



IX TECHNOLOGIES

ISMS

STATEMENT OF APPLICABILITY

ISO/IEC 27001:2022/Amd.1:2024(en)

Version:	1.0
Date:	2025-02-05
Valid until:	
Confidentiality:	Low

ix Technologies B.V.

Westvest 41
2611 AZ Delft
The Netherlands

1 VERSION AND REVISION HISTORY

This description of the way leadership and support of the ISMS of Ix Technologies is implemented is subject to version control to ensure that all changes are properly tracked and documented. The table below outlines the version history and any revisions made to the document.

Version	Date	Description
0.8	2025-01-09	First draft
0.9	2025-02-03	First version after review
1.0	2025-02-05	Update of control applicability based on internal audit feedback

2 SCOPE

The scope of the ISMS of ix technologies is defined as follows:

Information security related to all activities for development, maintenance, hosting and support of specialized, custom software applications for desktop, mobile and web, whereby hosting is outsourced.

3 CONTROLS

For each control in Annex A of ISO27001, the table below describes whether it is applicable given specific risks that are of importance to Ix technologies. If applicable, it describes how the control is implemented (containing references to other documents if any).

#	Control	Description	Appl?	Legal	SLA	Risk
5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, and published.	Yes	•	•	•
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	Yes			•
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	Yes			•
5.4	Management responsibilities	Management shall require all personnel to apply information security policies and procedures of the organization.	Yes			•
5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	Yes			•
5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or professional associations.	Yes			•
5.7	Threat intelligence	Information relating to information security threats shall be collected and analyzed to produce threat intelligence.	Yes			•
5.8	Information security in project management	Information security shall be integrated into project management.	Yes			•
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets shall be developed and maintained.	Yes			•
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use of information and other associated assets shall be identified and implemented.	Yes			•
5.11	Return of assets	Personnel shall return all the organization's assets upon change or termination of employment, contract,	Yes			•
5.12	Classification of information	Information shall be classified according to the organization's confidentiality, integrity, and availability needs.	Yes			•
5.13	Labelling of information	Procedures for information labelling shall align with the adopted classification scheme.	Yes			•

#	Control	Description	Appl?	Legal	SLA	Risk
5.14	Information transfer	Transfer rules and agreements should be in place for all transfer facilities between parties.	Yes		•	•
5.15	Access control	Rules for physical and logical access to information should be established based on business needs.	Yes			•
5.16	Identity management	The full lifecycle of identities shall be managed.	Yes			•
5.17	Authentication information	Authentication information should be managed and handled securely within the organization.	Yes			•
5.18	Access rights	Rights to information and assets should be provisioned, reviewed, and removed as necessary.	Yes			•
5.19	Information security in supplier relationships	Processes for managing supplier-related security risks should be defined and implemented.	Yes			•
5.20	Addressing information security in agreements	Relevant security requirements should be agreed with suppliers.	Yes			•
5.21	Managing ICT supply chain security	Processes should address risks related to ICT products and services in the supply chain.	Yes			•
5.22	Monitoring and change in supplier services	Regular monitoring and management of supplier security practices are required.	Yes			•
5.23	Information security for cloud services	Acquisition, use, and exit from cloud services should comply with security requirements.	Yes			•
5.24	Incident management planning	Organizations should prepare for incident management by defining processes, roles, and responsibilities.	Yes	•	•	•
5.25	Assessment and decision on information security events	The organization shall assess information security events and decide if they are to be categorized as information security incidents.	Yes	•	•	•
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Yes	•	•	•
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve information security controls.	Yes	•	•	•
5.28	Collection of evidence	The organization shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security events.	Yes	•	•	•

#	Control	Description	Appl?	Legal	SLA	Risk
5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Yes		•	•
5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.	Yes			•
5.31	Legal, statutory, regulatory, and contractual requirements	Relevant legal, statutory, regulatory, and contractual requirements for information security shall be identified, documented, and kept up to date.	Yes	•	•	•
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Yes	•	•	•
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access, and unauthorized release.	Yes			•
5.34	Privacy and protection of personally identifiable information (PII)	The organization shall identify and meet requirements regarding the preservation of privacy and protection of PII in accordance with applicable laws and regulations.	Yes	•	•	•
5.35	Independent review of information security	The organization's approach to managing information security shall be reviewed independently at planned intervals or when significant changes occur.	Yes			•
5.36	Compliance with policies, rules, and standards for information security	Compliance with the organization's information security policies, rules, and standards shall be regularly reviewed.	Yes			•
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Yes			•
6.1	Screening	Background verification checks on candidates shall be carried out prior to joining the organization and on an ongoing basis, considering applicable laws, ethics, and business requirements.	Yes	•		•
6.2	Terms and conditions of employment	Employment agreements shall state personnel's and the organization's responsibilities for information security.	Yes			•
6.3	Information security awareness, education, and training	Personnel of the organization and relevant parties shall receive appropriate information security awareness, education, and regular updates of the organization's policies.	Yes			•

