Vendor Management Policy

|  |  |
| --- | --- |
| Owner |  |
| Approver |  |
| Last Reviewed |  |

# Scope

All data and information systems owned or used by [Company Name] that are business critical and/or process, store, or transmit [Company Name] data. This policy applies to all employees of [Company Name] and to all software vendors which [Company Name] utilizes to deliver services. (e.g. Cloud vendors, SaaS vendors, integrations, add-ons)

# Policy

Information security requirements for mitigating the risks associated with vendor's access to the organization's assets shall be agreed with the vendor and documented.

For all vendors who may access [Company Name] data, systems, or networks, proper due diligence shall be performed prior to provisioning access or engaging in processing activities.

## Addressing Security in Agreements

Relevant information security requirements shall be established within the contract with the vendor.

# Monitoring, Evaluation & Review of Vendors and Integrations

[Company Name] shall perform an initial review of each vendor prior to onboarding and assign an initial vendor risk level. Vendors will be tracked within vendor management system. The vendor risk level will determine the level of diligence in the initial review and annually thereafter. The level of review is as follows:

# New Vendor Review Criteria

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risk Level** | **Criteria** | **Review Requirements** | **Example** | **Approvals Required New Vendors)** |
| High | A  vendor/integration is a high risk if used to store, transmit, process, change or access sensitive [Company Name] data and would have a high impact on [Company Name] business services. | New: Review of SOC 2 OR ISO 27001, or  CAIQ/similar and send security questionnaire dependent on risk and other certifications available |  |  |
| Medium | A  vendor/integration is a medium risk if the vendor/integration has limited access to sensitive data or if vendor service failure would have a  non-critical impact on [Company Name] business's services. | New: Review of SOC 2 OR ISO 27001, or  CAIQ/similar. If the vendor does not have any of the three, evaluate risk then send security questionnaire if necessary. |  |  |
| Low | A  vendor/integration is low risk if it does not store or | New: Review of publicly available security |  |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | access data other than publicly available data (ex: business contact) or if the vendor service failure would have little or no impact on [Company Name] business' services. | information.  If the vendor does not have any security certifications  SOC 2, ISO  27001 or supporting security documentation, send security questionnaire dependent on risk. |  |  |

\*Free vendors will not go through Finance review

If the vendor includes an integration, access rights and security are reviewed by the Security/IT teams as part of the new vendor process. Any integration requesting administrative permissions will be declined automatically due to security risk concerns.

 [Company Name] will additionally consider the following in the inspection of a vendor/integration

## Management of Changes to Vendors

Changes to the provision of services by vendors, including changes to agreements, services, technology, policies, procedures, or controls, shall be managed, taking account of the criticality of the business information, systems, and processes involved. [Company Name] shall assess the risk of any material changes made by vendors and make appropriate modifications to agreements and services accordingly.

Vendors depending on risk level, may be assessed appropriately for the following:

## Vendor Risk Management

[Company Name] will ensure that potential risks posed by sharing Confidential data are addressed according to this policy. Risk management plays an integral part in

the governance and management of the organization at a strategic and operational level.

[Company Name] shall not share or transmit Confidential data to a vendor without a fully executed written contract, statement of work or service agreement which describes expected service levels and any specific information security requirements.

## Vendor Security Standards

All vendors must maintain reasonable organizational and technical controls as assessed by [Company Name].

Assessment of vendors which receive, process, or store Confidential data shall consider the following controls as applicable based on the service provided and the sensitivity of data stored, processed or exchanged.

## Information Security Policy

Vendors maintain information security policies supported by their executive management, which are regularly reviewed.

## Risk Assessment & Treatment

Vendors maintain programs that assess, evaluate, and manage information and technology risks.

## Operations Security

Vendors implement commercially reasonable practices and procedures designed, as appropriate, to maintain operations security. Protections may include:

 Technical testing

 Protection against malicious software  Network protection and management  Technical vulnerability management

 Logging and monitoring  Incident response

 Business continuity planning

## Access Control

Vendors maintain a technical access control program.

## Secure System Development

Vendors maintain a secure development program consistent with industry software and systems development best practices including risk assessment, formal change management, code standards, code review and testing.

## Physical & Environmental Security

If vendors are storing or processing highly confidential data, their physical and environmental security controls should meet the requirements of the [Company Name] Physical Security Policy.

## Human Resources

Vendors maintain human resource policies and processes which include criminal background checks for any employees or contractors who access [Company Name] confidential information.

# Renewal Vendor Review Criteria

|  |  |  |  |
| --- | --- | --- | --- |
| **Risk Level** | **Criteria** | **Review Requirements** | **Example** |
| High | A vendor is a high risk if used to store, transmit, process, change or access sensitive [Company Name] data and would have a high impact on [Company Name] business services. | Annual compliance review of security documents (i.e CAIQ, SiG, white- papers) and certificates (ex: SOC 2, ISO 27001.  Documentation  within Jira ticket. |  |
| Medium | A vendor is a medium risk if the vendor/integration has limited access to sensitive data or if vendor service failure would have | Compliance review will be performed if a major change has been made to the a) vendor or b) [Company Name]ʼs usage.  Collection of |  |

|  |  |  |  |
| --- | --- | --- | --- |
|  | a non-critical impact on [Company Name] business's services. | security certificates during renewal. |  |
|  | A vendor is low | Collection of security certificates during renewal, if available |  |
|  | risk if it does not |  |
|  | store or access |  |
|  | data other than |  |
|  | publicly available |  |
| Low | data (ex: business  contact) or if the |  |
|  | vendor service |  |
|  | failure would have |  |
|  | little or no impact |  |
|  | on [Company Name] |  |
|  | business' services. |  |

**Termination of a Vendor/Integration**

Contracts with vendors shall contain clauses which govern termination and disposal of data. [Company Name] will ensure data is deleted from vendors upon termination based on criticality. For high risk vendor terminations  [Company Name] will ensure [Company Name] data is deleted. This can also involve a self deletion from an admin userʼs dashboard or settings.

## Compliance & Legal

[Company Name] shall consider all applicable regulations and laws when evaluating vendors who will access, store, process or transmit [Company Name] Confidential data.

## Relevant Documents:

Security/Compliance Review for Inbound Software/SaaS Purchases

Your [Company Name] Guide to Software/SaaS Procurement

Data Management Policy

Security Review for New Software and Vendor

## Review

This policy will be reviewed annually.

## Exceptions

Requests for an exception to this Policy must be submitted to the Director of Engineering, Security or the General Counsel for approval and documented within the Company ticketing system.

## Violations & Enforcement

Any known violations of this policy should be reported to the Director of Engineering, Security or the General Counsel. Violations of this policy can result in immediate withdrawal or suspension of system and network privileges and/or disciplinary action in accordance with company procedures up to and including termination of employment.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author** | **Approved by** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |