**Supply Chain and Business Partner Policy**

# ***Version Control Table***

| Version | Date | Author | Description |
| --- | --- | --- | --- |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| 1.0 |  |  |  |
| **1.0** |  |  |  |
|  |  |  |  |

| **Date of Next Revision** |  |
| --- | --- |

This policy will be reviewed for continued completeness, relevance, and accuracy within 1 year of being granted “final” status, and at yearly intervals thereafter.

The version control table will show the published update date and provide a thumbnail of the major change. CAUTION: the thumbnail is not intended to summarise the change and not a substitute for reading the full text.

# ***Table of Contents***

[**Version Control Table**](#_1t3h5sf) **2**

[**Table of Contents**](#_4d34og8) **3**

[**Purpose**](#_63rqrq7ix9vb) **3**

[**Scope**](#_s986lmz0m8b9) **4**

[**Policy**](#_rnh2rm3aff3p) **4**

[**Supplier Risk Assessment**](#_obq6x7298ar4) **4**

[**Vendor Due Diligence**](#_d5qvuoo1qb1q) **5**

[**Supplier Agreements**](#_la36m79v20t) **6**

[**Vendor Management**](#_gpd0ukxvoqaj) **6**

[**Vendor Compliance Monitoring**](#_io6ipyifgxu1) **6**

[**Change, Review, and Update**](#_5gvei5yt6zoy) **7**

[**Disciplinary Action**](#_tq744a9tyzj0) **7**

[**Responsibility**](#_z0lmne9fwh3i) **7**

[**Related Documents**](#_v6z7e8uoe1xk) **7**

# **Purpose**

The purpose of this policy is to describe the conditions of how to maintain information security when the third parties are involved in *[Company]’s* internal operations.

# **Scope**

The scope of this policy covers all of *[Company]’s* suppliers and business partners. This policy applies to all suppliers who access *[Company]’s* information or suppliers hosting the company’s information assets.

# **Policy**

## **Supplier Risk Assessment**

The risks associated with supplier management are described in the Risk Assessment. Information security requirements for mitigating the risks associated with suppliers’ access to the information assets must be agreed upon with the supplier and documented.

Each potential supplier or business partner is assessed by conducting the risk analysis with “low,” “medium,” and “high” ratings.

| **Rating** | **Low** | **Medium** | **High** |
| --- | --- | --- | --- |
| **Business impact** | The nominal impact could get along without it. Does not connect to any piece of *[Company]* infrastructure. | Significant but non-critical business impact. | Mission-critical. |
| **Customer-facing** | No | Indirect | Direct |
| **Access to customer data** | No access. | Access to often public but personally identifiable information (e.g., email addresses) | Access to non-public personally identifiable information (e.g., email content). |

The rating indicates the level of due diligence *[Company]* requires for each vendor:

* **Low-risk** vendors typically require little analysis;
* **Medium-risk** vendors should be evaluated to determine the appropriate level of due diligence required;
* **High-risk** vendors require extensive review.

## **Vendor Due Diligence**

Due diligence means describing the selected vendor’s ability to meet the service and security requirements. *[Company]* does this by sending a Vendor Assessment Questionnaire. Once it is completed, the company reviews the responses and decides the possibilities of further cooperation.

A due diligence review might include further discussions regarding the following topics:

* **Regulatory**: Can the vendor create regulatory risk for *[Company]*?
* **Reputation**: How might the vendor impact *[Company]’s* reputation?
* **Financial**: Can the vendor impact *[Company]* or its customers financially?
* **Access to customer data**: To what extent will the vendor handle sensitive *[Company]* data?
* **Operational effectiveness**: How might *[Company]* be affected if the vendor experienced downtime? If the vendor ceased operations suddenly? Are there other potential vendors that *[Company]* could work with?

To perform successful due diligence, these criteria must be evaluated and documented:

* Company’s reputation and history;
* Quality of services provided to other customers;
* Number and competence of staff and managers;
* Financial stability of the company and commercial record;
* Retention rates of the company’s employees;
* Criminal records;
* Security certifications (ISO 27001, SOC 2, PCI-DSS, etc.).

## **Supplier Agreements**

* All contracts with suppliers shall be monitored and reviewed. Contracts shall include appropriate provisions to ensure the security of information and systems.
* All third-party suppliers are required to sign the NDA before accessing the company's internal/confidential information.
* Relevant information security requirements must be established with each supplier.
* The requirements should specify:
  + What data is assessed by the supplier;
  + What data is held by the supplier;
  + When the supplier holds data;
  + Access methods;
  + Data retention statement when the contract ends.

## **Vendor Management**

* The Legal Counsel maintains a complete list of all vendors, associated risk rankings, and the date of the most recent evaluation.
* Multi-factor authentication should be enabled on all accounts for all vendors.

## **Vendor Compliance Monitoring**

* *[Company]* should monitor all vendors critical to operations regarding their compliance with information security standards by obtaining and reviewing copies of each vendor’s available security reports annually or sharing a security checklist for these needs.
* For more powerful suppliers than *[Company]* (for example, Amazon), it’s pointless to have controls and policies that the suppliers will not adhere to. So we rely on their standard policies, controls, independent third-party examination reports (ISO27001, SOC2, etc.), and agreements.
* With other suppliers, we develop more close working relationships where high-value information and assets are at risk, adding to our information assets in some (positive) way. This is likely to lead to improved working relationships, and therefore deliver better business results too.

# **Change, Review, and Update**

This policy shall be reviewed once every year unless the owner considers an earlier review necessary to ensure that the policy remains current. IT Manager shall exclusively perform changes to this policy.

# **Disciplinary Action**

Employees who violate this policy may face disciplinary consequences in proportion to their violation. Our management will determine how severe an employee’s offense is and take the appropriate action.

# **Responsibility**

The IT Manager is responsible for ensuring this policy is followed.

This policy shall be reviewed yearly or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

# Reference

* *[SOC 2 or ISO 27001 controls]*

# **Related Documents**

* Risk Management Policy