Statement of Applicability (SoA) Template

Document Control Information

- **Document Title:** Statement of Applicability
- **Document Version:** 1.0
- **Last Updated:** [DATE]
- **Document Owner:** [ROLE/NAME]
- **Approved By:** [ROLE/NAME]
- **Next Review Date:** [DATE]

1. Introduction

1.1 Purpose

This Statement of Applicability (SoA) identifies the controls from ISO 27001:2022 Annex A that are applicable to [ORGANIZATION NAME]'s Information Security Management System (ISMS). It provides justification for the inclusion or exclusion of controls and indicates their implementation status.

1.2 Scope

This SoA covers all information security controls within the defined scope of [ORGANIZATION NAME]'s ISMS as documented in [REFERENCE TO SCOPE DOCUMENT].

2. Control Implementation Status

The following table provides a comprehensive overview of all ISO 27001:2022 Annex A controls, their applicability to [ORGANIZATION NAME], implementation status, and justification.

Legend:

- **Applicable:** Yes/No
- **Implemented:** Yes/Partially/No/Planned
- **Justification:** Reason for inclusion or exclusion of the control
- **Implementation Evidence:** Reference to documents, procedures, or systems that demonstrate implementation

3. Organizational Controls (A.5)

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
A.5.1	Policies for information security	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.2	Information security roles and responsibilities	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.3	Segregation of duties	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.4	Management responsibilities	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.5	Contact with authorities	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.6	Contact with special interest groups	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.7	Threat intelligence	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.8	Information security in project management	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.9	Inventory of information and other associated assets	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.10	Acceptable use of information	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
	and other associated assets				
A.5.11	Return of assets	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.12	Classification of information	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.13	Labelling of information	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.14	Information transfer	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.15	Access control	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.16	Identity management	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.17	Authentication information	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.18	Access rights	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.19	Information security in supplier relationships	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.20	Addressing information security within supplier agreements	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.21	Managing information security in the	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
	ICT supply chain				
A.5.22	Monitoring, review and change management of supplier services	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.23	Information security for use of cloud services	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.24	Information security incident management planning and preparation	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.25	Assessment and decision on information security events	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.26	Response to information security incidents	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.27	Learning from information security incidents	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.28	Collection of evidence	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.29		[Yes/No]	[Status]	[Justification]	

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
	Information security during disruption				[Evidence Reference]
A.5.30	ICT readiness for business continuity	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.31	Legal, statutory, regulatory and contractual requirements	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.32	Intellectual property rights	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.33	Protection of records	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.34	Privacy and protection of PII	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.35	Independent review of information security	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.36	Compliance with policies, rules and standards for information security	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.5.37	Documented operating procedures	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

4. People Controls (A.6)

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
A.6.1	Screening	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.6.2	Terms and conditions of employment	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.6.3	Information security awareness, education and training	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.6.4	Disciplinary process	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.6.5	Responsibilities after termination or change of employment	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.6.6	Confidentiality or non-disclosure agreements	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.6.7	Remote working	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.6.8	Information security event reporting	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

5. Physical Controls (A.7)

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
A.7.1	Physical security perimeters	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.2	Physical entry	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.3	Securing offices, rooms and facilities	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.4	Physical security monitoring	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.5	Protecting against physical and environmental threats	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.6	Working in secure areas	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.7	Clear desk and clear screen	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.8	Equipment siting and protection	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.9	Security of assets off-premises	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.10	Storage media	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
A.7.11	Supporting utilities	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.12	Cabling security	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.13	Equipment maintenance	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.7.14	Secure disposal or re-use of equipment	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

6. Technological Controls (A.8)

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
A.8.1	User endpoint devices	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.2	Privileged access rights	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.3	Information access restriction	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.4	Access to source code	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.5	Secure authentication	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.6	Capacity management	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.7		[Yes/No]	[Status]	[Justification]	[Evidence Reference]

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
	Protection against malware				
A.8.8	Management of technical vulnerabilities	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.9	Configuration management	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.10	Information deletion	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.11	Data masking	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.12	Data leakage prevention	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.13	Information backup	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.14	Redundancy of information processing facilities	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.15	Logging	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.16	Monitoring activities	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.17	Clock synchronization	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.18	Use of privileged utility programs	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
A.8.19	Installation of software on operational systems	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.20	Networks security	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.21	Security of network services	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.22	Segregation of networks	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.23	Web filtering	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.24	Use of cryptography	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.25	Secure development life cycle	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.26	Application security requirements	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.27	Secure system architecture and engineering principles	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.28	Secure coding	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.29	Security testing in development and acceptance	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

Control ID	Control Name	Applicable	Implemented	Justification	Implementation Evidence
A.8.30	Outsourced development	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.31	Separation of development, test and production environments	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.32	Change management	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.33	Test information	[Yes/No]	[Status]	[Justification]	[Evidence Reference]
A.8.34	Protection of information systems during audit testing	[Yes/No]	[Status]	[Justification]	[Evidence Reference]

7. Summary of Control Implementation

7.1 Control Implementation Statistics

- Total number of controls: 93
- Number of applicable controls: [NUMBER]
- Number of implemented controls: [NUMBER]
- Number of partially implemented controls: [NUMBER]
- Number of planned controls: [NUMBER]
- Number of not implemented controls: [NUMBER]
- Number of not applicable controls: [NUMBER]

7.2 Implementation Plan for Outstanding Controls

[PROVIDE DETAILS OF IMPLEMENTATION PLANS FOR CONTROLS THAT ARE NOT YET FULLY IMPLEMENTED]

8. Approval

This Statement of Applicability has been reviewed and approved by:

Name: _____ Position: _____ Date: _____ Signature: _____