[Organization logo]

[Organization name]

Commented [270011]: All fields in this document marked by square brackets [ ] must be filled in.

SUPPLIER SECURITY POLICY

Commented [270012]: To learn how to select the security clauses, read these articles:

- 6-step process for handling supplier security according to ISO 27001 https://advisera.com/27001academy/blog/2014/06/30/6-step-process-for-handling-supplier-security-according-to-iso-27001/
- Which security clauses to use for supplier agreements? https://advisera.com/27001academy/blog/2017/06/19/which-security-clauses-to-use-for-supplier-agreements/

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

Commented [270013]: The document coding system should be in line with the organization's existing system for document coding; in case such a system is not in place, this line may be deleted.

Change history

Date	Version	Created by	Description of change
	0.1	27001Academy	Basic document outline

Table of contents

1. Purpose, scope and users

The purpose of this document is to define the rules for relationships with suppliers and partners, including the providers of cloud services.

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].

Commented [270014]: This high-level policy is written according to ISO 27001 Annex A control A.5.19, defining requirements for mitigating the risks associated with supplier's access to the organization's assets, and does not describe detailed practices to be followed.

If your organization wants to define detailed practices to be followed by suppliers, please see as an example the document IT Security Policy.

Commented [270015]: Include the name of your organization.

Commented [270016]: Include the name of your organization.

2. Reference documents

- ISO/IEC 27001 standard, clauses A.5.7, A.5.11, A.5.19, A.5.20, A.5.21, A.5.22, A.5.23, A.6.1, A.6.2, A.6.3 and A.8.30
- Risk Assessment and Risk Treatment Methodology
- Risk Assessment and Risk Treatment Report
- Access Control Policy
- Confidentiality Statement

Commented [27A7]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "06_Risk_Assessment_and_Risk_Treatment".

Commented [27A8]: You can find a template for this document in the ISO 27001 Documentation Toolkit folder "06_Risk_Assessment_and_Risk_Treatment".

3. Relationship with suppliers and partners

3.1. Identifying the risks

Commented [270019]: Delete this section if control A.5.19 is found not applicable.

[redacted]
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.

[redacted]

Commented [2700110]: Delete this section if control A.6.1 is found not applicable.

[redacted]

Commented [2700111]: E.g. experience of their other clients, credit history, onsite audit, etc.

3.3. Contracts

Commented [2700112]: Delete this section if control A.5.20 is found not applicable.

[Job title] is responsible for deciding which security clauses will be included in the contract with a supplier or partner. Such decision must be based on the results of risk assessment and treatment.

The following clauses are mandatory in the agreements with suppliers:

- [redacted]
- [redacted]

- How the information about threats is communicated between the supplier and the buyer
- [redacted]

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

[redacted]

a particular supplier or partner.

3.4. Training and awareness

[redacted]

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

[redacted]

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

3.6. 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.

3.7. Removal of access rights / return of assets

[redacted]

4. Managing records kept on the basis of this document

Record name	Storage location	Person responsible for storage	Controls for record protection	Retention time

Commented [2700113]: Include the name of your organization.

Commented [2700114]: Delete this section if control A.6.3 is found not applicable.

Commented [2700115]: You can suggest this training to the supplier to raise awareness of their employees and track their knowledge: https://training.advisera.com/awareness-session/security-awareness-training/

Commented [2700116]: Delete this section if control A.5.22 is found not applicable.

Commented [2700117]: [redacted]

Commented [2700118]: On-site audits should be performed only if there are high risks related to a supplier/partner.

Commented [2700119]: To learn more about this topic, read this article:

How to perform an ISO 27001 second-party audit of an outsourced supplier https://advisera.com/27001academy/blog/2017/10/10/how-to-perform-an-iso-27001-second-party-audit-of-an-outsourced-supplier/

Commented [2700120]: Adapt as required, i.e. based on assessed risks.

Commented [2700121]: This is usually the Security Officer.

Commented [2700122]: Delete this section if control A.5.22 is found not applicable.

Commented [2700123]: Delete this paragraph if control A.5.18 is found not applicable.

Commented [2700124]: Delete this section if control A.5.11 is found not applicable.

Commented [2700125]: Alter these records to match what you already have in your company. If you do not have similar records, you can create new ones in the format that suits you best.

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

Commented [2700126]: Adapt this period according to your specific needs.

5. 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.

Commented [2700127]: This is only a recommendation; adjust frequency as appropriate.

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

- [illegible]
- [illegible]

[job title]
[name]

[signature]

Commented [2700128]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed.