[organization logo]

[organization name]

Comment [DK1]: All fields in this document marked by square brackets [ ] must be filled in.

SUPPLIER SECURITY POLICY

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

Comment [DK2]: 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
01/10/2013	0.1	Dejan Kosutic	Basic document outline

Table of contents

1. PURPOSE, SCOPE AND USERS 3

2. REFERENCE DOCUMENTS 3

3. RELATIONSHIP WITH SUPPLIERS AND PARTNERS 3

3.1. IDENTIFYING THE RISKS 3
3.2. SCREENING 3
3.3. CONTRACTS 3
3.4. TRAINING AND AWARENESS 4
3.5. MONITORING AND REVIEW 4
3.6. CHANGES OR TERMINATION OF SUPPLIER SERVICES 4
3.7. REMOVAL OF ACCESS RIGHTS / RETURN OF ASSETS 4

4. MANAGING RECORDS KEPT ON THE BASIS OF THIS DOCUMENT 4

5. VALIDITY AND DOCUMENT MANAGEMENT 5

6. APPENDICES 5

1. 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].

2. 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

3. Relationship with suppliers and partners

3.1. Identifying the risks

Comment [DK3]: Delete this section if control A.15.1.1 is found not applicable

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.

3.2. Screening

Comment [DK4]: Delete this section if control A.7.1.1 is found not applicable

[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.

Comment [DK5]: E.g. experience of their other clients, credit history, onsite audit, etc.

3.3. Contracts

Comment [DK6]: Delete this section if control A.15.1.2 is found not applicable

[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.

3.4. 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.

3.5. 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].

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

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.

Comment [DK7]: Delete this section if control A.7.2.2 is found not applicable

Comment [DK8]: Delete this section if control A.15.2.1 is found not applicable

Comment [DK9]: If necessary, tables may be prepared prescribing in more detail which elements must be monitored and how frequently

Comment [DK10]: On-site audits should be performed only if there are high risks related to a supplier/partner

Comment [DK11]: Adapt as required, i.e. based on assessed risks

Comment [DK12]: This is usually the Security Officer

Comment [DK13]: Delete this section if control A.15.2.2 is found not applicable

Comment [DK14]: Delete this paragraph if control A.9.2.6 is found not applicable

Comment [DK15]: Delete this section if control A.8.1.4 is found not applicable

4. 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	Contract owner's	Contract owner	Only the contract owner	3 years

Comment [DK16]: Adapt this period according to your specific needs

review	computer		can access those records	

5. Validity and document management

This document is valid as of [date].

The owner of this document is [job title], who must [illegible] at least once a year.

Comment [DK17]: 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:

- number and significance of [illegible]
- [illegible] contract owner is not defined

6. Appendices

- Security Clauses for Suppliers and Partners

[job title]
[name]

[signature]

Comment [DK18]: Only necessary if the Procedure for Document and Record Control prescribes that paper documents must be signed