\*\* 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** |
| dd.mm.yyyy | 0.1 | EUGDPRAcademy | Basic document outline |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Table of contents**

[1. Purpose, scope and users 3](#_Toc114515676)

[2. Reference documents 3](#_Toc114515677)

[3. Applicability of controls 3](#_Toc114515678)

[4. Acceptance of Residual Risks 18](#_Toc114515679)

[5. Validity and document management 18](#_Toc114515680)

# Purpose, scope and users

The purpose of this document is to define which controls (safeguards) 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 and all personal data processing activities.

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
* DPIA Register

# Applicability of controls

The following controls from ISO 27001 Annex A are applicable:

| ID | Controls according to ISO/IEC 27001 | … | Justification for selection/ non-selection | … | … | Status |
| --- | --- | --- | --- | --- | --- | --- |
| A.5.1 | … |  |  |  | … |  |
| A.5.2 | Information security roles and responsibilities |  |  |  | … |  |
| A.5.3 | Segregation of duties |  |  |  | … |  |
| A.5.4 | … |  |  |  | … |  |
| A.5.5 | … |  |  |  | … |  |
| A.5.6 | Contact with special interest groups |  |  |  | … |  |
| A.8.32 | Change management | … |  |  | [Security Procedures for IT Department] / [Change Management Policy], [Secure Development Policy] |  |
| A.8.33 | Test information |  |  |  | [Secure Development Policy] |  |
| A.8.34 | Protection of information systems during audit testing |  |  |  | [Internal Audit Procedure] |  |

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

To download full version of this document click here: <https://advisera.com/27001academy/documentation/statement-of-applicability/>