Vendor Management Plan

Department: Information Technology, Ethics & Compliance, Purchasing & Contract Services

Focus Area: Entire University

1. Purpose and Objectives

This Vendor Management Plan (VMP) outlines how Utah State University protects its Institutional Data and information systems from potential risks associated with third-party vendors that support various university functions. The VMP focuses on ensuring that vendors handling institutional data do so in compliance with applicable laws and university policies.

Contracts are assessed and categorized into three tiers—Low, Moderate, and High Risk—based on the classification of the institutional data being processed. This risk-based approach guides how the university evaluates vendors' security and privacy practices, and determines the specific contractual terms required to safeguard data.

To remain responsive to evolving cyber threats, regulatory updates, and technology shifts, the plan is subject to regular review and revision.

2. Scope

This Vendor Management Plan applies when any USU unit, college, department, faculty, staff, or a government agency acting on behalf of USU, enters into a contract with a third-party vendor that will process Institutional Information, regardless of whether that information includes personally identifiable information (PII). This includes any data classified as Low, Moderate, or High Risk under USU's Data Classification Standard.

3. Exclusions

This Vendor Management Plan does not apply to the following situations:

- Contracts with third-party vendors who receive only fully de-identified data, and where re-identification is not reasonably possible.
- Contracts solely for the provision of general internet or connectivity services (e.g., ISPs), provided no institutional information is stored or processed by the provider beyond what is necessary to deliver the service.

4. Definitions

4.1. Personally Identifiable Information (PII): Refers to data that directly identifies an individual or can be used to identify an individual when combined with other information. This data falls into three categories: low-risk, moderate-risk, and high-risk. Refer to the **USU Institutional Data Classification** for details on each category.

4.2. **Process or Processing:** It means any operation or set of operations performed on PII, including collection, recording, organization, structuring, storage, adaptation, alteration, access, retrieval, consultation, use, disclosure by transmission, transfer, dissemination, alignment, combination, restriction, erasure, or destruction.

4.3. **Third-Party Contract:** This is a legally binding agreement between a third-party vendor and Utah State University, in which the vendor commits to providing goods or services that are crucial for USU's operations but fall outside of USU's primary areas of expertise. The contract specifies the responsibilities, expectations, terms, and conditions mutually agreed upon by both parties, ensuring clear understanding of deliverables, timelines, and payment terms.

4.4. **Data Processing Language:** Refers to the legal language that defines the scope of data processing, including security measures, the use of subprocessors, and the rights of data subjects. It outlines detailed protocols for breach notification, data retention, and secure data disposal. The USU Data Processing Language functions as a Data Processing Agreement (DPA) and is incorporated into the USU Addendum. It plays a critical role in maintaining the integrity and confidentiality of personally identifiable information (PII) and ensuring compliance with applicable data protection laws and regulations.

4.5. **Business Associate Agreement (BAA):** BAA is a legally binding document required under the Health Insurance Portability and Accountability Act (HIPAA) when a covered entity enlists the services of a business associate to handle Protected Health Information (PHI). This agreement sets forth the responsibilities of the business associate in protecting the privacy and security of PHI to comply with HIPAA regulations. It details the permissible uses and disclosures of PHI by the business associate, ensuring that they meet stringent standards to safeguard patient information against unauthorized use or disclosure.

4.6. **Higher Education Community Vendor Assessment Toolkit (HECVAT):** The HECVAT is an standardized questionnaire utilized to evaluate a third-party vendor's security and compliance controls for handling USU data. It outlines the vendor's proposed use of USU systems and data, the specific data involved, and assesses the vendor's ability to adequately safeguard institutional data throughout the full lifecycle of the product or service. While this is the standard vendor assessment tool, alternative risk questionnaires or evaluation methods may be used if reviewed and approved by the Information Assurance Team.

4.7. **De-Identified Data:** De-identified data refers to information that has been processed to remove or obscure all personal identifiers, making it no longer possible to reasonably identify an individual directly or indirectly. This includes the removal of names, ID numbers, addresses, and any other data elements that could allow re-identification when combined with other information. For more detailed requirements and best practices, refer to the USU De-Identification Guidelines.

5. Procedure Requirements

Utah State University classifies contracts based on the type of data. Refer to the **USU Institutional Data Classification** for details on each category.

Prior to establishing a contractual relationship with a vendor, USU units must identify the data that will be shared with or accessed by the vendor and the appropriate data classification.

The review process and contractual requirements should be tailored based on the contract's risk level:

Table N. 1

Type of Contract	Type of Data	BAA	Data Processing Language	HECVAT
High-Risk Contract	**High-Risk Data**	✗	✓	✓
High-Risk Contract	**High-Risk Data HIPAA**	✓	✓	✓
Moderate-Risk Contract	**Moderate-Risk Data**	✗	✓	✗
Low-Risk Contract	**Low-Risk Data**	✗	✗	✗

6. Contractual Requirements for PII Data Processing

When USU or a government agency contracting on behalf of an educational entity enters a Data Processing Agreement (DPA) with a third-party vendor to disclose personally identifiable information (PII), the DPA must:

6.1. Provide a detailed description of the type of PII, the nature and purpose of data processing, the number and types of individuals whose data will be utilized, whether the product or service involves processing PII from individuals outside of the United States, and if so, specify the countries or regions involved. Additionally, clarify if the processing involves USU's Critical Institutional Data (CID) or export control data.

6.2. Include a list of sub-processors, detailing who owns and manages access to these sub-processors, their geographic locations, and their specific processing activities.

6.3. Require the third-party vendor to limit the use of PII exclusively to the purposes of providing the contracted products or services within the terms of the negotiated data processing contract.

6.4. Establish requirements and restrictions on the collection, use, storage, and sharing of PII by the third-party vendor that are necessary for USU to ensure compliance with applicable regulations.

6.5. Describe the data disposition processes by which the third-party vendor will return, delete, or destroy PII when it is no longer necessary to retain or upon request by USU.

6.6. Allow the educational entity or its designee to audit the third-party contractor to verify compliance with the data processing contract and applicable legal provisions at its request, and require the contractor to cooperate with such audits.

6.7. The DPA must also stipulate that the third-party vendor is required to notify USU without undue delay, and in no case later than 72 hours after detecting any data breach or security incident impacting the University's PII. This notification should detail the incident's specifics, including the types of data compromised, the number of individuals affected, potential consequences, and immediate corrective measures undertaken. The vendor must collaborate with USU to mitigate damages and implement agreed-upon preventive actions to avert future breaches.