University System of New Hampshire

CYBERSECURITY RISK MANAGEMENT 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. Management of cybersecurity risk is essential to honoring that commitment. As such, USNH uses a formal Cybersecurity Risk Management Program to shield USNH and its component institutions from probable adverse impacts to operational capability, financial strength, and reputation resulting from cybersecurity incidents.

A comprehensive assessment and understanding of cybersecurity risks is necessary to enable informed, practical decision making on security control implementation, risk mitigation prioritization, and cybersecurity investment.

The Cybersecurity Risk Management Program is part of the overall Cybersecurity Program and is an input into the USNH Enterprise Risk Management (ERM). This Standard outlines the components of this Program, defines responsibilities for USNH community members required to participate in the Program, and establishes requirements for the ongoing maintenance and improvement of the Program.

2 SCOPE

The Cybersecurity Risk Management Program applies to all USNH information technology resources and by extension, to any administrative, academic, or business unit responsible for managing those resources. Additionally, critical administrative, academic, and business unit processes (critical business processes), as defined in the Business Process Risk Designations section of this Standard, are also inscope for the Cybersecurity Risk Management Program and subject to the requirements outlined in this Standard.

University System of New Hampshire

3 AUDIENCE

USNH community members who are responsible for information technology resources or critical business processes, as well as the leadership of the administrative, academic, and business units those community members belong to, should understand this Standard and their compliance responsibilities.

4 STANDARD

Risk is the probable frequency and probable magnitude of future loss. Effective cybersecurity risk management means decreasing both the probable frequency and the probable magnitude of future cybersecurity incidents in order to decrease future losses. To do this, Cybersecurity Governance, Risk, & Compliance (GRC) shall develop and maintain a comprehensive Cybersecurity Risk Management Program under the leadership of the CISO.

CYBERSECURITY RISK MANAGEMENT PROGRAM OBJECTIVES

Effective management of cybersecurity risk is critical to supporting the achievement of the USNH mission and the strategic objectives of each of its component institutions. As an essential aspect of cybersecurity governance at USNH, this Program aims to:

- Develop a comprehensive picture of cybersecurity risk at USNH
- Enable decision making on security control implementation, risk mitigation prioritization, and cybersecurity investment
- Make conscious, documented decisions about cybersecurity risk treatment
- Expand awareness of cybersecurity risk across USNH and its component institutions

CYBERSECURITY RISK MANAGEMENT FRAMEWORK

The Cybersecurity Risk Management Program uses a Cybersecurity Risk Management Framework (CRMF) to provide structure and consistency of approach to the management of information security risk. The primary objectives of the CRMF are to:

- Define the methodology used to identify, assess, analyze, and manage USNH's cybersecurity risks
- Establish roles and responsibilities for cybersecurity risk management at USNH
- Ensure consistency in cybersecurity risk management across all USNH institutions and at all organizational levels

The CRMF is comprised of the following elements:

Cybersecurity Risk Management Standard (this document)

Defines the purpose, scope, audience, requirements, roles and responsibilities, and terminology for cybersecurity risk management at USNH.

Cybersecurity Risk Management Strategy

This strategy, which is described in greater detail below, provides guidance on how cybersecurity risk management is handled at USNH. The strategy defines core concepts and informs the different processes used within the Program (e.g., Risk Assessment, Risk Analysis).

Cybersecurity Risk Tolerance Statement

Defines USNH's tolerance for cybersecurity risk and guides the selection of risk treatment options in alignment with the University System's overall risk tolerance. This statement informs the Risk Management Strategy and drives the structure of the *Cybersecurity Risk Heat Map* used in the Risk Analysis process.

Cybersecurity Risk Assessment Process

This process, which is described in greater detail below, outlines a series of sequential activities used to identify, assess, respond to, and monitor cybersecurity risk. Additionally, it defines the different organizational contexts used to ensure development of a comprehensive picture of cybersecurity risk across USNH. This process is the heart of the Program and is used to identify the risk issues and scenarios that need to be analyzed.

Cybersecurity Risk Assessment Procedures

Documented procedures for performing risk assessments at the organizational/strategic, business process, administrative, academic, or business unit, and information technology resource levels. These procedures support the Risk Assessment Process.

Cybersecurity Risk Analysis Tool

Analysis of cybersecurity risk issues identified during the Risk Assessment Process is conducted using tools that conform with the FAIR™ taxonomy and analytics model. These tools are used to perform a quantitative analysis for each Risk Scenario identified during the Risk Assessment process. The results of this analysis determine which risks require risk treatment and are documented in the Risk Assessment Report.

