Vendor Management Policy

Purpose

The purpose of this policy is to establish the scope and objectives for the selection, acquisition, and management of products and services from third-party vendors, in order to maintain the security of <Company Name>'s information assets that are accessible by those vendors.

Scope

This policy is applicable to all vendors used by <Company Name> to store or process information on behalf of <Company Name>, vendors that work with <Company Name> systems, and vendors who develop applications or services for <Company Name>.

Ownership

[POLICY OWNER]

is responsible for implementing and maintaining this policy.

Policy Statement

<Company Name> relies on the services of third-party vendors to help it achieve its mission and efficiently run its daily operations. In many cases, these vendors must access sensitive data in order to support critical <Company Name> operations. To maintain the security, confidentiality, and integrity of such data, <Company Name> must ensure that third-party service providers implement and effectively operate appropriate controls.

Inventory and classification

The company maintains an inventory of its vendors and classification of the data they store or process.

<Company Name> maintains a complete list of all its vendors and classifies them based on the classification of the systems each vendor provides. The methodology <Company Name> employs to classify its systems is defined in the Data Classification Policy. Once every system provided by a vendor has been classified according to this policy, the vendor's classification becomes that of the most sensitive system it provides.

Vendor risk assessment

As part of the risk management process, vendors storing data classified as Customer Sensitive undergo due diligence and risk assessment.

A vendor's classification determines the extent of the risk assessment that must be conducted with regards to the systems it provides, and the safeguards that must be put in place to ensure the vendor's continued compliance with relevant requirements and regulations. For example, vendors classified as Customer Confidential require the highest level of diligence and contractual obligations.

<Company Name> maintains a full checklist for performing vendor risk assessments as part of its vendor risk assessment procedure. The assessment process adheres to the following principles:

Vendors that store, process, or authenticate Customer Sensitive data must:

- Implement security safeguards to protect <Company Name> data that are at least as strict as those <Company Name> applies to its own systems
- Design and implement controls to mitigate and contain data security risks through proper separation of duties, role-based access, and least-privilege access for all personnel within their supply chain
- Ensure that applicable information security controls are integrated in all service support processes applicable to their contractual relationship with<Company Name>(customer support, etc)
- Make security incident information promptly available to<Company Name>

Risk assessments must be conducted before doing business with a new vendor, and revisited when the relationship with the vendor changes significantly, including when contracts are renewed.

A mutual Non-Disclosure Agreement (mNDA) may need to be signed with the prospective vendor, if sensitive information (such as business strategy or plans) is to be shared during the evaluation period.

<Company Name> may require that the vendor complete a Vendor Assessment Questionnaire (VAQ), or accept current SOC 2 or ISO 27001 certifications as an alternative.

In addition, vendor assessment takes into account how the vendor might impact:

- <Company Name>'s regulatory risk
- <Company Name> reputation and financial risk
- <Company Name>'s product performance, availability, or operational effectiveness
- <Company Name> business continuity exposure, in case the vendor has long-term issues or goes out of business altogether

Once the above information is collected and reviewed, [POLICY OWNER]

determines whether <Company Name> can work with the vendor.

Vendor Agreements

Agreements with third-party services that handle Customer Sensitive data include requirements and expectations regarding data confidentiality and the vendor's security responsibilities

<Company Name>'s agreements with third-party vendors are not expected to be custom, and may be identical to the default agreement offered by each vendor. However, an agreement with every vendor must be in place, and this agreement must include provisions that cover:

- The scope of the business relationship and services offered
- Clearly outlined obligations to fulfill relevant information security requirements between <Company Name> and the vendor. Any division of responsibility must be clearly defined
- Non-disclosure of confidential information
- Vendor obligations to enforce security requirements over their supply chain subprocessors, as applicable
- Terms for termination of the business relationship and the treatment of <Company Name> data in such an event
- The performance and availability of the service (SLA), if possible