SoA_Extern_English

Table of contents

Statement of Applicability (SoA)....3
Changehistory....3
1. Purpose, Area of application and users....3
2. Measures from Appendix A....4

Statement of Applicability (SoA)

Version:	1.1
Date of the version:	08.06.2026
Created by:	Berit Wiedner
Approved by:	Ingmar Eveslage
Confidentiality level:	Public

Changehistory

Date of	**Version**	**Created by**	**Description of the change**
28.4.2026	1.0	BW	First Version of the SoA
08.06.2026	1.1	BW	Added justification column

1. Purpose, Area of application and users

The document contains a list of all measures in Annex A of ISO/IEC 27001. The measures are to be applied to the entire scope of the ISMS. Essential guidelines of the ISMS are created to fulfill the measures of Annex A. In addition, the measures are taken into account as part of risk management.

Users of the document are all employees of the organization with a function in the ISMS.

2. Measures from Appendix A

Control ID	Measures according to ISO/IEC 27001	Applicability (YES/ NO)	Justification	Implementation status
5.1	Information security policy	YES	Official, legalor contractual requirement	Implemented
5.2	Information security roles and responsibilities	YES	Official, legalor contractual requirement	Implemented
5.3	Separation of duties	YES	Risk management	Implemented
5.4	Responsibilities of the management	YES	Official, legalor contractual requirement	Implemented
5.5	Contact with authorities	YES	Official, legalor contractual requirement	Implemented
5.6	Contact with special interest group	YES	Official, legalor contractual requirement	Implemented
5.7	Threat analysis	YES	Risk management	Implemented
5.8	Information security in project management	YES	Risk management	Implemented
5.9	Inventory of values	YES	Business requirement	Implemented
5.10	Permitted use of values	YES	Business requirement	Implemented
5.11	Return of values	YES	Business requirement	Implemented

5.12	Classification of information	YES	Risk management	Implemented
5.13	Labeling of information	YES	Risk management	Implemented
5.14	Information transfer	YES	Risk management	Implemented
5.15	Access control	YES	Risk management	Implemented
5.16	User administration	YES	Risk management	Implemented
5.17	Authentication information	YES	Risk management	Implemented
5.18	Access rights	YES	Risk management	Implemented
5.19	Information security for supplier relationships	YES	Risk management	Implemented
5.20	Treatment of security in supplier agreements	YES	Risk management	Implemented
5.21	Supply chain for information and communication technology	YES	Risk management	Implemented
5.22	Monitoring and verification of supplier services	YES	Business requirement	Implemented

5.23	Information security for the use of cloud services	YES	Risk management	Implemented
5.24	Planning and preparation of information security incident management	YES	Risk management	Implemented
5.25	Assessment of and decision on information security incidents	YES	Risk management	Implemented
5.26	Response to information security incidents	YES	Risk management	Implemented
5.27	Lessons learned from information security incidents	YES	Risk management	Implemented
5.28	Collecting evidence	YES	Official, legalor contractual requirement	Implemented
5.29	Information security during interruptions	YES	Official, legalor contractual requirement	Implemented
5.30	ICT readiness for business continuity	YES	Official, legalor contractual requirement	Implemented
5.31	Legal, regulatory, self-imposed or contractual requirements	YES	Official, legalor contractual requirement	Implemented
5.32	Intellectual property rights	YES	Official, legalor contractual requirement	Implemented

5.33	Protection of records	YES	Official, legal or contractual requirement, risk management	Implemented
5.34	Privacy and protection of personal information	YES	Official, legalOr contractual requirement	Implemented
5.35	Independent review of information security	YES	Official, legalOr contractual requirement	Implemented
5.36	Compliance with guidelines, rules and standards for information security	YES	Official, legalOr contractual requirement	Implemented
5.37	Documented operating procedures	YES	Business requirement	Implemented
6.1	Security check	YES	Official, legalor contractual requirement	Implemented
6.2	Employment and contractual conditions	YES	Official, legalor contractual requirement	Implemented
6.3	Information security awareness, education and training	YES	Risk management	Implemented
6.4	Regulatory process	YES	Official, legalor contractual requirement	Implemented

