[organization logo]

[organization name]

**SUPPLIER SECURITY POLICY**

|  |  |
| --- | --- |
| Code: |  |
| Version: |  |
| Date of version: |  |
| Created by: |  |
| Approved by: |  |
| Confidentiality level: |  |

**Change history**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **Version** | **Created by** | **Description of change** |
| YYYY-MM-DD | 0.1 | Dejan Kosutic | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc415652342)

[2. Reference documents 3](#_Toc415652343)

[3. Relationship with suppliers and partners 3](#_Toc415652344)

[3.1. Identifying the risks 3](#_Toc415652345)

[3.2. Screening 3](#_Toc415652346)

[3.3. Contracts 3](#_Toc415652347)

[3.4. Training and awareness 4](#_Toc415652348)

[3.5. Monitoring and review 4](#_Toc415652349)

[3.6. Changes or termination of supplier services 4](#_Toc415652350)

[3.7. Removal of access rights / return of assets 4](#_Toc415652351)

[4. Managing records kept on the basis of this document 4](#_Toc415652352)

[5. Validity and document management 5](#_Toc415652353)

[6. Appendices 5](#_Toc415652354)

# Purpose, scope and users

The purpose of this document is to define the rules for relationship with suppliers and partners.

This document is applied to all suppliers and partners who have the ability to influence confidentiality, integrity and availability of [organization name]'s sensitive information.

Users of this document are top management and persons responsible for suppliers and partners in [organization name].

# Reference documents

* ISO/IEC 27001 standard, clauses A.7.1.1, A.7.1.2, A.7.2.2, A.8.1.4, A.14.2.7, A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
* Risk Assessment and Risk Treatment Methodology
* Risk Assessment and Risk Treatment Report
* Access Control Policy
* Confidentiality Statement

# Relationship with suppliers and partners

## Identifying the risks

Security risks related to suppliers and partners are identified during the risk assessment process, as defined in the Risk Assessment and Risk Treatment Methodology. During the risk assessment, special care must be taken to identify risks related to information and communication technology, as well as risks related to product supply chain.

[job title] decides whether it is necessary to additionally assess risks related to individual suppliers or partners.

## Screening

[job title] decides whether it is necessary to perform background verification checks for individual suppliers and partners, and if yes – which methods must be used.

## Contracts

[job title] is responsible for deciding which security clauses will be included in the contract with supplier or partner. Such decision must be based on the results of risk assessment and treatment; however, the clauses which stipulate confidentiality and return of assets after the termination of the agreement are mandatory. Further, the contracts must ensure reliable delivery of the products and services, which is particularly important with cloud service providers.

A list of suggested clauses is given in appendix Security Clauses for Suppliers and Partners.

[job title] will decide whether the individual employees of the supplier/partner will have to sign the Confidentiality Statements when working for [organization name].

[job title] decides who will be the contract owner for each contract – i.e. who will be responsible for a particular supplier or partner.

## Training and awareness

Contract owner decides which employees of suppliers and partners need security awareness and training.

[job title] is responsible to provide all the training and raising of awareness of those employees.

## Monitoring and review

Contract owner must regularly check and monitor the level of service and fulfillment of security clauses by suppliers or partners, reports and records created by the supplier/partner, as well as audit the supplier or partner at least once a year.

All the security incidents related to the partner’s/supplier’s job must be forwarded immediately to [job title].

## Changes or termination of supplier services

Contract owner proposes changes or termination of the contract, and [job title] makes the final decision. If necessary, [job title] will perform a new risk assessment before the changes are accepted.

## Removal of access rights / return of assets

When the contract is changed or terminated, the access rights for employees of partners/suppliers must be removed according to the Access Control Policy.

Further, when the contract is changed or terminated, the contract owner must make sure all the equipment, software or information in electronic or paper form is returned.

# Managing records kept on the basis of this document

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Record name | Storage location | Person responsible for storage | Controls for record protection | Retention time |
| Contracts with suppliers and partners | [cabinet, safe, or similar] | [job title] | Only [job title] has access to the [cabinet, safe] | 5 years after the termination of the contract |
| Records of monitoring and review | Contract owner’s computer | Contract owner | Only the contract owner can access those records | 3 years |

# Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must check and, if necessary, update the document at least once a year.

When evaluating the effectiveness and adequacy of this document, the following criteria need to be considered:

* number and significance of incidents arising from suppliers’ and partners’ activities
* number of contracts where the contract owner is not defined

# Appendices

* Security Clauses for Suppliers and Partners

[job title]

[name]

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

[signature]