University System of New Hampshire

VENDOR CLOUD SERVICE SECURITY STANDARD

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

1 PURPOSE

This Standard outlines requirements for secure use of vendor cloud-hosted and software-as-a-service (SaaS) applications (vendor cloud services) in support of University System of New Hampshire (USNH) administrative, academic, and business unit needs.

Vendor cloud services are information technology resources provided by external parties that enable USNH and its component institutions to gain additional capabilities.

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

Use of a vendor cloud service to capture, store, process, transmit, or otherwise manage institutional information does not absolve USNH from its responsibility for ensuring that information is properly and securely handled, stored, and managed.

2 SCOPE

This Standard covers all vendor cloud services including those that are licensed by USNH or one of its component institutions and those that are licensed or utilized only by individual USNH community members for purposes of conducting USNH or component institution business. It covers all vendor cloud services, regardless of the cost to license those services, including services offered free of charge.

3 AUDIENCE

All USNH community members who are responsible for or interested in using vendor cloud services to conduct USNH or component institution business should understand this Standard and ensure they are

compliant with the requirements it defines.

4 STANDARD

In order to effectively manage the cybersecurity and other risks specific to the use of vendor cloud 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

Use of unapproved vendor cloud services to conduct USNH or component institution business or to capture, store, process, transmit, or otherwise manage institutional information is not allowed. This includes the use of vendor cloud services like Google docs, Drop Box, or similar for the storage of institutional information, data, files, or documentation.

Administrative, academic, and business units are advised that 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 requested functionality.

DEFINITION AND DISCOVERY

Administrative, academic, and business units interested in pursuing a vendor cloud service to provide needed functionality shall engage Enterprise Technology & Services (ET&S) to assist with definition of the unit's business need and high-level requirements. Once the high-level requirements for the desired functionality have been defined, ET&S shall determine if there is an existing solution that provides this functionality and can meet the defined requirements.

SOLUTION SELECTION

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

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

University System of New Hampshire

VETTING

In order to effectively manage cybersecurity risk, all vendor cloud services used to conduct USNH or component institution business or to capture, store, process, transmit, or otherwise manage institutional information shall be vetted by Cybersecurity Governance, Risk, and Compliance (GRC). Based on the intended use of the vendor cloud service and the institutional information involved, Cybersecurity GRC shall determine if the requested use of that vendor cloud service shall be allowed or if additional vetting and formal approval is required.

The formal approval process for vendor cloud services includes:

- 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
- Contract term/licensing agreement vetting by Cybersecurity GRC to ensure appropriate data security provisions are included
- USNH/Institutional Data Steward approval for access to and use of the institutional information needed by the vendor cloud service
- Designation of a Business Application Owner or Technology Service Owner for the vendor cloud service

ENGAGEMENT

Administrative, academic, and business units shall not sign any vendor cloud service contract, licensing agreement, or master services agreement, or agree to any terms of service, including renewal agreements, without engaging ET&S and USNH Procurement Services. This ensures that legacy engagements that were in place prior to the development of these requirements are appropriately vetted for security posture, data use, and contract terms.

Wherever possible, vendor cloud services shall leverage the central authentication services provided by ET&S for authentication of USNH community members.

If central authentication services cannot be used to enable access to a cloud service, the cloud service shall use USNH username or USNH email address as the username for access to vendor cloud services, and USNH community members shall be explicitly instructed not to use the same password as they use for their USNH credentials.

ADMINISTRATION, SUPPORT, AND MAINTENANCE

Administrative, academic, and business units that procure vendor cloud services shall be responsible for securely administering the cloud service and providing support, maintenance, and vendor relationship

management for that service, either directly or through negotiated support agreements ET&S.

Administrative, academic, and business units that procure vendor cloud services shall designate an individual to act as the Business Application Owner/Technology Service Owner for the vendor cloud service and provide this information to ET&S.

The Business Application Owner/Technology Service Owner shall engage with Cybersecurity GRC for assistance in determining security requirements for administration of the cloud service.

All cloud services administered by administrative, academic, or business units shall complete Cybersecurity Risk Assessments as outlined in the *Cybersecurity Risk Management Standard*. The intention of this Risk Assessment is to confirm the appropriate security controls are in place for internal management of the vendor cloud service. This is different than the vendor Security Assessment Review (SAR) process outlined previously, which deals specifically with the vendor's cybersecurity posture.

