THIRD-PARTY INFORMATION SECURITY MANAGEMENT STANDARD

Responsible Executive/University System Officer: Chief Information Security Officer
Responsible Office: Cybersecurity GRC
Approved Distribution: Public
Status: IN FORCE

1 PURPOSE

This standard outlines requirements for securing third-party services and products to manage, transmit or store sensitive or restricted information to support the University System of New Hampshire (USNH) administrative, academic, and business unit needs.

To gain the benefits of leveraging third-party products and services, USNH must effectively manage the accompanying impact on cybersecurity risk. The requirements defined in this standard seek to accomplish that task by establishing consistent processes and procedures for vetting and managing vendor services used to capture, store, process, and transmit institutional information for USNH or any of its component institutions.

The use of a vendor service does not absolve USNH from its responsibility for ensuring that information is properly and securely handled, stored, and managed.

2 SCOPE

This standard covers vendor services and products that manage, store, or transmit sensitive or restricted USNH information, including those licensed by USNH or one of its component institutions, those licensed or utilized only by individual USNH community members to conduct USNH or component institution business. It covers all third-party services, including free services, regardless of the cost of licensing those services.

3 AUDIENCE

All USNH community members who are responsible for or interested in using vendor services to conduct USNH or component institution business should understand this standard and ensure they are compliant with the requirements.

4 STANDARD

To effectively manage the cybersecurity and other risks specific to information technology services to conduct USNH or component institution business, the vendor engagement lifecycle shall be effectively managed. This lifecycle includes the following stages:

- Stage 1: Definition and Discovery
- Stage 2: Solution Selection
- Stage 3: Vetting
- Stage 4: Engagement
- Stage 5: Administration, Support, and Management

Using unapproved vendor services to conduct USNH or component institution business or to capture, store, process, transmit, or otherwise manage institutional information is prohibited. This includes using vendor services like Google docs, DropBox, or similar for storing institutional information, data, files, or documentation.

Failure to follow this lifecycle and to engage with the appropriate USNH and institutional units at each stage can result in delays in contract signing, completion of vetting processes, and overall implementation of the requested functionality.

4.1 DEFINITION AND DISCOVERY

Administrative, academic, and business units interested in pursuing an information technology service or product shall engage Enterprise Technology & Services (ET&S) to assist with defining the unit's business needs and high-level requirements. ET&S shall determine if an existing solution provides this functionality and can meet the specified requirements.

4.2 SOLUTION SELECTION

Business unit needs that can be met with existing solutions shall be implemented as outlined in the *System Acquisition, Development, and Maintenance Lifecycle Standard.*

Administrative, academic, and business units with defined needs that cannot be met with existing solutions shall engage with USNH Procurement to identify potential vendor offerings via standard USNH Procurement Request for Information (RFI) and Request for Proposal (RFP) processes.

4.3 Vetting

To effectively manage cybersecurity risk, Cybersecurity Governance Risk and Compliance (GRC) shall vet all services and products that store, process and transmit USNH information. Based on the intended use of and institutional information involved, Cybersecurity GRC shall determine if the requested use of that vendor shall be permitted or if additional vetting and formal approval are required.

The formal approval process for vendor information technology services includes the following:

- Completion of the Vendor Security Assessment Review (SAR) process
- SAR Approval from Cybersecurity GRC
- Contract/licensing agreement vetting by USNH Procurement and, where appropriate, assistance with licensing agreement or contract term negotiations
- USNH/Institutional Data Steward approval for access to and use of the institutional information needed by the vendor service
- Designation of a Business Application Owner or Technology Service Owner for the vendor service

4.4 Engagement

Administrative, academic, and business units shall not sign any service contract, licensing agreement, or master services agreement or agree to any terms of service without engaging ET&S and USNH Procurement Services. Users engaging in renewal agreements should also work with Procurement Services to ensure legacy engagements are properly vetted.