Cybersecurity Risk Acceptance Standard:

University System of New Hampshire

This Standard defines the requirements for acceptance of cybersecurity risk at USNH. Risk Acceptance is one of the risk treatment options that may be selected at the end of the Risk Analysis.

Cybersecurity Risk Assessment Report:

This Report reflects the results of an individual risk assessment conducted for specific information technology resources, critical business processes, or organizational/strategic concerns. This report captures the assets included in the assessment, the threat events considered, the risk issues identified, the analysis of specific risk scenarios related to those issues, and the resulting rated cybersecurity risks.

This report also includes an assessment specific Risk Action Plan that identifies the recommended risk treatment for each identified risk. The information in this section of the report is used to build out the Cybersecurity Risk Register.

Cybersecurity Risk Register:

This is a centrally managed record of all risks identified through individual risk assessments, internal audit observations, approved exceptions/waivers/risk acceptances, and cybersecurity incident response debriefs. The register, which may be comprised of several different levels organized to meet specific risk management needs, is used to:

- Inform cybersecurity and information technology leadership
- Track and monitor risk treatment activities
- Identify gaps in cybersecurity control implementation

Cybersecurity Risk Management Program Maintenance:

Defines requirements for ensuring the Cybersecurity Program is maintained and continuously improved. Provided in this document.

CYBERSECURITY RISK MANAGEMENT STRATEGY

Assumptions

- Risks with the potential to impact life and safety, financial strength, and institutional reputation have been given the highest priority and, when limitations exist in regards to available resources and funding for performing risk assessments or applying risk mitigation, priority shall be given to assessments and /or risks that are more likely to impact these areas
- While the goal should be to mitigate risk wherever possible, thoughtful consideration shall be given to the costs associated with mitigation activities, including both the hard dollar costs and

the potential to negatively impact operations (technical, operational, academic). Effective risk management may require finding the appropriate balance

- Information used in the Risk Assessment Process, including definitions of threats, threat communities, risk scenarios, and the methodology for analyzing cybersecurity risk, shall be defined by Cybersecurity GRC with oversight and approval by the CISO

Constraints

- Without a clear risk appetite or risk tolerance statement from USNH Enterprise Risk Management (ERM), risk appetite/tolerance for cybersecurity specific risks shall be determined by the Chief Information Officer (CIO) and CISO and documented in the Cybersecurity Risk Tolerance Statement
- Resources within Cybersecurity GRC available to perform or assist with risk assessments, monitor risks, and perform other critical cybersecurity risk management activities are limited and the pace at which this program can be developed, expanded, and managed shall be determined by the amount of resources allocated to it

Prioritization of Risk Management Resources and Activities

- Risks involving information that is classified as PROTECTED, RESTRICTED, or CONFIDENTIAL and information technology resources used to capture, store, process, transmit, or otherwise manage information with those classifications, and information technology resources used to process financial transactions shall be given the highest priority from a risk assessment prioritization perspective

Business Process Risk Designations

Business processes performed by any administrative, academic, and business unit that involve information that is classified as RESTRICTED or CONFIDENTIAL or that handle financial transactions shall be designated as “critical business processes” and those units shall be required to comply with the requirements defined in this Standard.

Other business processes performed by administrative, academic, and business units may be designated as “critical business processes” at the discretion of the CISO. In the event that a business process that does not meet the definition above is designated as critical by the CISO, the leadership of the business unit responsible for that process will be notified by Cybersecurity GRC.

A list of critical business processes is maintained by Cybersecurity GRC.

University System of New Hampshire

Cybersecurity Risk Analysis

Enterprise Technology & Services (ET&S) uses the FAIR™ ontology and analytics model for cybersecurity risk analysis. This approach provides a consistent, comprehensive, quantitative methodology for analyzing risk across the University System. Based on the results of the analysis, each identified risk is rated using the Cybersecurity Heat Map, which determines the overall criticality of that risk according to the following scale:

Impact	Likelihood				
	Rare	Unlikely	Possible	Likely	Almost Certain
Catastrophic	Moderate	Moderate	High	Very High	Very High
Major	Low	Moderate	Moderate	High	Very High
Moderate	Low	Moderate	Moderate	Moderate	High
Minor	Very Low	Low	Moderate	Moderate	Moderate
Insignificant	Very Low	Very Low	Low	Low	Moderate

Risks are rated based on where their probable loss frequency and probable loss magnitude fall when plotted on the *Cybersecurity Risk Heat Map*, which aligns with the *Cybersecurity Risk Tolerance Statement*. The current Heat Map is available from Cybersecurity GRC and is included in each *Cybersecurity Risk Assessment Report*.

