Written Information Security Program (WISP)

Responsible Executive/University System Officer: Chief Information Security Officer (CISO)
Responsible Office: Cybersecurity Governance Risk and Compliance (GRC)
Approved Distribution: PUBLIC
Status: IN FORCE

1. Introductory
The objectives of this comprehensive written information security program (WISP) include defining, documenting, and supporting the implementation and maintenance of the administrative, technical, and physical safeguards USNH has selected to protect the personal information it collects, creates, uses, and maintains.

2. Purpose
The University System of New Hampshire (USNH) Written Information Security Program (WISP) is intended to:

- Ensure the security, confidentiality, integrity, and availability of personal and other sensitive information that USNH collects, creates, uses, and maintains.
- Protect against any anticipated threats or hazards to the security, confidentiality, integrity, or availability of such information.
- Protect against unauthorized access to or use of USNH maintained personal and other sensitive information that could result in substantial harm or inconvenience to any customer or employee.
- Define an information security program that is appropriate to USNH’s size, scope, and business, its available resources, and the amount of personal and other sensitive information that USNH 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 USNH community members and third parties.
This WISP applies to USNH computing, network and information systems and services.

The data covered by this WISP includes any information stored, accessed or collected at UNSH or for USNH operations, whether in paper, electronic or other form.
4. Roles and Responsibilities

USNH has designated the Chief Information Security Officer (CISO) and the Cybersecurity department to implement, coordinate, and maintain this WISP. USNH Cybersecurity shall be responsible for:

- Implementation and maintenance of this WISP, including:
  - Assessing internal and external risks to personal and other sensitive information and maintaining related documentation, including risk assessment reports and remediation plans;
  - Coordinating the development, distribution, and maintenance of information security policies, standards and procedures;
  - Coordinating the design of reasonable and appropriate administrative, technical, and physical safeguards to protect personal and other sensitive information;
  - Ensuring that the safeguards are implemented and maintained to protect personal and other sensitive information throughout USNH, where applicable;
  - Overseeing service providers that access or maintain personal and other sensitive information on behalf of USNH;
  - Monitoring and testing the information security program’s implementation and effectiveness on an ongoing basis;
  - Defining and managing incident response procedures; and
  - Establishing and managing enforcement policies and procedures for this WISP, in collaboration with USNH human resources and management.

- Engaging qualified information security personnel, including:
  - Providing them with security updates and training sufficient to address relevant risks; and
  - Verifying that they take steps to maintain current information security knowledge.

- Employee, contractor, and (as applicable) stakeholder training, including:
  - Providing periodic training regarding this WISP, USNH’s safeguards, and relevant information security policies and procedures for all employees, contractors, and (as applicable) stakeholders who have or may have access to personal or other sensitive information, updated as necessary or indicated by USNH’s risk assessment activities.
  - Ensuring that training attendees formally acknowledge their receipt and understanding of the training and related documentation.
  - Retaining training and acknowledgment records.

- Defining and managing an exceptions process to review, approve or deny, document, monitor, and periodically reassess any necessary and appropriate, business-driven requests for deviations from this WISP or USNH’s cyber security policies and procedures.
• Periodically, but at least annually, reporting to USNH’s management and the Board of Trustees in writing regarding the status of the WISP and USNH’s safeguards to protect personal and other sensitive information, including the program’s overall status, compliance with applicable laws and regulations, material matters related to the program, such as risk assessment, risk management and control decisions, service provider arrangements, testing results, cyber incidents or policy violations and management’s responses, and recommendations for program changes.

5. Related Security Policies and Procedures

As part of this WISP, USNH will develop, maintain, and distribute information security policies and standards in accordance with applicable laws and regulations.

• Establish and maintain the following policies;
  o USNH Acceptable Use Policy
  o USNH Cybersecurity Policy
  o USNH Information Classification Policy
  o USNH Password Policy
  o USNH Privacy Policy

• Maintain all Cybersecurity standards established to protect institutional data.

• Ensure policies and standards are in alignment with applicable federal, state, and local regulations;
  o Family Educational Rights and Privacy Act (FERPA)
  o General Data Protection Regulation (GDPR)
  o Gramm-Leach-Bliley Act (GLBA)
  o Health Insurance Portability and Accountability Act (HIPAA)
  o Payment Card Industry (PCI)
  o Red Flags Rule

6. Identification and Assessment of Risks to USNH

As a part of developing and implementing this WISP, USNH will conduct and base its information security program on a periodic, documented risk assessment, at least annually, or whenever there is a material change in USNH’s business practices that may implicate the security, confidentiality, integrity, or availability of records containing personal or other sensitive information. This process is outlined by the USNH Risk Management Standard.

7. Data Safeguards
USNH 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 personal or other sensitive information that USNH owns or maintains on behalf of others.

