availability of personally identifiable information that The University owns or maintains on behalf of others.

Safeguards shall be appropriate to the size, scope, and business; its available resources; and the amount of personal information that is owned or maintained on behalf of others, while recognizing the need to protect both customer and employee information;

8. SERVICE PROVIDER OVERSIGHT

Reasonable steps will be taken to select, retain and oversee each third party service provider that may have access to or otherwise create, collect, use, or maintain PII on its behalf by:

- Evaluating the service provider's ability to implement and maintain appropriate security measures, consistent with this WISP and all applicable laws, regulations, mandates and institutional policy and obligation.
- Requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws, regulations, mandates and institutional policy and obligations.
- Monitoring and auditing the service provider's performance to verify compliance with this WISP and all applicable laws, regulations, mandates and institutional policy and obligations.

9. MONITORING

Regular testing and monitoring of the implementation and effectiveness of the information security program to ensure that it is operating in a manner reasonably calculated to prevent unauthorized access to or use of personally identifiable information. After each risk assessment, any gaps found will be addressed to ensure confidentiality, integrity, availability, and incident response procedures are updated to reasonably and appropriately address identified gaps.

10. INCIDENT RESPONSE

NSU will establish a written incident response plan designed to promptly respond to, and recover from, any security event materially affecting the confidentiality, integrity, or availability of customer information in your control.

11. ENFORCEMENT

Violations of this WISP may result in disciplinary action, in accordance with information security policies and procedures and human resources policies. Please see Northeastern State University's HR policy for details regarding The University's disciplinary process.

12. PROGRAM REVIEW & CHANGE MANAGEMENT

Northeastern State University will review this WISP and the security measures defined herein will conduct a review on a regular basis, and at least annually or whenever there is a material change in the University's business practices that may reasonably implicate the security, confidentiality, integrity, or availability of institutional assets and data.

PROGRAM GLOSSARY

Term	Definition
Controlled Unclassified Information (CUI)	Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable laws, regulations, and government-wide policies
Cybersecurity Maturity Model Certification (CMMC)	An assessment framework and assessor certification program designed to increase the trust in measures of compliance to a variety of standards published by the National Institute of Standards and Technology.
Incident Response	The preparation, detection, analysis, containment, and recovery activities to support incident declaration/resolution
Information/Data Classification	The process of categorizing data assets based on their information sensitivity
National Institute of Standards & Technology (NIST)	a set of guidelines for mitigating cybersecurity risks, published by the US National Institute of Standards and Technology (NIST) based on industry standards, guidelines, and best practices.
Personally Identifiable Information (PII)	Information that, when used alone or with other relevant data, can identify an individual
Risk Assessment	A process with multiple steps that intends to identify and analyze all of the potential risks and issues that are detrimental to the business
Safeguards	Appropriately configured controls and processes that match and align with the necessary requirements needed for effective security
Security Incident	An event that may indicate that an organization's systems or data have been compromised or that measures put in place to protect them have failed.
Service Provider	A vendor that provides IT solutions and/or services to end users and organizations
WISP	Written Information Security Program