Security Categorization

Security Categorization is a risk management tool used across the Cybersecurity Program to consistently express the potential impacts of an adverse event on the confidentiality, integrity, and availability of USNH information and information technology resources. This categorization is specific to the asset it is assigned to and does not change based on different threat conditions or risk mitigations. It is used in the Cybersecurity Risk Assessment process, and in other aspects of the Cybersecurity Program, to facilitate risk-based decision making.

All Information technology resources, and critical business processes shall be assigned a security categorization based on the methodology outlined in the *Security Categorization Standard*.

University System of New Hampshire

CYBERSECURITY RISK ASSESSMENT PROCESS

All Cybersecurity Risk Assessments shall follow the basic structure outlined below:

- Define the scope of the Risk Assessment (e.g., which information technology resources or business processes does it include)
- Identify in-scope assets (e.g., people, processes, information, information technology resources) with the potential to be impacted by a cybersecurity threat event
  Identify specific threat events with the potential to adversely impact the identified assets
- Identify risk issues that need to be analyzed to define specific cybersecurity risks
- Rate identified risks to determine which risks require action and to guide risk treatment selection
- Select appropriate risk treatment option for each risk
- Identify a Risk Action Plan for each identified risk requiring one
- Document results in a Risk Assessment Report which includes a Risk Action Plan

Cybersecurity GRC shall develop and maintain specific processes, procedures, and deliverables, which may include tools, forms, and templates, for conducting risk assessments at each of the three Tiers described below.

Cybersecurity GRC shall notify stakeholders when risk assessments need to be completed, facilitate the completion of all required risk assessments, and track completion of all required risk assessments.

Cybersecurity GRC shall retain a copy of all current Risk Assessment Reports and an archive of prior Risk Assessment Reports for one year after the new risk assessment is completed.

RISK ASSESSMENT TIERS

In order to provide a comprehensive understanding of Cybersecurity Risk across USNH and its component institutions, risk shall be assessed using the three-tier model recommended by the National Institute of Standards and Technology (NIST).

Tier 1 – Organization, Institution, and System

Risk in this tier is associated with strategic, systemic, or operational concerns and is primarily identified using the consolidated results of multiple individual risk assessments from Tiers 2 and 3 or from threat and/or vulnerability information.

Example of a Tier 1 risk: IT Disaster Recovery Plan developed without input from administrative, academic, or business units results in failure to recover mission critical information technology resources quickly enough to avoid negatively impacting critical business operations after an ice storm takes out power to the UNH Data Center for 5 days.

Tier 1 risk assessments involve Cybersecurity GRC, the CISO, and the CIO and may also include senior administrative, academic, or business unit leadership from across all USNH institutions. Risks identified and assessed in Tier 1 are used to drive USNH-wide cybersecurity strategy, policy, and investment.

Tier 1 risks shall be reviewed bi-annually in accordance with the USNH Enterprise Risk Management (ERM) process. Additional reviews may be required, at the discretion of the CIO or the CISO, in the wake of significant strategic, systemic, or operational changes.
(NIST, 2011)

Tier 2 – Critical Business Processes and Administrative, Academic, and Business Units

Risk in this tier is associated with administrative, academic, or business unit processes and procedures. As information and information technology resources are utilized in every administrative, academic, and business unit across USNH, there may be a need to assess cybersecurity risk in any administrative, academic, or business unit, across units, and across institutions. Examples:

- Business processes used to handle financial aid applications and administer awards at all USNH institutions
- Information handling procedures within academic units used for advising, student engagement, etc.
- Financial transaction processes and procedures within a unit
- The Change Management Program used to manage changes to information technology resources

The *USNH Cybersecurity Policy* establishes the requirement that all USNH and component institution administrative, academic, and business units participate in the Cybersecurity Risk Management Program and conduct Cybersecurity Risk Assessments as requested. Cybersecurity GRC, working with the individual administrative, academic, and business units, shall develop a Tier 2 risk assessment schedule that outlines when initial risk assessments shall be conducted for each individual unit, at each institution. Scheduling shall be prioritized based on risk assumptions and critical business process risk assessments shall be scheduled first.

