University System of New Hampshire

CYBERSECURITY RISK ACCEPTANCE STANDARD

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

1 PURPOSE

The goal of the University System of New Hampshire's (USNH) Cybersecurity Risk Management Program is to ensure that cybersecurity risk across the University System and its component institutions is managed effectively in order to prevent adverse events from impacting the confidentiality, integrity, and availability of institutional information and information technology resources. While mitigation of risk should be considered for all cybersecurity risk, there are times when the optimal strategy for managing a risk is Risk Acceptance.

This Standard defines the process and requirements for Cybersecurity Risk Acceptance at USNH and its component institutions.

2 SCOPE

This Standard applies to all cybersecurity risks.

3 AUDIENCE

All USNH employees should be aware of and understand the concepts in this Standard. However, it is primarily applicable to:

- Administrative, academic, and business unit leadership, who are required to participate in the Cybersecurity Risk Management Program
- Business Application Owners/ Technology Service Owners

4 STANDARD

When a cybersecurity risk is identified that cannot or will not be mitigated, avoided, or transferred, the

risk shall be accepted by the appropriate member of administrative, academic, or business unit leadership. Acceptance of risk is an acknowledgement that a risk and its potential to cause losses to USNH and/or its component institutions is understood and, with that understanding, affirmatively choosing not to mitigate, transfer, or avoid it, even if the probable frequency and/or probable magnitude of loss falls outside USNH's risk tolerance or appetite. When risk is accepted, responsibility for possible losses resulting from accepting the risk belongs to the administrative, academic, or business unit accepting it.

This means that the administrative, academic, or business unit accepting the risk shall be responsible for direct and indirect costs incurred due to any cybersecurity incidents that the Chief Information Security Officer (CISO) determines are the result of accepting the risk.

Based on the level of non-mitigation and the severity of potential loss, additional sign off by different levels of senior management may be required. Risk Acceptance, even when approved by senior leadership of an administrative, academic, or business unit shall be subject to revocation by the Chief Information Officer (CIO) or the CISO at any time and may be subject to Internal Audit's annual follow-up procedures.

Risk acceptance shall be documented using the *Cybersecurity Risk Acceptance Form*, which Cybersecurity Governance, Risk, & Compliance (GRC) completes, with the assistance of the unit responsible for accepting the risk.

Acceptance of cybersecurity risk requires, at a minimum, the signature approval of the CISO and the leadership of the relevant administrative, academic, or business unit. Only senior leadership can accept risk on behalf of the University System or one of its component institutions.

At the discretion of the CISO or the CIO, additional levels of approval may be required in circumstances where the severity of the potential adverse impact requires visibility and acceptance of USNH or institutional executive leadership.

If the risk includes any institutional information with regulatory compliance obligations, the appropriate University System or institutional compliance authority shall also provide a signature approval.

Accepted risks shall be reviewed annually and if appropriate, the acceptance of that risk shall be renewed for another year.

Cybersecurity Governance, Risk, & Compliance (GRC) shall administer the Cybersecurity Risk Acceptance Process and is responsible for maintaining the pertinent records related to risk acceptance.

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.

6 ENFORCEMENT

Failure to comply with this Standard puts the University System, its component institutions, and its information and information technology resources at risk and may result in disciplinary action. Disciplinary procedures shall 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 Rights, Rules, and Responsibilities).

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

The requirement for risk acceptance cannot be excepted.

8 ROLES AND RESPONSIBILITIES

Administrative, Academic, and Business Unit Leadership:

- Review and approve Cybersecurity Risk Acceptance requests for their area
- Ensure any agreed or required compensating controls are implemented and managed as outlined

Business Application Owners:

- Identify, in collaboration with Cybersecurity Governance, Risk, & Compliance (GRC), cybersecurity risks that require Risk Acceptance
- Provide information needed to complete Risk Acceptance Form
- Implement any agreed or required compensating controls

Chief Information Officer (CIO):

- Review and approve/reject requests for Risk Acceptance
- Confirm areas where the risk requires additional levels of USNH or component institution approval and acceptance

Chief Information Security Officer (CISO):

- Oversee the Cybersecurity Risk Acceptance Process
- Review and approve/reject requests for Risk Acceptance
- Sign approved Risk Acceptance Forms
- Identify areas where the risk requires additional levels of USNH or component institution approval and acceptance and make recommendations to this effect to the CIO

Cybersecurity Governance, Risk, & Compliance (GRC):

- Identify cybersecurity risks that require risk acceptance
- Facilitate the Cybersecurity Risk Acceptance Process
- Collect, store, and track all cybersecurity risk acceptance documentation

Technology Service Owners:

- Identify, in collaboration with Cybersecurity Governance, Risk, & Compliance (GRC), cybersecurity risks that require Risk Acceptance
- Provide information needed to complete Risk Acceptance Form
- Implement any agreed or required compensating controls

University System and Institutional Leadership:

- Review and acknowledge cybersecurity risk acceptance for their area of responsibility
- Review and approve/reject risk acceptance, when required

9 DEFINITIONS

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

- Availability
- Business Application Owner
- Compensating Control
- Confidentiality
- Information
- Cybersecurity Incident
- Information Technology Resource
- Institutional Information
- Integrity
- Mitigate
- Risk
- Risk Acceptance

University System of New Hampshire

- Risk Management
- Risk Tolerance
- Technology Service Owner

10 Related Policies and Standards

- USNH Cybersecurity Policy
- Cybersecurity Exception Standard
- Cybersecurity Risk Management 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, & Compliance (GRC) via this Support Form.

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

DOCUMENT HISTORY

Effective Date:	15 FEB 2021
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 02 SEP 2020, V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, 13 AUG 2020, V0.1
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, AUG/SEP 2020, V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, 13 AUG 2020, V0.1
Revision History:	REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 08 MAR 2020, V0.1