[redacted]

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

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.

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

[redacted]

compliant with the requirements it defines.

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.

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

[redacted]

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

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 engag

- 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 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 ς SENSITIVE, Tier 3 ς PROTECTED, and Tier 3 - RESTRICTED

- Use of new vendor cloud services to capture, store, process, transmit, or otherwise manage institutional information classified as anything other than PUBLIC 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 process

Tier 5 - CONFIDENTIAL

- Use of new vendor cloud services to capture, store, process, transmit, or otherwise manage institutional information classified as CONFIDENTIAL 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
- Where applicable, approval from the appropriate institutional HIPAA Privacy Officer and the HIPAA Security Officer
- 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
-

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 respon

¶ Perform vendor Security Assessment Reviews, as needed

¶ Recommend language and/or provisions for contract terms and licensing agreements to ensure