University System of New Hampshire

CYBERSECURITY AWARENESS AND TRAINING STANDARD

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: PUBLIC
Status: IN REVIEW

1 PURPOSE

Our people are the best resource we have for safeguarding the privacy of our constituents and the confidentiality, integrity, and availability of the information we hold on their behalf. To leverage this powerful resource, we must work together as a University System to cultivate a Cybersecurity aware culture. This kind of culture facilitates the integration of Cybersecurity best practices into day to day activities, operational business processes, and decision making at all levels of the University System of New Hampshire (USNH).

This Standard defines the Cybersecurity Awareness and Training Program which ensures all USNH community members:

- Know their cybersecurity responsibilities
- Know how to properly utilize and protect the institutional information and information technology resources entrusted to them
- Understand how to comply with the cybersecurity Policies and Standards that apply to them

2 SCOPE

This Standard applies to all USNH community members who have access to USNH information technology resources and institutional information, regardless of its format. It defines all aspects of Cybersecurity Awareness and Training at USNH.

3 AUDIENCE

All USNH community members with active relationships with USNH and its component institutions, including students, faculty, and staff, should understand the requirements outlined in this Standard.

University System of New Hampshire

4 STANDARD

CYBERSECURITY AWARENESS AND TRAINING PROGRAM

In support of our core mission of education, the Chief Information Security Officer (CISO) shall ensure all employees are aware of their cybersecurity responsibilities and have the necessary knowledge and training to fulfill them by implementing a Cybersecurity Awareness and Training Program. The program shall be inclusive of all awareness and training components defined in this Standard.

CYBERSECURITY AWARENESS

Under the oversight of the CISO, Cybersecurity Governance, Risk, & Compliance (GRC) shall develop, implement, administer, facilitate, and manage a range of activities geared to building a security-aware culture across all USNH institutions. These activities shall include, but not be limited to:

- Participating in institution-wide events like University Day
- Hosting speakers, presentations, and interactive sessions targeting specific cybersecurity topics
- Providing in-person training or advisory services to address specific concerns for administrative, academic, and business units
- Issuing alerts and advisories, as appropriate, to the USNH community
- Representing cybersecurity on institutional committees and task forces
- Coordinating and running Cybersecurity incident response drills
- On-campus awareness mechanisms like digital signs, websites, etc.

EMPLOYEE CYBERSECURITY TRAINING

New Employees

All newly hired USNH employees shall complete basic cybersecurity training, either in-person or via a computer-based training (CBT) program, within the first 30 days of employment. Assessment of content comprehension shall be used to gauge the effectiveness of the training. The New Hire Cybersecurity Training Program shall be developed, implemented, managed, and maintained by Cybersecurity GRC.

Current Employees

All USNH employees shall complete a cybersecurity refresher training course, either in-person or via a CBT program, annually. Assessment of content comprehension shall be used to gauge the effectiveness of the training. The Employee Cybersecurity Training Program shall be developed, implemented, managed, and maintained by Cybersecurity GRC.

Additionally, all USNH employees participate in the USNH Phishing Awareness Program outlined below.

ROLE-SPECIFIC TRAINING FOR EMPLOYEES

Employees whose responsibilities require interaction with certain types of institutional information as well as those with specific cybersecurity responsibilities shall be required to complete role-specific cybersecurity training courses. Managers in administrative, academic, and business units with cybersecurity role-based training requirements are responsible for notifying Cybersecurity GRC when new employees join the unit. Managers of these units shall provide a current list of employees, annually, to facilitate completion of training requirements.

Although specific required frequencies are defined for each role-based training requirement, substantial changes to regulations, security control implementations, or information technology resources used in these areas may result in a requirement to complete out of band training.

The following areas currently have role-based training requirements:

- **GLBA Cybersecurity Training**
  - Any employee who interacts with student financial aid information is required to complete the designated cybersecurity training course, in person or via CBT, annually, to satisfy GLBA (Gramm Leach Bliley Act) training requirements
  - Cybersecurity GRC is responsible for developing, implementing, maintaining, and monitoring compliance with the GLBA Cybersecurity Training Program
- **PCI-DSS Compliance Training**
  - Any employee who handles credit card processing is required to complete the designated PCI-DSS (Payment Card Industry – Data Security Standard) Training Program via CBT, annually
  - The PCI data stewards at each institution are responsible for developing, implementing, maintaining, and monitoring compliance with the PCI-DSS Training Program
- **HIPAA Compliance Training**
  - All employees working in components subject to HIPAA (Health Insurance Portability and Accountability Act) Regulations are required to complete training, in person or online
  - The HIPAA Privacy Officer is responsible for developing, implementing, maintaining, and monitoring compliance with the HIPAA Training Program, with assistance from Cybersecurity GRC
- **Advanced Cybersecurity Training**
  - Employees with specific cybersecurity responsibilities may be required to complete additional training programs at the discretion of the CISO
  - Employees who are required to complete this type of training will be notified by Cybersecurity & Networking and advised on additional training requirements

  - Cybersecurity GRC is responsible for developing, implementing, maintaining, and monitoring compliance with any advanced cybersecurity requirements
- **Cybersecurity Incident Response Training**
  - Cybersecurity GRC provides training on the Incident Response Plan and any related, role-specific procedures
  - Role-based annual training is required for the following:
    - All members of the Cybersecurity Ops & IAM (Cyber Ops) team
    - Non-Cyber Ops members of the standing IRT (including back-up designees)
    - Institutional Subject Matter Experts
    - First level support team members (specifically on Cybersecurity Incident Reporting Procedures)

STUDENT CYBERSECURITY TRAINING

All incoming freshman and transfer students are required to complete basic cybersecurity training as part of orientation.