Additionally, annual access audits, as defined in the *Access Management Standard*, shall be conducted. The designated Business Application Owner/ Technology Service Owner for the vendor cloud service shall be responsible for ensuring these annual processes are completed.

The Business Application Owner or Technology Service Owner designated for a vendor cloud service shall be responsible for ensuring any institutional information captured, stored, processed, transmitted, or otherwise managed by that vendor cloud service is backed up in accordance with requirements provided in relevant ET&S Standard(s).

Vendor cloud 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

Management of Institutional Information Used by Cloud services

The *USNH Information Classification Policy* establishes a framework for classifying institutional information using the following tiers. Details about each classification can be reviewed in the policy.

- Tier 1 – PUBLIC
- Tier 2 – SENSITIVE
- Tier 3 – PROTECTED
- Tier 4 – RESTRICTED

The following adapts the information classification framework to help inform decisions on the appropriateness of vendor cloud services for different administrative, academic, or business situations.

Tier 1 - PUBLIC

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

information shall be authorized by Cybersecurity GRC
- Use of existing approved vendor cloud services for PUBLIC institutional information is allowed and does not require Cybersecurity GRC approval
- Each new use of a previously approved vendor cloud service requires Data Steward approval via the *Data Access Request process* outlined below
- Administrative, academic, or business unit shall:
    - Ensure that use of vendor cloud services 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 cloud service

Tier 2 – SENSITIVE and Tier 3 – PROTECTED

- Use of new vendor cloud services to capture, store, process, transmit, or otherwise manage institutional information classified as SENSITIVE and PROTECTED requires formal approval as outlined above
- Use of vendor cloud services that have been previously approved is allowed, but requires:
    - 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 use of the specific data elements via the *Data Access Request* process

Tier 3 - RESTRICTED

- Use of new vendor cloud services to capture, store, process, transmit, or otherwise manage institutional information classified as RESTRICTED requires formal approval as outlined above
- Use of vendor cloud services that have been previously approved is allowed, but requires:
    - 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 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 cloud service intended to capture, store, process, transmit, or otherwise manage RESTRICTED institutional information related to the processing of credit card payments

University System of New Hampshire

VENDOR SECURITY ASSESSMENT REVIEW (SAR)

Any vendor cloud 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. Administrative, academic, and business units shall plan accordingly to ensure adequate time to complete the SAR process prior to contract signing. 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 to complete. In most cases, the time needed to complete this process is determined by the vendor and how quickly they respond to requests for information.

A representative from the administrative, academic, or business unit 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 cloud service that does not receive Cybersecurity GRC approval after completing the SAR process, acceptance of that risk shall be required. Senior leadership of the unit licensing the unapproved vendor cloud service shall be responsible for risk acceptance as outlined in the *Cybersecurity Risk Acceptance Standard.*

DATA ACCESS AND USE REQUEST PROCESS

Approval to access and/or use any institutional information, regardless of classification, in a vendor cloud 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

Business Application Owner/Technology Service Owner:

- Ensure cloud services are appropriately vetted or approved prior to 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 relationship, contract renewals, and upgrade activities
- Ensure secure administration of the vendor cloud service including, when applicable, appropriate administration of local application accounts
- Provide end-user support for the vendor cloud service
- Understand the appropriate retention period and, when applicable, the destruction date of the institutional data used in the cloud 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
- Ensure any institutional information captured, stored, processed, transmitted, or otherwise managed by that cloud service is backed up in accordance with requirements in relevant ET&S Standard(s)
- Complete annual Cybersecurity Risk Assessment and annual access audit for the vendor cloud service
- Report any notification of a potential or confirmed cybersecurity incident received from the cloud service vendor to Cybersecurity GRC

Cybersecurity Governance, Risk, & Compliance (GRC):

- Authorize use of vendor cloud services that don’t require formal approval
- Determine if vendor cloud services under consideration require 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 secure administration of cloud services
- Track completion of vendor cloud service annual Cybersecurity Risk Assessments

Data Steward:

- Review and approve/deny of requests to use requested institutional information in his/her assigned subject area within a cloud service

USNH Community Members:

- Follow this standard when procuring vendor cloud services

USNH Procurement Services:

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

University System of New Hampshire

- 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

---

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

University System of New Hampshire

Revision History:	REVIEW DRAFT FINALIZED, R BOYCE-WERNER, 09 MAR 2020