IT VENDOR MANANGEMENT POLICY

Table of Contents

TEMPLATE information (DELETE BEFORE USING)

This template is provided as an example of a policy or procedure that is based on the NIST 800-171 standards. It should be used as a reference point to create your own policy. It is important to note that no policy or procedure is "one-size fits all" and this document will require modification before use.

Authority

This policy was created with guidance from the following standards:

- State Administrative Manual (SAM) 3500: Purchases
- State Administrative Manual (SAM) 5300: Information Technology - Office of Information Security
- NIST 800-171 Rev. 2 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations Systems)
- NIST Cybersecurity Framework

Purpose

The purpose of this policy is to establish a process for which IT vendor risk is identified, appropriate due diligence is performed and maintained to protect [COLLEGE] data, and ownership for these responsibilities is assigned.

Terms and Definitions

Memorandum of Understanding (MOU): A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission.

People: All contractors, third-party processors, and vendors.

Request for Proposal (RFP): A document that solicits a proposal, often made through a bidding process, by an agency or company interested in procurement of a commodity, service, or valuable asset, to potential suppliers to submit business proposals.

SOC 2: Stands for "System and Organization Controls II" report. This is a suite of reports designed to provide customers and other key stakeholders with insight into the design and operating effectiveness of system-level controls of a service organization or entity-level controls of other organizations. It is important to note that there is a difference between a SOC 2 Type 1 and Type 2.

- SOC 2 Type 1: The design of the controls is evaluated, but the implementation of the controls is not audited. In simple terms, the organization says it is doing the right things, but it hasn't been validated.

- SOC 2 Type 2: The design and implementation of the controls is audited over a period of time. In simple terms, the organization says it is doing the right things, and it has been validated that they are doing what they say.

Vendor: Product and service providers used for internal purposes (e.g., IT infrastructure) or integrated into products and services. Also referred to as "Suppliers" or "Third Parties"

Scope

This policy applies to the [COLLEGE], employees, contractors, subcontractors, vendors, consultants, advisors, and other personnel who have access to [COLLEGE] technology assets.

Exceptions

No exceptions for this policy are currently in place.

[COLLEGE] reserves the right to amend, revoke or terminate this policy in part or in its entirety, as it may deem necessary from time to time in accordance with applicable law.

Vendor Selection

In cases where a Request for Proposal (RFP) is issued, the RFP shall contain detailed information security requirements related to the NIST 800-171 Rev. 2 standards. RFPs for critical vendors should request security-related documentation, including vulnerability scans/penetration tests, data breach reports, and third-party audits such as SOC 2 Type 2 reports.

[TEMPLATE NOTE – RFP policy may vary at the local college level and may be guided by State Administrative Manual 3503 – Competitive Purchases. It is recommended that a direct reference to local policy is included for reference.]

All vendor contracts, regardless of whether an RFP was issued, shall be reviewed to verify that the following are clearly defined:

- Security-related Service Level Agreements (SLAs) and Key Performance Indicators (KPIs)
- Data protection and retention requirements
- Access to and requirements for handling sensitive information such as PII or ePHI
- Incident response and business continuity procedures and obligations
- Security lapse notification requirements, especially concerning data breaches
- Vendor termination requirements and transition plans
- Subcontracting and outsourcing permissions
- Audit and inspection conditions

In addition, all contracts issued shall contain provisions that address the following:

- Obligation on the part of the vendor to keep all sensitive information confidential.
- Obligation on the part of the vendor to notify the [COLLEGE] if a breach of service provider security measures occurs.
- Continuance of these stipulations beyond the length of term of the contract at least until such time as the vendor retains no sensitive [COLLEGE] data.

Vendor Categorization

Vendors shall be categorized based on risk using the following guidelines. The Vendor Risk Assessment shall be updated annually or when a new vendor is added.

Vendor Level	Definition
Critical	Vendors that have access to [COLLEGE] systems or data or provide services that are mission critical and there is no immediate replacement, or it would be difficult to replace the vendor's service.
Non-Critical	Vendors that do not have access to [COLLEGE] systems or data and are easily replaceable.

Vendor Monitoring

A vendor risk management matrix shall be maintained by the [COLLEGE]. It is important for the matrix to be updated as vendors are onboarded or relevant information changes. It will contain:

- Inventory of vendors, their respective risk categories, and summary of their functions
- Systems/Applications owned/hosted by each vendor
- Data stored/processed/transmitted by each vendor, including PII and ePHI
- Involvement in Incident Response/Business Continuity Planning (IR/BCP) procedures
- Information security point of contact

The [COLLEGE] shall review vendors on the following timetable to ensure continued policy compliance:

- Critical vendors shall be reviewed on an annual basis. Management will review SOC Reports, when available, as a substitute for in-person review of vendor security controls and processes for all vendors who store critical [COLLEGE] information on their systems at their location. In the absence of a formal SOC report, other audit reports and tests of key controls can be considered for adequacy in attesting to the sufficiency of the vendor's Information Security Program.
- Non-critical vendors shall be reviewed upon contract renewal.

Questions

Questions regarding the information in this Policy should be directed to [COLLEGE IT or SECURITY GROUP].

Reference Documents

Document	Link
NIST Cybersecurity Framework	https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
NIST 800-171	https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
CA State Administrative Manual (SAM)	https://www.dgs.ca.gov/Resources/SAM
[LOCAL CONTRACTS POLICY]	[Provide link to local contracts policy for reference]

Relevant Standards

Area	NIST Reference
NIST CSF	ID.AM-6, PR.AT-3