University System of New Hampshire

CYBERSECURITY EXCEPTION STANDARD

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

1 PURPOSE

The University System of New Hampshire (USNH) is committed to safeguarding the information and information technology resources used to support the overall mission of the University System and its component institutions. The requirements in this Standard help the University System manage risks to the system, institutions, and all who study and work here.

The University System recognizes that there are instances and circumstances where business needs, academic activities, and/or research project requirements cannot adhere to the established cybersecurity Policies and Standards. The intent of this Standard is to provide a mechanism for the proactive identification of business processes, procedures, and technology use that do not meet the established cybersecurity requirements. It empowers members of the community to request assistance in managing the risk(s) associated with non-compliance.

Some examples of exceptions are:

- Use of software that requires a device running on old operating system
- Processes involving community members or administrators sharing accounts
- Servers or other information technology resources with vulnerabilities that cannot be fixed because of extenuating circumstances
- Business processes that cannot meet requirements because of resource constraints

2 SCOPE

This Standard applies to any exception related to a USNH or institution-specific Technology or Cybersecurity Policy or Standard.

3 AUDIENCE

All USNH community members, including faculty, staff, and students, who access, capture, store, process, transmit, or otherwise manage USNH information or information technology resources shall be familiar with this Standard and understand how the requirements outlined here affect them.

4 STANDARD

REQUESTING AN EXCEPTION

Any USNH community member who identifies a circumstance where the requirements established in a USNH Cybersecurity Policy or Standard cannot be complied with, may request an exception to that Policy and/or Standard, in part or in full.

Exceptions are temporary exemptions from Policy or Standard compliance.

Requests for exceptions shall include the following information:

- Specific reference to the Policy or Standard for which the exception is being requested
- List of the business units, business processes, information technology resources, and institutional information to which the exception applies
- Rationale providing justification for the exception being requested
- Specific information on the compensating controls that are already in place or to be implemented to mitigate the risks resulting from non-compliance.
- Timeframe requested
- Requestor's name, email address, and administrative, academic, or business unit
- Head of the requesting unit
- Describe why compliance is not possible (e.g. the total cost to comply with the Policy or Standard or the negative impact to USNH community members including an estimate of the number of community members that may be negatively impacted)

PROCESSING EXCEPTION REQUESTS

Cybersecurity & Networking (CS&N) is responsible for management of exception requests under this Standard. Working closely with the requester, CS&N shall document the exception, determine the risk associated with granting the exception, assess compensating controls, and make a recommendation as to whether the exception should be approved, not approved, or if the circumstance requires completion of the Cybersecurity Risk Acceptance process which is defined in the *Cybersecurity Risk Acceptance Standard*.

The exception review and assessment process shall include consideration of the following:

- Compensating controls currently in place and/or those planned to be implemented

- Extended timeframe required to achieve compliance
- Justification for non-compliance, within the required timeline or at all
- Security Categorization of the information, information technology resources, and/or critical business processes involved
- Impact on organizational mission
- Risk(s) presented or increased
- Technical obstacles to compliance
- Operational obstacles to compliance
- Any other environment-specific information provided in the request

Approval of Exception Requests

All exception requests shall be approved by administrative, academic, or business unit leadership and the Chief Information Security Officer (CISO) or Director, Cybersecurity Governance, Risk, and Compliance (GRC), at a minimum. In circumstances where Cybersecurity & Networking determines it is warranted, additional institution-specific or University System leadership approvals may be required.

Cybersecurity & Networking shall handle the approval process and communicate approval/denial decisions back to the original requester once all approval levels have reviewed and either approved or denied the exception.

Appealing Exception Decisions

Administrative, academic, and business unit leadership may appeal denial of an cybersecurity exception to the Chief Information Officer (CIO). All requests shall be made in writing and processed via the Cybersecurity GRC office.

Expiration of Approved Exception Requests

Cybersecurity & Networking (CS&N) shall track all approved exceptions and alert the requester or unit leadership when exceptions are within 30 days of expiration. The requesting unit shall be responsible for informing CS&N if the exception is no longer needed or if an extension needs to be requested. Failure to respond to CS&N notifications or inquiries prior to the exception's expiration date shall result in the exception expiring. If an exception is still needed after expiration, it shall be resubmitted as a new request.

Extension of Expiring Exception Requests

If an expiring exception needs to be extended beyond its original expiration date, the requesting unit shall notify Cybersecurity & Networking in advance of expiration and may be required to provide additional or updated information as part of the extension request process. Exception extension requests require the same approvals as the original exception.

Impact to In-Force Exceptions on Policy or Standard Change

If the Policy and/or Standard referenced in an in-force exception needs to be modified, Cybersecurity GRC shall review any applicable in-force exceptions to assess the impact of the modifications. If the Policy or Standard modifications require changes to any in-force exception, Cybersecurity GRC shall be responsible for guiding the requesting unit through whatever process is required in relation to the impacted exception.

Record Keeping for Exception Requests

Cybersecurity Governance, Risk, & Compliance (GRC) shall track and manage all cybersecurity exception requests through exception lifecycle. An audit trail documenting the request, approval/denial, rationale, and expiration (where appropriate) for each exception shall be maintained by GRC for a period of five years after expiration. Information about approved exceptions may be provided to authorized parties upon request.

Exception documentation shall be retained in a secure repository that can only be accessed by authorized personnel.

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 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 ROLES AND RESPONSIBILITIES

Administrative, Academic, and Business Unit Leadership:

- Review and approve/deny exception requests for administrative, academic, and business units

Chief Information Officer (CIO):

- Review and make final determination on any appeals submitted for denied cybersecurity exceptions

Chief Information Security Officer (CISO):

- Review and approve/deny all exception requests
- Oversee Cybersecurity Exception process

Cybersecurity Governance, Risk, & Compliance (GRC):

- Process requests for cybersecurity exceptions including intake, tracking requests, developing exception documentation, supporting requesters, and submitting to appropriate reviewers for approval/denial
- Notify requester of approval/denial
- Track approved exceptions and notify requesting unit prior to expiration
- Process requests for extensions to in-force exceptions
- Retain exception documentation
- Analyze the impact of modifications to Policies and Standards on existing exceptions and working with impacted USNH community members to address that impact

USNH Community Members:

- Identify circumstances where cybersecurity Policy and Standard exceptions are needed within their administrative, academic, or business units
- Provide requested information to complete the exception request process

8 DEFINITIONS

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

- Compensating Control
- Critical Business Process
- Exception
- Information
- Information Technology Resource
- Institutional Information
- Mitigate
- Policy
- Procedure
- Risk
- Risk Acceptance
- Security Categorization
- Standard

9 RELATED POLICIES AND STANDARDS

- USNH Cybersecurity Policy
- USNH Information Classification Policy
- USNH Password Policy

Additionally, except for the Cybersecurity Risk Management Standard, all cybersecurity Standards reference this 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:	15 FEB 2021
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 02 SEP 2020, V1

University System of New Hampshire

	CYBERSECURITY POLICY & STANDARD WORKING GROUP, 18 JUN 2020, V0.1
Reviewed by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, AUG/SEP 2020, V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, MAY/JUNE 2020. V0.1
Revision History:	DRAFTED, R BOYCE-WERNER, 22 JAN 2020, V0.1