[redacted]

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

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.

[redacted]

compliant

[redacted]

In order to effectively manage

[redacted]

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 . 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 , 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 at the request of USNH or its component institution

The 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 –

[redacted]

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 USN32eao32eao32eao32eao32eao32ea

[redacted]

Non-compliant technology and/or activities may be mitigated as deemed necessary by the CISO and/or CIO.