**ISO/IEC 27001:2022 – STATEMENT OF APPLICABILITY (SOA)**

**DOCUMENT CONTROL**

|  |  |
| --- | --- |
| Document Title: | Statement of Applicability (SoA) |
| ISMS Reference: | ISMS-SOA-001 |
| Version: | 1.0 |
| Status: | Final |
| Date Created: | [Insert Date] |
| Last Reviewed: | [Insert Date] |
| Next Review Date: | [Insert Date – Typically Annual] |
| Document Owner: | Information Security Manager |
| Approved By: | Chief Information Security Officer (CISO) |

**PURPOSE**

The purpose of this document is to define and justify the applicability, implementation status, and control Commentary for each of the information security controls in **Annex A** of the ISO/IEC 27001:2022 standard. It supports risk treatment, demonstrates compliance, and links each control to organizational requirements, legal and contractual obligations, and identified risks.

**TABLE OF CONTENTS:**

[Scope of the Information Security Management System (ISMS) 2](#_Toc197189731)

[Risk Assessment Methodology Summary 2](#_Toc197189732)

[Control Applicability Matrix (Annex A) 2](#_Toc197189733)

[A.5 Organizational Controls 3](#_Toc197189734)

[A.6 People Controls 3](#_Toc197189735)

[A.7 Physical Controls 4](#_Toc197189736)

[A.8 Technological Controls 4](#_Toc197189737)

[Mapping to Legal, Regulatory, and Contractual Requirements 5](#_Toc197189738)

[Evidence Strategy 5](#_Toc197189739)

[Review & Maintenance 5](#_Toc197189740)

[Approval 5](#_Toc197189741)

## SCOPE OF THE INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

This SoA applies to the entire information security management system (ISMS) of:

**Organization:** [Company Name]  
**Scope Statement:** [Define ISMS boundaries — e.g., “The ISMS covers all information systems, people, and processes supporting the delivery of SaaS products to healthcare clients, including cloud infrastructure, application development, and customer support, operating from remote and corporate locations.”]

## Risk Assessment Methodology Summary

The organization uses a [qualitative/quantitative] risk assessment methodology based on asset-threat-vulnerability-risk models, consistent with ISO/IEC 27005. Each control is selected, excluded, or justified based on:

* Results from the risk assessment and risk treatment process
* Legal, regulatory, and contractual obligations
* Business and stakeholder requirements

A full risk assessment report is maintained separately (Ref: e.g. ISMS-RA-001).

## Control Applicability Matrix (Annex A)

This section lists all 93 Annex A controls organized by theme, and includes:

* Applicability (Yes/No)
* Implementation Status
* Justification (for non-application)
* Risk or legal requirement link
* Evidence type/source

### A.5 Organizational Controls

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Control ID** | **Control Title** | **Applicable** | **Implemented** | **Justification / Commentary** | **Risk or Obligation Link** | **Evidence** |
| A.5.1 | Policies for information security | Yes | Yes | Essential for ISMS governance | ISO Requirement | Policy Document (IS-001) |
| A.5.2 | Information security roles and responsibilities | Yes | Yes | Supports accountability across security domains | Organizational Governance | Org Chart, Job Descriptions |
| A.5.4 | Contact with authorities | Yes | Yes | Required for reporting incidents | Regulatory – GDPR, HIPAA | Contact List, Procedures |
| A.5.23 | Information security in project management | Yes | Yes | Mandatory to manage security early in projects | Risk from insecure design | Project Checklist |
| A.5.29 | Supplier relationships management | Yes | Yes | Needed due to cloud vendors and third-party dependencies | SOC 2, ISO, Vendor Risk | Contracts, Risk Register |

*Add remaining A.5 controls accordingly.*

### A.6 People Controls

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Control ID** | **Control Title** | **Applicable** | **Implemented** | **Justification / Commentary** | **Risk or Obligation Link** | **Evidence** |
| A.6.1 | Screening | Yes | Yes | Important to verify employee integrity | HR Policy, Insider Threat Risk | HR Files, Background Check Logs |
| A.6.3 | Termination or change of employment | Yes | Yes | Avoid unauthorized access post-employment | Insider Threat | HR Exit Checklist |

*Add remaining A.6 controls accordingly.*

### A.7 Physical Controls

*(Often limited or excluded in cloud-native orgs)*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Control ID** | **Control Title** | **Applicable** | **Implemented** | **Justification / Commentary** | **Risk or Obligation Link** | **Evidence** |
| A.7.4 | Physical security perimeter | No | No | Fully cloud-based with no owned, leased, or managed data centers | Not Applicable | N/A |
| A.7.5 | Physical Entry Controls | No | No | Fully remote workforce | Not Applicable | N/A |
| A.7.8 | Secure disposal or reuse of equipment | Yes | Yes | Disposal of laptops, phones with encryption | PII/PHI risk | Asset Disposal Log |
| A.7.9 | Removal of assets | No | No | No physical asset removal due to virtualized systems | Not Applicable | N/A |

### A.8 Technological Controls

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Control ID** | **Control Title** | **Applicable** | **Implemented** | **Justification / Commentary** | **Risk or Obligation Link** | **Evidence** |
| A.8.1 | User endpoint devices | Yes | Yes | Laptops used in remote/hybrid model | Endpoint Risk | MDM Reports |
| A.8.7 | Protection against malware | Yes | Yes | Prevent ransomware, phishing | Compliance, Security Risk | AV/EDR Logs |
| A.8.23 | Web filtering | Yes | Yes | Prevent access to malicious domains | Insider Risk, Zero Trust | DNS Filter Logs |

## Mapping to Legal, Regulatory, and Contractual Requirements

|  |  |
| --- | --- |
| **Requirement** | **Controls Addressed** |
| GDPR (EU 2016/679) | A.5.1, A.5.30, A.8.34, A.6.1, A.8.35 |
| HIPAA | A.5.2, A.5.12, A.8.1, A.8.28, A.6.3 |
| SOC 2 – Security/Availability | A.5.1, A.5.17, A.5.23, A.8.7, A.5.30 |
| ISO/IEC 27701 (if PIMS linked) | A.5.1, A.8.35, A.8.34 |

## Evidence Strategy

Each implemented control must be auditable through formal documentation or automated reporting. Evidence types include:

* **Policies & Procedures:** Stored in ISMS portal (e.g., Confluence)
* **System Logs & Reports:** Centralized in SIEM (e.g., Splunk, ELK)
* **Screenshots or Exports:** Screenshots of system settings (IAM, backups)
* **Configuration Baselines:** Infrastructure-as-Code (e.g., Terraform state files)
* **Training Records:** LMS completion logs

## Review & Maintenance

This SoA will be reviewed:

* At least **annually**
* After significant changes to the ISMS or organizational structure
* Following internal or external audit findings

## Approval

| **Name** | **Title** | **Signature** | **Date** |
| --- | --- | --- | --- |
| [CISO Name] | Chief Information Security Officer | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Date] |
| [ISMS Lead Name] | ISMS Manager | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | [Date] |