Once a Tier 2 risk assessment has been conducted for a critical business process or an administrative, academic, or business unit, Cybersecurity GRC shall recommend, based on the results of that assessment, the appropriate risk assessment cycle for that process or unit. Cybersecurity GRC may also recommend to the CISO that a business process be designated as a critical business process or that the critical business process designation be removed, based on the risk assessment results.

Tier 2 risk assessments shall be conducted in 1 year, 2 year, and 3 year cycles, based on the degree of risk identified during the initial assessment.

Units who have completed an initial risk assessment shall be required to participate in a subsequent risk assessment in the following circumstances:

- When business processes are redesigned or revamped to the extent that training, documentation, or communication is required to inform those who perform the business process
- When there is a change to an information technology resource used to complete the business process
- When changes are made to regulations or legal requirements that impact the institutional information or business processes used by the unit If requested by the CISO
- As required by the assigned risk assessment cycle – annually, bi-annually, or every three years

All completed Tier 2 Cybersecurity Risk Assessment Reports shall be signed off by Unit Leadership and the CISO. Risks identified and assessed in Tier 2 shall be added to the Cybersecurity Risk Register and may be used to inform risk activities in Tier 1 and to identify areas where additional Tier 3 risk assessments shall be conducted.

Administrative, academic, and business unit leadership shall ensure the Risk Action Plans resulting from Risk Assessments are implemented in their areas of influence and that the status of those Plans is communicated to Cybersecurity GRC regularly and as requested.

Tier 3 – Information Technology Resources and Capabilities

Risk in this tier is associated directly with an information technology resource or group of resources representing a capability. Examples:

- An Information System like Banner HR/Fin which includes the underlying infrastructure used to create the system like servers and databases and the software and applications that sits on that infrastructure (Banner 8, Banner 9, WISE, SSO Manager, Xtender, etc)
- An Information Technology Capability like the USNH Network which includes all the individual information technology resources like switches and routers needed to provide the capability as well as any infrastructure like servers and databases, and applications or software, that are used to manage and administer that capability
- An individual information technology resource like Salesforce, which is a cloud-application provided by a vendor

In conjunction with the ET&S Leadership team lead by the CIO, the CISO shall identify all specific information technology resources and capabilities requiring a risk assessment.

Tier 3 Risk Assessments shall be facilitated by Cybersecurity GRC with the participation and input of the Business Application Owner and/or Technology Service Owner(s) responsible for the information technology resource or capability and those who support it.

Cybersecurity GRC, working with Business Application Owner and/or Technology Service Owner(s), shall develop a Tier 3 risk assessment schedule that outlines when initial risk assessments shall be conducted for each information technology resource or capability. Scheduling shall be prioritized based on risk

assumptions and risk assessments for information technology resources shall be scheduled according to the security categorization of that resource, beginning with those categorized as HIGH.

Tier 3 risk assessments shall be conducted in 1 year, 2 year, and 3 year cycles, based on the amount of cybersecurity risk identified for the information technology resource or capability during the initial risk assessment. Initial risk assessment results may also be used to recommend a change to the security categorization of the information technology resource or capability.

Information technology resources or capabilities for which an initial risk assessment has been completed shall require a subsequent risk assessment in the following circumstances:

- When the information technology resource or capability is modified, upgraded, or redesigned to the extent that training, documentation, or communication to the USNH community is required
- When changes are made to regulations or legal requirements that impact the institutional information captured, stored, processed, transmitted, or otherwise managed by that resource
- If requested by the CISO
- As required by the assigned risk assessment cycle – annually, biannually, or every three years

All completed Tier 3 Cybersecurity Risk Assessments shall be signed off by the Technology Service Owner, the appropriate ET&S Leadership, and the CISO. Risks identified and assessed in Tier 3 may be used to inform risk activities in Tier 1 and Tier 2.