Wherever possible, products and services shall leverage the central authentication services provided by ET&S USNH community members. If the service cannot implement single-sign-on (SSO), community members shall use their USNH username to access vendor services, and passwords shall abide by the USNH Password Policy.

4.5 Administration, Support, and Maintenance

Administrative, academic, and business units that procure information technology products and services shall:

- Be responsible for securely administering the service and providing support, maintenance, and vendor relationship management for that service directly or through negotiated support agreements ET&S.

- Designate an individual as the business application/Technology Service Owner for vendor service/product and provide this information to ET&S.
- Engage with Cybersecurity GRC to assist in determining security requirements for service administration.

The Business Application Owner or Technology Service Owner designated for an information technology product or service shall ensure any institutional information captured, stored, processed, transmitted, or otherwise managed by that service is backed up.

Information technology services used for USNH or component institution business shall provide the ability to:

- Make institutional information available to USNH or its component intuition upon request
- Permanently remove institutional information as dictated in the *Information Technology Resource Secure Disposal Standard* at the request of USNH or its component institution

4.5.1 Management of Institutional Information Used by services

Community members leveraging third-party vendors shall leverage the *USNH Information Classification Policy* to help inform decisions on the appropriateness of services for different administrative, academic, or business situations.

Tier 1 - PUBLIC

- New vendor services or products that capture, store, process, transmit, or otherwise manage PUBLIC

  Cybersecurity GRC shall authorize information
- Use of existing approved vendor services for PUBLIC institutional information is allowed and does not require Cybersecurity GRC approval
- Each new use of a previously approved vendor service requires Data Steward approval via the *Data Access Request process* outlined below
- Administrative, academic, or business units shall:
  - Ensure that the use of vendor services or product does not violate any existing USNH or component institution licensing agreements
  - Ensure that only approved PUBLIC information is captured, stored, processed, transmitted, or managed in this service

Tier 2 – SENSITIVE and Tier 3 – PROTECTED

- Use of new information technology services or products to capture, store, process, transmit, or otherwise manage institutional information classified as SENSITIVE and PROTECTED requires formal approval as outlined above
- Previously approved information technology services that are allowed but require:
  - Confirmation from Cybersecurity GRC that:

        - The classification of the information involved matches the classification of information the vendor has been approved to handle
        - The existing vendor has an active SAR approval in place
    - Data Steward approval for the use of the specific data elements via the *Data Access Request* process

Tier 3 - RESTRICTED

- Use of new vendor services to capture, store, process, transmit, or otherwise manage institutional information classified as RESTRICTED requires formal approval as outlined above
- Previously approved cloud services that are allowed but require:
    - Confirmation from Cybersecurity GRC that:
        - The classification of the information involved matches the classification of information the vendor has been approved to handle
        - The existing vendor has an active SAR approval in place
    - Data Steward approval for the use of the specific data elements via the *Data Access Request*
- Where applicable, approval from the appropriate institutional HIPAA Privacy Officer and the HIPAA Security Officer may be required

USNH or component institution PCI Manager or Committee shall approve any service or product intended to capture, store, process, transmit, or otherwise manage RESTRICTED institutional information related to the processing of credit card payments.

4.6 Vendor Security Assessment Review (SAR)

Any product or service used to capture, store, process, transmit, or otherwise manage institutional information with a classification other than PUBLIC shall be vetted using the Security Assessment Review (SAR) process. This process requires the proposed vendor to complete an industry-standard security control assessment, may involve several rounds of review and clarification between Cybersecurity GRC and the vendor, and can take an extended period. In most cases, the time needed to complete this process is determined by the vendor and how quickly they respond to requests for information. Administrative, academic, and business units shall plan accordingly to ensure adequate time to complete the SAR process before contract signing.

An administrative, academic, or business unit representative engaging with the vendor shall be assigned as the primary liaison between Cybersecurity GRC and the proposed vendor. Additional Information about this process is available by request from Cybersecurity GRC.

