**<Your Company Logo>**

**Supplier Security Policy**

# ***Version Control Table***

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
| 1.0 | <Date> | <Author> | Issued |
| 1.0 | <Date> | <Author> | Reviewed |
| 1.0 | <Date> | <Author> | Approved |
| **1.0** | <Date> | <Author> | **Granted “FINAL” status** |

|  |  |
| --- | --- |
| **Date of Next Revision** | **<date>** |

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

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

# 

# ***Table of Contents***

[**The Path to Compliance 2**](#_htrkie77tuhx)

[**We'll guide you through, ensuring a smooth path to compliance: 2**](#_bor2nqthjwhg)

[**Need Expert Assistance? 2**](#_j1ad4z2lk78s)

[**Version Control Table 4**](#_arxqdy8knprl)

[**Table of Contents 5**](#_cj9vnfyr0ye6)

[**Purpose 6**](#_6rdebqtyz67)

[**Scope 6**](#_z4gzxs2rscp8)

[**Responsibilities 6**](#_ymrhyl6jj99x)

[**Policy 6**](#_rp1yfmi46axf)

[Supplier Risk Assessment 6](#_tzqdkfnf38k6)

[Screening 6](#_r98lr3prdh9p)

[Supplier agreements 6](#_akez5qro96wi)

[NDA 7](#_x6fn8hdi6ler)

[Supplier Management 7](#_vaugb696cm7b)

[Monitoring 7](#_uehwicbzif4w)

[Termination of agreements 7](#_kjzhwhc0xpm5)

[**Disciplinary actions 7**](#_oo4pebgvtuk2)

[**Change, Review, and Update 7**](#_5eyfoygex9zs)

[**Responsibility 8**](#_fxvzxllev4xj)

[**Reference 8**](#_n01zof837vbs)

[**Related Documents 8**](#_mi6e65mrklvd)

# 

# 

# Purpose

Supplier Security Policy describes the conditions of how to maintain the security of information when third parties are involved in the company’s internal operations.

# Scope

This policy applies to all suppliers who access the <Company> information or suppliers hosting the company’s information assets.

# Responsibilities

**ISMS Manager:**

* Manage supplier security process;
* Identify all third-parties in the company with COO;
* Monitor third-parties.

**COO:**

* Keep track of all contractual agreements and NDA with all third parties with ISMS Manager.

# Policy

## Supplier Risk Assessment

The risks associated with supplier management are described in the <Company> 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.

## Screening

Precise due diligence must be done before selecting a supplier using the risk-based approach.

## Supplier agreements

All contracts with suppliers shall be monitored and reviewed. Contracts shall include appropriate provisions to ensure the security of information and systems.

Relevant information security requirements must be established with each supplier.

Requirements include specifying (if applicable):

* What company data is to be processed by the supplier;
* Where and how the supplier stores data;
* The process of sanitization of storage media that is applied during the contract and will be applied at contract termination;
* Access method;
* Who within the supplier will be managing the risks for the delivery of the contract.

### NDA

All third parties are required to sign an NDA before accessing the company’s internal/confidential information.

## Supplier Management

The suppliers must be divided into 3 groups due to their access to critical information and assets and their criticality to the business.

|  |  |  |
| --- | --- | --- |
| **Priority** | **Category** | **Description** |
| Priority 1 | High | The critical infrastructure is hosted in the supplier environment. |
| Priority 2 | Medium | Suppliers provide the tools necessary for successful business operations. |
| Priority 3 | Low | The supplier doesn’t have a lot of impact on the company, so it doesn’t affect the continuity of service. |

## Monitoring

The third parties are annually monitored if they meet security service level agreements.

## Termination of agreements

After the termination of the agreement, all assets must be returned, and access rights are removed.

# Disciplinary actions

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

# 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. Changes to this policy shall be exclusively performed by the ISMS Manager and approved by the ISMS Committee.

# Responsibility

This is the responsibility of the ISMS Manager to maintain and make sure everyone is aware of this policy.

# Reference

* ISO 27001 Annex A.15.1.1 Information Security Policy for Supplier Relationships
* ISO 27001 Annex A.15.1.2 Addressing Security Within Supplier Agreements
* ISO 27001 Annex A.15.1.3 Information & Communication Technology Supply Chain
* ISO 27001 Annex A.15.2.1 Monitoring & Review of Supplier Services
* ISO 27001 Annex A.15.2.2 Managing Changes to Supplier Services

# Related Documents

* <Company> Business Continuity Plan