6.5	Responsibilities upon termination or change of employment	YES	Official, legalor contractual requirement	Implemented
6.6	Confidentiality or non-disclosure agreements	YES	Official, legalor contractual requirement, risk management	Implemented
6.7	Teleworking	YES	Risk management	Implemented
6.8	Reporting of information security incidents	YES	Risk management	Implemented
7.1	Physical security perimeter	YES	Risk management	Implemented
7.2	Physical access control	YES	Risk management	implemented
7.3	Securing offices, rooms and facilities	YES	Risk management	Implemented
7.4	Physical security monitoring	YES	Risk management	Implemented
7.5	Protection against external and environmental threats	YES	Official, legalor contractual requirement	implemented
7.6	Working in secure areas	YES	Risk management	Implemented
7.7	Policy for a tidy working environment and screen locks	YES	Business requirement	Implemented

7.8	Placement and protection of devices and equipment	YES	Business requirement	Implemented
7.9	Safety of devices, equipment and assets outside the premises	YES	Risk management	Implemented
7.10	Removable disk	YES	Risk Management	Implemented
7.11	Utilities	YES	Official, legalor contractual requirement	Implemented
7.12	Safety of the cabling	YES	Official, legalor contractual requirement	Implemented
7.13	Maintenance of devices and equipment	YES	Official, legalor contractual requirement	Implemented
7.14	Safe disposal or reuse of	YES	Official, legalor contractual requirement	Implemented
8.1	User terminals	YES	Risk management	Implemented
8.2	Management of privileged access rights	YES	Risk management	Implemented
8.3	Information access restriction	YES	Risk management	Implemented
8.4	Access control for source code of programs	YES	Risk management	Implemented
8.5	Secure login procedure	YES	Risk management	Implemented

8.6	Capacity control	YES	Official, legal or contractual requirement	Implemented
8.7	Measures against malware	YES	Risk management	Implemented
8.8	Handling of technical vulnerabilities	YES	Risk management	Implemented
8.9	Configuration management	YES	Business requirement	Implemented
8.10	Deletion of information	YES	Official, legalor contractual requirement	Implemented
8.11	Masking of data	YES	Official, legalor contractual requirement	Implemented
8.12	Prevention of data loss	YES	Risk management	Implemented
8.13	Securing information	YES	Risk management	Implemented
8.14	Availability of information processing facilities	YES	Official, legalor contractual requirement	Implemented
8.15	Event logging	YES	Risk management	Implemented
8.16	Monitoring activities	YES	Risk management	Implemented
8.17	Clock synchronization	YES	Risk management	Implemented
8.18	Use of aid programs with privileged rights	YES	Risk management	Implemented

8.19	Installation of software on systems in operation	YES	Business requirement	Implemented
8.20	Network control measures	YES	Risk management	Implemented
8.21	Security of network services	YES	Risk management	Implemented
8.22	Separation in networks	YES	Risk management	Implemented
8.23	Web filtering	YES	Risk management	Implemented
8.24	Use of cryptography	YES	Risk management	Implemented
8.25	Secure development life cycle	YES	Risk management	Implemented
8.26	Securing application services	YES	Risk management	Implemented
8.27	Secure system architecture and technical principles	YES	Risk management	Implemented
8.28	Safe development	YES	Risk management	Implemented
8.29	Safety tests in development and acceptance	YES	Risk management	Implemented
8.30	Outsourced development	YES	Risk management	implemented

8.31	Separation of development, test and operating environments	YES	Risk management	Implemented
8.32	Change management	YES	Business requirement	Implemented
8.33	Test data	YES	Risk management	Implemented
8.34	Measures for audits of information systems	YES	Official, legalor contractual requirement	Implemented