(NIST, 2011)

Selection and Documentation of Risk Treatment

Once risks have been identified and analyzed as part of the Risk Assessment Process, Cybersecurity GRC shall assist Business Application Owner and/or Technology Service Owner(s) and Unit Leadership in selecting a risk treatment option for each risk. There are four treatment options available for handling cybersecurity risks at USNH:

Risk Mitigation

Risk mitigation involves making changes to things like business processes, information technology resources, or security controls to reduce the overall risk, reduce the probable frequency that the risk will cause a loss, and/or reduce the probable magnitude of that loss. Examples of risk mitigation are:

- Upgrading a computer from Windows 7, which is no longer supported, to Windows 10, which is supported, in order to make it harder for unauthorized parties to gain access to it
- Adding a peer-review step to a business process to decrease the likelihood that confidential information is provided to the wrong person

Risk Avoidance

Risk avoidance involves eliminating something, like an information technology resource or part of a business process, in order to stop that particular risk from arising. Examples of risk avoidance are:

- Replacing a scientific instrument that requires the use of Windows XP, an unsupported operating system, with a new piece of instrumentation that can utilize a modern operating system Consolidating the steps in a business process to remove the need to have student workers access information classified as CONFIDENTIAL

Risk Transference

Risk transference involves engaging with some other entity, like a vendor or an insurance provider, to share the probable magnitude the risk. Examples of risk transference are:

- Purchasing a cybersecurity insurance policy to protect against the potential financial impacts of a cybersecurity incident
- Putting contractual protections in place to ensure a vendor who will be storing institutional information will be required to pay all or part of costs associated with any adverse financial impact of trusting them with that information

Risk Acceptance

Risk acceptance involves understanding a risk and its potential to cause losses and affirmatively choosing to acknowledge that risk and not to mitigate, transfer, or avoid it, even if the probable frequency and/or probable magnitude of loss falls outside ET&S's risk tolerance or appetite. Accepting risk on behalf of USNH or one of its component institutions can only be done by senior leadership of an administrative, academic, or business unit as outlined in the *Cybersecurity Risk Acceptance Standard*. Examples of risk acceptance are:

- Allowing a scientific instrument running an unsupported operating system to connect to the network
- Allowing an administrative unit to receive RESTRICTED information via email because the cost to mitigate, transfer, or avoid that risk is more than the potential loss to USNH if an cybersecurity incident occurred because of this practice
- Choosing not to incur the cost of developing and maintaining a "hot" disaster recovery site even though the potential impact could be catastrophic because the probability of a natural disaster occurring does not warrant the expense

Recording of Risk Treatment Options

A risk treatment option shall be selected for each risk and documented in the Risk Action Plan section of the *Cybersecurity Risk Assessment Report*. This information feeds into the *Cybersecurity Risk Register* which is used for monitoring the implementation of risk treatments, action plans, and other risk management activities.

RISK REGISTER AND RISK MONITORING

Cybersecurity GRC shall maintain an Cybersecurity Risk Register that encompasses all cybersecurity risks identified during Tier 1,2, or 3 risk assessments, as part of the Cybersecurity Exception and Risk Acceptance processes, along with those risks identified during internal assessments conducted by USNH Internal Audit and external assessments like pen-testing engagements.

The Cybersecurity Risk Register shall be the primary tool used to monitor Cybersecurity Risk. Frequency of monitoring activities shall be based on the severity of the risk as established in the Risk Assessment Process and the security categorization of the information technology resource or business process most closely tied to the risk. At a minimum, all risks on the Cybersecurity Risk Register shall be reviewed every six months.

CYBERSECURITY RISK MANAGEMENT PROGRAM MAINTENANCE

The CISO shall ensure all aspects of the Cybersecurity Risk Management Program are reviewed and updated by Cybersecurity GRC annually, or as needed to address continuous improvement opportunities, organizational changes, or other factors.

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 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

Risk Assessment requirements defined in this Standard cannot be exempted via the Cybersecurity Exception process.

8 ROLES AND RESPONSIBILITIES

Administrative, Academic, and Business Unit Leadership:

- Participate in the Cybersecurity Risk Management program, including identification of assets and services, allocation of resources, risk prioritization, risk acceptance, and development of risk treatment plans
- Collaborate with Cybersecurity GRC to:
  - Complete the Cybersecurity Risk Assessment Process as assigned
  - Develop Risk Action Plans for identified risks
- Sign-off on Risk Assessment Reports for their unit(s) including those for critical business processes within their units
- Ensure Risk Action Plans for their unit(s) are implemented
- Report updates on Risk Action Plans to Cybersecurity GRC

Business Application Owners:

- Participate in the Cybersecurity Risk Management program, including identification of assets and services, risk identification and assessment, risk prioritization, risk acceptance, and development of risk treatment plans
- Sign-off on Risk Assessment Reports for their applications
- Implement Risk Action Plans for their business applications
- Report updates on Risk Action Plans to Cybersecurity GRC

Chief Information Officer (CIO):