The Student Cybersecurity Training Program shall be developed, implemented, managed, and maintained by Cybersecurity GRC.

Additionally, all enrolled students at USNH component institutions participate in the USNH Phishing Awareness Program outlined below.

USNH PHISHING AWARENESS PROGRAM

All USNH employees, students, sponsored users, and emeritus shall participate in the USNH Phishing Awareness Program. This program provides USNH community members with a realistic phishing experience in a safe and controlled environment. This type of awareness training provides the USNH community with the opportunity to become familiar with and more resilient to the kinds of tactics used in real phishing attacks.

Each USNH community member shall be provided with regular simulated phishing training opportunities during each academic year. Community members who are unable to identify phishing simulations as phishing, and either click a link or open an attachment shall be considered susceptible to phishing. Susceptible community members shall be presented with just-in-time training as part of the simulation experience.

Community members who are susceptible to multiple simulations shall be required to complete online Phishing Awareness training within 15 days of proving susceptible.

Cybersecurity GRC is responsible for administration, monitoring, and management of the USNH Phishing Awareness Program.

University System of New Hampshire

CYBERSECURITY TRAINING RECORDKEEPING

In cooperation with other authorities responsible for administering elements of this program, USNH Cybersecurity GRC shall maintain comprehensive training records indicating which employees and students have completed each individual cybersecurity training requirements for a minimum of two years to ensure a full accounting of annual training is always available.

5 MAINTENANCE OF PROCESSES AND PROCEDURES RELATED TO THIS STANDARD

As part of the mandatory annual review of this Standard required by the *USNH Cybersecurity Policy*, the processes and procedures that support the requirements defined in this Standard will be reviewed, and where needed, updated to ensure currency and continuous improvement.

6 ENFORCEMENT

Failure to comply with this Policy puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures will be appropriate for the individual responsible for non-compliance (e.g., students, faculty, staff, vendors) as outlined in the relevant institutional regulations for that individual (e.g., student conduct and/or applicable personnel policies).

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.

Employees who are members of institutionally recognized bargaining units are covered by the disciplinary provisions set forth in the agreement for their bargaining units.

7 EXCEPTIONS

Requests for exceptions to this Standard shall be submitted and approved according to the requirements provided in the *Cybersecurity Exception Standard*.

8 ROLES AND RESPONSIBILITIES

Administrative, Academic, and Business Unit Managers:

- Ensure employees are fulfilling their cybersecurity training responsibilities
- Notify Cybersecurity GRC when new employees begin in roles that have cybersecurity role-based training requirements

- Provide a current list of employees in those roles, annually, to facilitate completion of training requirements

Chief Information Security Officer (CISO):

- Oversee and set direction for Cybersecurity Awareness and Training Program
- Identify and define advanced cybersecurity training needs
- Determine when out of band training needs to be provided to address significant changes in regulation, legislation, industry standards, or USNH policy

Cybersecurity Governance, Risk, & Compliance (GRC):

- Develop, administer, and manage all aspects of the Cybersecurity Awareness and Training Program including:
  - Awareness activities
  - New Hire Employee Training
  - Employee Training
  - GLBA Training
  - Student Training
  - Advanced Cybersecurity Training
  - Cybersecurity Incident Response Training
  - USNH Phishing Awareness Program
- Maintain comprehensive cybersecurity training records for USNH community members

HIPAA Privacy Officer(s):

- Develop, implement, and maintain the HIPAA Training Program
- Monitor compliance with the HIPAA Training Program

PCI Leaders:

- Develop, implement, and maintain the PCI-DSS Training Program
- Monitor compliance with the PCI-DSS Training Program

USNH Community Members:

- Complete all cybersecurity training requirements
- Participate in USNH Phishing Awareness Program

9 DEFINITIONS

See the ET&S Policy & Standard Glossary for full definitions of each term.

- Availability

University System of New Hampshire

- Computer-Based Training
- Confidentiality
- Cybersecurity
- Exception
- Gramm Leach Bliley Act (GLBA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Information
- Information Security
- Information Technology Resource
- Institutional Information
- Integrity
- Out of Band
- PCI-DSS
- Phishing
- Policy
- Standard
- Susceptible
- USNH Community Member
- Waiver

10 Related Policies and Standards

- USNH Cybersecurity Policy
- Cybersecurity Exception Standard

CONTACT INFORMATION

For USNH community members: Questions about this Standard, requests for additional information or training, or reports of violations can be directed to Cybersecurity Governance, Risk, and Compliance (GRC) via this Support Form.

All other requests can be submitted here: Submit an IT Question.

DOCUMENT HISTORY

Effective Date:	01 MAY 2021
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 27 JAN 2021 v1

University System of New Hampshire

	CYBERSECURITY POLICY & STANDARD WORKING GROUP, 27 AUG 2020 V0.2
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, JAN 2021 v0.2 CYBERSECURITY POLICY & STANDARD WORKING GROUP, AUG 2020
Revision History:	REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 09 MAR 2020