University System of New Hampshire

Incident Response Standard for Cybersecurity

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity & Networking
Approved Distribution: Designated Reviewers Only
Status: In-Force

1 PURPOSE

This standard outlines the procedures and responsibilities for responding to cybersecurity incidents within the university to protect the confidentiality, integrity, and availability of university information assets, minimize damage, and maintain the trust of the university community.

2 SCOPE

This standard applies to all university departments, units, employees, contractors, and third-party service providers who handle university data and information systems.

3 AUDIENCE

All USNH community members who access USNH information technology resources should be familiar with this Standard.

4 STANDARD

4.1 Incident Identification:

- Reporting:
  - All personnel who suspect or discover a cybersecurity incident must immediately report it to the designated incident response team or contact.
  - If contact is unknown, please reach out to: USNH Helpdesk at (603) 862-4242 or at https://www.usnh.edu/it/about/cybersecurity/cybersecurity-incident-reporting

- Classification:
    - Incidents should be classified based on severity and potential impact to determine the appropriate response level.

4.2 Incident Response Process:

- Incident Response Team:
    - The university will maintain a dedicated incident response team responsible for coordinating and executing the incident response plan.
- Assessment:
    - Upon notification, the incident response team will assess the incident's scope, impact, and potential risks.
- Containment and Mitigation:
    - Take immediate steps to contain and mitigate the incident to prevent further damage or data loss.
- Eradication:
    - Identify the root cause and eliminate the source of the incident.
- Recovery:
    - Implement recovery plans and restore affected systems and services to normal operation.
- Communication:
    - Maintain clear and timely communication with all relevant stakeholders, including affected parties, university leadership, legal counsel, and law enforcement, as necessary.
- Documentation:
    - Maintain detailed records of the incident, including actions taken, evidence collected, and communications.
- Legal and Regulatory Compliance:
    - Comply with all applicable laws and regulations concerning cybersecurity incidents.
    - Notify affected parties and regulatory authorities, if required by law.
- Notification:
    - Notify affected individuals if their personal information is compromised in accordance with applicable data breach notification laws.
- Lessons Learned:
    - Conduct a post-incident analysis to identify weaknesses in the incident response process and make necessary improvements.

University System of New Hampshire

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 shall be reviewed and, where needed, updated to ensure currency and continuous improvement.

- The Chief Information Security Officer (CISO) or designated cybersecurity officer is responsible for coordinating and leading the incident response efforts.
- All university personnel must cooperate with the incident response team and follow established procedures.
- The university will provide training and awareness programs to educate employees and contractors on their responsibilities in the event of a cybersecurity incident.

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.

University System of New Hampshire

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:	October 19, 2023
Approved by:	Thomas Nudd, CISO
Reviewed by:	Dr David A Yasenchock, Director, Cybersecurity GRC
Revision History:	V 1.0