- Develop, in collaboration with the CISO, the ET&S Cybersecurity Risk Tolerance Statement
- Participate in Tier 1 Risk Assessment activities, as needed

Chief Information Security Officer (CISO):

- Manage the Cybersecurity Risk Management Program and coordinate the development and maintenance of all supporting materials needed to run the program
- Oversee all operational activities associated with the Cybersecurity Risk Management Program
- Develop, in collaboration with the CIO, the ET&S Cybersecurity Risk Tolerance Statement
- Identify administrative, academic, and business processes that need to be designated as critical business processes
- Identify, with the assistance of Enterprise IT Leadership, all information technology resources and capabilities to ensure comprehensive participation in the Cybersecurity Risk Management Program
- Review and approve Cybersecurity Risk Model
- Conduct initial and subsequent Tier 1 Risk Assessments
- Identify the need for out of band Tier 1 Risk Assessments based on significant strategic, systemic, or operational changes
- Sign-off on completed Risk Assessment Reports
- Ensure all aspects of the Cybersecurity Risk Management Program are reviewed and updated annually

Enterprise Technology & Services Leadership:

- Assist the CISO in identifying all information technology resources and capabilities that require completion of a risk assessment
- Participate in the Cybersecurity Risk Management program, as needed, including identification of assets and services, allocation of resources, risk prioritization, risk acceptance, and development of risk treatment plans
- Sign-off on Risk Assessment Reports for information technology resources and units under their purview
- Ensure Risk Action Plans for information technology resources and units under their purview are implemented
- Report updates on Risk Action Plans to Cybersecurity GRC

Cybersecurity Governance, Risk, and Compliance (GRC):

- Develop and administer the Cybersecurity Risk Management Program
- Develop and maintain all supporting materials needed to run the Program

- Establish the procedures for performing Risk Analysis
- Develop and maintain specific processes, procedures, and deliverables, which may include tools, forms, and templates, for conducting risk assessments at each of the three Tiers
- Participate in Tier 1 Risk Assessments
- Develop schedules for the completion of initial Tier 2 and 3 risk assessments
- Notify stakeholders when risk assessments need to be completed
- Coordinate, facilitate, and oversee the completion of Cybersecurity Risk Assessments
- Assist Service Owners and Unit Leadership in selecting risk treatment options and in the creation of Risk Action Plans
- Recommend addition or removal of critical business process designation to the CISO
- Recommend risk assessment cycles for each required Tier 2 and Tier 3 risk assessment
- Track completion of all required risk assessments
- Monitor progress on completion of Risk Action Plans
- Maintain the Cybersecurity Risk Register
- Maintain a central repository of all Cybersecurity Risk Management Program documentation
- Identify and recommend continuous improvement opportunities for all aspects of the Cybersecurity Risk Management Program
- Review and update all aspects of the Cybersecurity Risk Management Program annually

Technology Service Owners:

- Participate in the Cybersecurity Risk Management program, including identification of assets and services, risk identification and assessment, risk prioritization, risk acceptance, and development of risk treatment plans
- Sign-off on Risk Assessment Reports for their information technology resources
- Implement Risk Action Plans for their information technology resources or capabilities
- Report updates on Risk Action Plans to Cybersecurity GRC

USNH Community Members:

- Participate in risk assessments, as needed, to provide subject matter expertise

9 DEFINITIONS

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

- Asset
- Availability
- Business Application Owner

- CONFIDENTIAL Information
- Confidentiality
- Critical Business Process
- Exception
- FAIR™
- Information
- Information Security Incident
- Information Technology Resource
- Institutional Information
- Integrity
- Mitigate
- Out of Band
- PROTECTED Information
- RESTRICTED Information
- Risk
- Risk Acceptance
- Risk Assessment
- Risk Tolerance
- Security Categorization
- Security Control
- Technology Service Owner
- Threat
- USNH Community Member
- Vulnerability

10 RELATED POLICIES AND STANDARDS

- USNH Information Classification Policy
- USNH Cybersecurity Policy
- Cybersecurity Risk Acceptance Standard
- Security Categorization Standard

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:	15 SEPT 2022
Approved by:	CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, 27 JAN 2021 V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, 15 SEPT 2022
Reviewed by:	DR David A Yasenchock, Cybersecurity GRC, SEPT 2022 V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, SEPT 2022
Revision History:	REVIEW DRAFT FINALIZED, DR David A Yasenchock, 15 SEPT 2022