**Data Classification**

USNH employs a comprehensive data classification schema that leverages four levels of classification. Each category denotes a unique level of sensitivity. Data classification is as follows: 1. Public, 2. Protected, 3. Restricted, 4. Sensitive.

Once data is classified, departments must ensure that the appropriate levels of security controls are applied to the data.

**Encryption**

USNH requires that all users employ USNH Cybersecurity approved encryption solutions to all sensitive USNH data to preserve the confidentiality and integrity of and control the accessibility to, where this data is processed, stored or transmitted.

**Access & Storage**

Access to USNH data and systems is granted through authorized access controls established by USNH. Access is reviewed on a periodic basis to ensure access is appropriate.

**Data Destruction**

Records containing personal or sensitive information are destroyed once the information is no longer fit for business needs unless federal guidelines require that information be destroyed by a particular timeframe. Data is destroyed in such a way that cannot be recovered after the process is complete.

**8. Computer System Safeguards**

USNH applies industry best practices to maintaining the confidentiality, availability, and integrity of information systems by maintaining up-to-date firewall protection, operating system security patches, and malware protection. The most current security updates are applied regularly. USNH performs regular Intrusion Detection monitoring and logging to prevent unauthorized access.

**9. Password requirements**
USNH requires that all users and members authenticate with an unique ID and password to access systems and data. Passwords must adhere to the USNH Password Policy. USNH may require higher forms of authentication such as Single Sign On (SSO) or Multi-Factor Authentication (MFA).

10. Third Party Agreements

USNH will assess each of its service providers that may have access to or otherwise create, collect, use, or maintain personal or other sensitive information 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 and USNH’s obligations, requiring the service provider by contract to implement and maintain reasonable security measures, consistent with this WISP and all applicable laws and USNH’s obligations.

Data owners / stewards are responsible for confirming third-party service providers are maintaining appropriate security measures and data handling procedures to protect USNH data consistent with this program.

11. Employee training

USNH requires that all employees are trained in the handling and care of sensitive data and information. Training may consist of onboarding, privacy security and online certifications. All users are required to follow standards and guidelines in conjunction with any training to ensure secure data handling.

12. Incident Response and Reporting

Incidents that raise concerns about the privacy or security of Personal Information must be reported promptly upon discovery to USNH Cybersecurity.

The Cybersecurity Incident Response Team shall investigate all reported security incidents and Breaches. Led by the Cybersecurity Operations Directory, the Cybersecurity Incident Response Team is responsible for:

- Development and maintenance of the USNH information security incident response plan.
- Coordination and response to incidents in accordance with the requirements of federal, state and local laws.
- Minimize the potential negative impact to USNH, client and 3rd party as a result of such incidents.
- Restore services to a normalized and secure state of operation.
- Provide clear and timely communication to all interested parties.

13. Enforcement

Violations of this WISP may result in disciplinary action in accordance with USNH HR Policy.
14. Appendix

- **Family Educational Rights and Privacy Act (FERPA)**
  - A federal law that protects the privacy of student education records. The law applies to all schools that receive funds under an applicable program of the U.S. Department of Education. FERPA gives parents certain rights with respect to their children’s education records. These rights transfer to the student when he or she reaches the age of 18 or attends a school beyond the high school level. Students to whom the rights have transferred are "eligible students."

- **General Data Protection Regulation (GDPR)**
  - A regulation in the European Union (EU) law for data protection and privacy. This policy sets forth a standard for any organization involved with the transferring or collecting of data and information from the citizens of the European Union. In the University setting, schools must follow the privacy guidelines in order to protect the data of international students.

- **Gramm-Leach-Bliley Act (GLBA)**
  - The Gramm-Leach-Bliley Act requires financial institutions or companies that offer consumers financial products or services like loans, financial or investment advice, or insurance to explain their information sharing practices to their customers and to safeguard sensitive data.

- **Health Insurance Portability and Accountability Act (HIPAA)**
  - The Health Insurance Portability and Accountability Act (HIPAA) requires that any medical institution or university protect and maintain the privacy of a patient's or student's electronic medical records.

- **Payment Card Industry (PCI)**
  - The PCI is a set of technical and operational standards set forth to protect a cardholder’s financial data and information that organizations must follow. These standards ensure that organizations use secure and best practice methods to accept, transmit or store card data.

- **Red Flags Rule**
  - The Red Flags Rule requires many businesses and organizations to implement a written Identity Theft Prevention Program designed to detect the warning signs or red flags of identity theft in their day-to-day operations.

15. Document History

Effective Date: 3/17/23
Drafted: USNH Cybersecurity GRC
Reviewed by: USNH Cybersecurity Committee
Approved by: Tom Nudd

Written Information Security Policy
Effective Date: 3/17/23
Last Revised Date: 3/17/23