#	Control	Description	Appl?	Legal	SLA	Risk
6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to address violations of the information security policy.	Yes			•
6.5	Responsibilities after termination or change of employment	Security responsibilities and duties valid after termination or employment changes shall be defined, enforced, and communicated.	Yes			•
6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements shall reflect the organization's information protection needs and be regularly reviewed and signed by relevant parties.	Yes		•	•
6.7	Remote working	Security measures shall protect information accessed, processed, or stored remotely outside the organization's premises.	Yes			•
6.8	Information security event reporting	The organization shall provide mechanisms for personnel to report observed or suspected information security events promptly.	Yes	•	•	•
7.1	Physical security perimeters	Security perimeters shall be defined to protect areas containing information and other assets.	Yes			•
7.2	Physical entry	Secure areas shall have appropriate entry controls and access points.	Yes			•
7.3	Securing offices, rooms, and facilities	Physical security for offices, rooms, and facilities shall be designed and implemented.	Yes			•
7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Yes			•
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional threats to infrastructure, shall be designed and implemented.	Yes			•
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Yes			•
7.7	Clear desk and clear screen	Clear desk and screen rules for papers and removable storage media shall be defined and enforced.	Yes			•
7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Yes			•
7.9	Security of assets off-premises	Off-site assets shall be protected.	Yes			•
7.10	Storage media	Storage media shall be managed through acquisition, use, transportation,	Yes			•

#	Control	Description	Appl?	Legal	SLA	Risk
		and disposal per the classification scheme.				
7.11	Supporting utilities	Information processing facilities shall be protected from disruptions caused by utility failures.	Yes			•
7.12	Cabling security	Cables carrying power, data, or services shall be protected from interception or damage.	Yes			•
7.13	Equipment maintenance	Equipment shall be maintained to ensure availability, integrity, and confidentiality of information.	Yes			•
7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be verified to ensure that any sensitive data and licensed software has been removed or security overwritten prior to disposal or re-use.	Yes			•
8.1	User endpoint devices	Information on or accessible via endpoint devices shall be protected.	Yes			•
8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	Yes			•
8.3	Information access restriction	Access to information shall be restricted per the topic-specific policy.	Yes			•
8.4	Access to source code	Read and write access to source code, development tools, and libraries shall be appropriately managed.	Yes			•
8.5	Secure authentication	Secure authentication technologies and procedures shall be implemented based on information access restrictions and the topic-specific policy on access control.	Yes			•
8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	Yes			•
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	Yes			•
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, and the organization's exposure to these vulnerabilities shall be evaluated with appropriate measures taken.	Yes			•
8.9	Configuration management	Configurations, including security configurations of hardware, software, services, and networks, shall be established, documented, implemented, monitored, and reviewed.	Yes			•
8.10	Information deletion	Information stored in systems, devices, or storage media shall be deleted when no longer required.	Yes			•

#	Control	Description	Appl?	Legal	SLA	Risk
8.11	Data masking	Data masking shall be used in accordance with the organization's policies, access control, and applicable legislation.	Yes			•
8.12	Data leakage prevention	Measures shall be applied to systems, networks, and devices to prevent leakage of sensitive information.	Yes			•
8.13	Information backup	Backup copies of information, software, and systems shall be maintained and regularly tested according to the organization's backup policy.	Yes		•	•
8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes			•
8.15	Logging	Logs that record activities, exceptions, faults, and other relevant events shall be produced, stored, protected, and analyzed.	Yes			•
8.16	Monitoring activities	Networks, systems, and applications shall be monitored for anomalous behavior, with appropriate actions taken to address potential security incidents.	Yes			•
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	Yes			•
8.18	Use of privileged utility programs	The use of utility programs capable of overriding system and application controls shall be restricted and tightly controlled.	Yes			•
8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	Yes			•
8.20	Networks security	Networks and network devices shall be secured, managed, and controlled to protect information in systems and applications.	Yes			•
8.21	Security of network services	Security mechanisms, service levels, and requirements of network services shall be identified, implemented, and monitored.	Yes			•
8.22	Segregation of networks	Groups of information services, users, and systems shall be segregated in the organization's networks.	Yes			•
8.23	Web filtering	Access to external websites shall be managed to reduce exposure to malicious content.	Yes			•
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic	Yes			•

#	Control	Description	Appl?	Legal	SLA	Risk
		key management, shall be defined and implemented.				
8.25	Secure development life cycle	Rules for secure development of software and systems shall be established and applied.	Yes			•
8.26	Application security requirements	Information security requirements shall be identified, specified, and approved for developing or acquiring applications.	Yes			•
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained, and applied to system development activities.	Yes			•
8.28	Secure coding	Secure coding principles shall be applied to software development.	Yes			•
8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development lifecycle.	Yes			•
8.30	Outsourced development	The organization shall direct, monitor, and review activities related to outsourced system development.	Yes			•
8.31	Separation of development, test, and production environments	Development, testing, and production environments shall be separated and secured.	Yes			•
8.32	Change management	Changes to information processing facilities and systems shall be subject to change management procedures.	Yes			•
8.33	Test information	Test information shall be appropriately selected, protected, and managed.	Yes			•
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving the assessment of operational systems shall be planned and agreed upon between the tester and appropriate management.	Yes			•