\*\* FREE PREVIEW VERSION \*\*

[organization logo]

[organization name]

**STATEMENT OF APPLICABILITY**

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

**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](#_Toc368134451)

[2. Reference documents 3](#_Toc368134452)

[3. Applicability of controls 3](#_Toc368134453)

[4. Acceptance of Residual Risks 22](#_Toc368134454)

[5. Validity and document management 23](#_Toc368134456)

# Purpose, scope and users

The purpose of this document is to define which controls are appropriate to be implemented in [organization name], the objectives of these controls and how they are implemented, as well as to approve residual risks and formally approve the implementation of said controls.

This document includes all controls listed in Annex A of the ISO 27001 standard. Controls are applicable to the entire Information Security Management System (ISMS) scope.

Users of this document are all employees of [organization name] who have a role in the ISMS.

# Reference documents

* ISO/IEC 27001 standard, clause 6.1.3 d)
* Information Security Policy
* Risk Assessment and Risk Treatment Methodology
* Risk Assessment and Risk Treatment Report

# Applicability of controls

The following controls from ISO 27001 Annex A are applicable:

| ID | Controls according to ISO/IEC 27001 | Appli-cability (YES/NO) | Justification for selection/ non-selection | Control objectives | Implementation method | Status |
| --- | --- | --- | --- | --- | --- | --- |
| A.5 | Information security policies |  |  |  |  |  |
| A.5.1 | Management direction for information security |  |  |  |  |  |
| A.5.1.1 | Policies for information  security |  |  |  | All policies referred to below in this column |  |
| A.5.1.2 | Review of the policies  for information  security |  |  |  | Each policy has a designated owner who has to review the document at planned interval |  |
| A.6 | Organization of information security |  |  |  |  |  |
| A.6.1 | Internal organization |  |  |  |  |  |
| A.6.1.1 | Information security  roles and responsibilities |  |  |  | Responsibilities for information security are listed in various ISMS documents. If required, [job title] defines additional responsibilities |  |
| A.6.1.2 | Segregation of duties |  |  |  | Any activity that includes sensitive information is approved by one person and implemented by another |  |
| A.6.1.3 | Contact with authorities |  |  |  | [Business Continuity Strategy], [Incident Response Plan] |  |
| A.6.1.4 | Contact with special  interest groups |  |  |  | [job title] is responsible for monitoring [list names of interest groups and security forums] |  |
| A.6.1.5 | Information security  in project management |  |  |  | Project manager is required to include applicable information security rules in every project |  |
| A.6.2 | Mobile devices and teleworking |  |  |  |  |  |
| A.6.2.1 | Mobile device policy |  |  |  | [Acceptable Use Policy] / [Mobile Device and Teleworking Policy], [Bring Your Own Device (BYOD) Policy] |  |
| A.6.2.2 | Teleworking |  |  |  | [Acceptable Use Policy] / [Mobile Device and Teleworking Policy] |  |

\*\* END OF FREE PREVIEW \*\*

To download full version of this document click here: <http://www.iso27001standard.com/en/documentation/Statement-of-Applicability>