If an administrative, academic, or business unit chooses to move forward with a vendor product or service that does not receive Cybersecurity GRC approval after completing the SAR process, acceptance of that risk shall be required. The unit's senior leadership licensing the unapproved vendor information technology service shall be responsible for risk acceptance as outlined in the *Cybersecurity Risk Acceptance Standard*.

4.7 Data Access and Use Request Process

Approval to access and/or use any institutional information, regardless of classification, in a vendor service shall be granted by the appropriate Data Steward via the *Data Access and Use Request* process administered by Cybersecurity GRC.

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 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

8.1 Business Application Owner/Technology Service Owner:

- Ensure information technology services are appropriately vetted or approved before implementation
- Ensure appropriate contract safeguards are added to the vendor contract terms or licensing agreement by working with USNH Procurement and Cybersecurity GRC
- Manage vendor relationships, contract renewals, and upgrade activities
- Ensure secure administration of the vendor information technology service, including, when applicable, appropriate administration of local application accounts
- Provide end-user support for the vendor information technology service
- Understand the proper retention period and, when applicable, the destruction date of the institutional data used in the system for which they are responsible (Contact the appropriate Data Steward for detailed retention information)
- Ensure secure destruction of institutional data when requested or indicated by the Data Steward responsible for that information
- Complete annual Cybersecurity Risk Assessment and annual access audit for the service
- Report any notification of a potential or confirmed cybersecurity incident received from the vendor to Cybersecurity GRC

8.2 Cybersecurity Governance, Risk, & Compliance (GRC):

- Authorize the use of vendor information technology services that don't require formal approval
- Determine if vendor information technology services under consideration need a vendor Security Assessment Review (SAR)
- Perform vendor Security Assessment Reviews as needed
- Recommend language and/or provisions for contract terms and licensing agreements to ensure maintenance of USNH's security posture
- Assist administrative, academic, and business units in determining required security controls for the secure administration of information technology services
- Track completion of vendor service annual Cybersecurity Risk Assessments

8.3 Data Steward:

- Review and approve/deny requests to use requested institutional information in their assigned subject area within an information technology service

8.4 USNH Community Members:

- Follow this standard when procuring vendor information technology services

8.5 USNH Procurement Services:

- Determine required language and/or provisions for the vendor service contract or licensing agreement inclusion
- Approve procurement requests for new information technology services

9 DEFINITIONS

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

- Access
- Business Application Owner
- Central Authentication Services
- Cloud Service
- Credentials
- Data Steward
- Health Insurance Portability and Accountability Act (HIPAA)
- Information
- Information Technology Resource
- Institutional Information
- Payment Card Industry – Data Security Standard (PCI-DSS)
- PROTECTED Information
- PUBLIC Information
- RESTRICTED Information
- Risk Acceptance
- SENSITIVE Information
- Technology Service Owner
- Username
- USNH Community Member
- Vendor

10 RELATED POLICIES AND STANDARDS

- USNH Cybersecurity Policy
- USNH Information Classification Policy
- Access Management Standard
- Cybersecurity Exception Standard
- Cybersecurity Risk Acceptance Standard
- Cybersecurity Risk Management Standard
- Information Technology Resource Secure Disposal Standard
- System Acquisition, Development, and Maintenance Lifecycle 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:	19 AUG 2021
Approved by:	CHIEF INFORMATION SECURITY OFFICER, T NUDD, 19 AUG 2021 V1 CYBERSECURITY POLICY & STANDARD WORKING GROUP, 08 OCT 2020 V0.3
Reviewed by:	USNH PROCUREMENT, FEB 2021, V1 CHIEF INFORMATION SECURITY OFFICER, D STOCKMAN, JAN 2021 V0.3 CYBERSECURITY POLICY & STANDARD WORKING GROUP, OCT 2020
Revision History:	REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 09 MAR 2020 V0.4 UPDATED MARCH 10, 2023 CYBERSECURITY GRC WORKING GROUP