Vendor Management Policy

This example serves as a basic overview of the sections to include within your own Vendor Management Policy. Your organization may choose to add sections that relate to your specific business functions.

Revision History

Status:		Draft		Approved		Adopted	
Document owner:	Name		Role				
Last review date:							

Change log	
Date:	Changes made:
Date:	Changes made:
Date:	Changes made:

Table of Contents

Vendor Management Policy

1 Purpose

_____ [COMPANY] utilizes third-party products and services to support our mission and goals. This Vendor Management Policy contains the requirements for how _____ [COMPANY] will preserve and protect information.

_____ [COMPANY] makes every effort to assure all third-party vendors are compliant and do not compromise the integrity, confidentiality, and privacy of _____ [COMPANY] or its data. Third parties include customers, partners, subcontractors, and contracted developers.

_____ [COMPANY] commits to regular reviews of this Vendor Management Policy annually by _____ [DOCUMENT OWNER].

2 Audience and scope

The policy applies to all vendors and partners who have the ability to impact the confidentiality, integrity, and availability of _____ [COMPANY] technology and sensitive information, or who are within the scope of _____ [COMPANY]'s information security program.

3 Roles and responsibilities

The roles and responsibilities of _____ [COMPANY] team members related to vendor management are as follows:

Vendor managers shall:

- Ensure that stakeholder requirements are complete and accurate as documented
- Ensure that vendor responses address all requirements
- Support vendor selection and contract negotiation
- Establish service level agreement (SLA) standards and monitor performance against these
- Communicate the status of the contract to stakeholders in a timely manner
- Ensure that key risks are identified and monitored
- Ensure that problems, issues, disputes, and other matters are resolved in a timely manner
- Manage the termination and transition process

Role: _____ **Responsibility:** _____

Role: _____ **Responsibility:** _____

Vendor Management Policy

4 Audience and scope

Refer to the Glossary of Terms located on _____ [COMPANY] website.

5 Assessments

Vendors are prohibited from accessing _____ [COMPANY] information security assets until a contract containing security controls is agreed to and signed by the appropriate parties.

Vendors must be evaluated prior to the start of any service and thereafter on an annual basis.

Vendors and partners must ensure that organizational records are protected, safeguarded, and disposed of securely. _____ [COMPANY] strictly adheres to all applicable legal, regulatory, and contractual requirements regarding the collection, processing, and transmission of sensitive data such as Personally Identifiable Information (PII).

_____ [COMPANY] may choose to audit vendors and partners to ensure compliance with applicable security policies, as well as legal, regulatory, and contractual obligations.

6 Management processes

Vendor agreements and contracts must specify:

- The _____ [COMPANY] information the vendor should have access to
- How _____ [COMPANY] information is to be protected by the vendor
- How _____ [COMPANY] information is to be shared between _____ [COMPANY] and the vendor
- Clear instructions for returning, destructing, or disposing of _____ [COMPANY] information in the vendor's possession at the end of the contract
- Minimum information security requirements
- Incident response requirements
- The right for _____ [COMPANY] to audit vendor

The vendor assumes responsibility regarding all information that is shared with a fourth-party vendor. The vendor is required to monitor the fourth party's information security practices that are in place to protect data.

Vendor Management Policy

Management processes (Cont.)

Vendor performance must be reviewed annually against contracts or SLAs. If the vendor is found to be in violation of the contract or SLA, the vendor will work with _____ [COMPANY'S] vendor manager until requirements are met.

_____ [COMPANY] information acquired by the vendor in the course of the contract cannot be used for the vendor's own purposes or shared with others.

_____ [COMPANY] will provide a point of contact for the vendor. The point of contact will work with the vendor to ensure the vendor is in compliance with these policies.

The vendor must report all security incidents directly to the appropriate _____ [COMPANY] point of contact within the timeframe defined in the contract.

Vendors must provide _____ [COMPANY] a list of key personnel working on the contract.

When the contract ends, the vendor will ensure that all sensitive information is collected and returned to _____ [COMPANY] or destroyed within the timeframe specified in the contract.

7 Enforcement

Any vendor, consultant, or contractor found to have violated this policy may be subject to sanctions up to and including removal of access rights, termination of contract(s), and related civil or criminal penalties.

8 Exceptions

_____ [COMPANY] business needs, local situations, laws and regulations may occasionally call for an exception to this policy. If an exception is needed, _____ [COMPANY] management will determine an acceptable alternative approach.