

ISMS ISO 27001 Statement of Applicability

Purpose

This document presents an ISO 27001 Statement of Applicability, listing the necessary controls as required by Annex A in the ISO/IEC 27001:2022 standard.

Document identification

This document was prepared in the following context.

Issuing organisation*	ebadu.pl sp. z o. o.
Context*	ISMS

The content of this document is the intellectual property of the ebadu.pl sp. z o.o. organization and is subject to legal protection.

Referenced documents

There are the following documents referenced.

Title	Comment
ISMS ISO/IEC 27001:2022	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements

Responsibility

The table below presents the RACI model for this document.

Role	Role name	Person
Responsible People or stakeholders who work on the document	ISMS Information Security Officer	Tomasz Puk
Accountable* A person who is the owner of the document	ISMS Information Security Officer	Tomasz Puk
Consulted People who are consulted on the document in its preparation	N/A	N/A
Informed People who are informed about the final document	ISMS Top Management	N/A

Approval

This document needs approval in writing from all RACI roles.

Statement of Applicability

The table below presents the statement of applicability as required by ISO/IEC 27001 Annex A. It presents the necessary controls, justification for their inclusions, the decision to their implementation as well as justification of exclusion.

No*	Control title*	Control*	Justification*	Method of fulfillment*
5	Organizational controls			
5.1	Policies for information security	Information security policy and topic-specific policies shall be defined, approved by management, published, communicated to and acknowledged by relevant personnel and relevant interested parties, and reviewed at planned intervals and if significant changes occur.	Informing employees and other interested parties about information security objectives and commitment to meeting applicable information security requirements in the company and continuous improvement in this area.	APPLICABLE
5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be defined and allocated according to the organization needs.	To ensure clear accountability and ownership for information security tasks and decisions	APPLICABLE
5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility shall be segregated.	To prevent conflicts of interest and unauthorized actions by requiring multiple individuals for critical tasks	APPLICABLE
5.4	Management responsibilities	Management shall require all personnel to apply information security in accordance with the established	To ensure leadership commitment and support for information security initiatives	APPLICABLE

		information security policy, topic-specific policies and procedures of the organization.		
5.5	Contact with authorities	The organization shall establish and maintain contact with relevant authorities.	To ensure compliance with legal and regulatory requirements and prompt handling of incidents	APPLICABLE
5.6	Contact with special interest groups	The organization shall establish and maintain contact with special interest groups or other specialist security forums and professional associations.	To manage interactions with external organizations and interest groups	APPLICABLE
5.7	Threat intelligence	Information relating to information security threats shall be collected and analysed to produce threat intelligence.	To proactively identify and mitigate emerging threats and vulnerabilities	APPLICABLE
5.8	Information security in project management	Information security shall be integrated into project management.	To ensure that security considerations are addressed throughout project lifecycles	APPLICABLE
5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including owners, shall be developed and maintained.	To have visibility and control over sensitive information and critical assets	APPLICABLE
5.10	Acceptable use of information and other associated assets	Rules for the acceptable use and procedures for handling information and other associated assets shall be identified, documented and implemented.	To guide employees in using organization resources responsibly and securely	APPLICABLE
5.11	Return of assets	Personnel and other interested parties as appropriate shall return all the organization's assets in their possession	To prevent unauthorized access to sensitive assets and information	APPLICABLE

		upon change or termination of their employment, contract or agreement.		
5.12	Classification of information	Information shall be classified according to the information security needs of the organization based on confidentiality, integrity, availability and relevant interested party requirements.	To apply appropriate protection measures to different levels of information	APPLICABLE
5.13	Labelling of information	An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	To visually indicate the level of protection required for different types of information	APPLICABLE
5.14	Information transfer	Information transfer rules, procedures, or agreements shall be in place for all types of transfer facilities within the organization and between the organization and other parties.	To protect the confidentiality and integrity of information during transmission	APPLICABLE
5.15	Access control	Rules to control physical and logical access to information and other associated assets shall be established and implemented based on business and information security requirements.	Implement encryption protocols for data in transit, establish secure file transfer methods, use encrypted communication channels for sharing sensitive information	APPLICABLE
5.16	Identity management	The full life cycle of identities shall be managed.	Best practice	APPLICABLE
5.17	Authentication information	Allocation and management of authentication information shall be controlled by a management process, including advising personnel on appropriate handling of authentication information.	Best practice	APPLICABLE

5.18	Access rights	Access rights to information and other associated assets shall be provisioned, reviewed, modified and removed in accordance with the organization's topic-specific policy on and rules for access control.	Best practice	APPLICABLE
5.19	Information security in supplier relationships	Processes and procedures shall be defined and implemented to manage the information security risks associated with the use of supplier's products or services.	Best practice	APPLICABLE
5.20	Addressing information security within supplier agreements	Relevant information security requirements shall be established and agreed with each supplier based on the type of supplier relationship.	Best practice	APPLICABLE
5.21	Managing information security in the information and communication technology (ICT) supply chain	Processes and procedures shall be defined and implemented to manage the information security risks associated with the ICT products and services supply chain.	Best practice	APPLICABLE
5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage change in supplier information security practices and service delivery.	Best practice	APPLICABLE
5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit from cloud services shall be established in accordance with the organization's	Best practice	APPLICABLE

		information security requirements.		
5.24	Information security incident management planning and preparation	The organization shall plan and prepare for managing information security incidents by defining, establishing and communicating information security incident management processes, roles and responsibilities.	Best practice	APPLICABLE
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.	Best practice	APPLICABLE
5.26	Response to information security incidents	Information security incidents shall be responded to in accordance with the documented procedures.	Best practice	APPLICABLE
5.27	Learning from information security incidents	Knowledge gained from information security incidents shall be used to strengthen and improve the information security controls.	Best practice	APPLICABLE
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.	Best practice	APPLICABLE
5.29	Information security during disruption	The organization shall plan how to maintain information security at an appropriate level during disruption.	Best practice	APPLICABLE
5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented, maintained and tested based on business continuity objectives	Best practice	APPLICABLE

		and ICT continuity requirements.		
5.31	Legal, statutory, regulatory and contractual requirements	Legal, statutory, regulatory and contractual requirements relevant to information security and the organization's approach to meet these requirements shall be identified, documented and kept up to date.	Best practice	APPLICABLE
5.32	Intellectual property rights	The organization shall implement appropriate procedures to protect intellectual property rights.	Best practice	APPLICABLE
5.33	Protection of records	Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release.	Best practice	APPLICABLE
5.34	Privacy and protection of personal identifiable information (PII)	The organization shall identify and meet the requirements regarding the preservation of privacy and protection of PII according to applicable laws and regulations and contractual requirements.	Best practice	APPLICABLE
5.35	Independent review of information security	The organization's approach to managing information security and its implementation including people, processes and technologies shall be reviewed independently at planned intervals, or when significant changes occur.	Best practice	APPLICABLE
5.36	Compliance with policies, rules and standards for information	Compliance with the organization's information security policy, topic-specific policies, rules and standards shall be regularly reviewed.	Best practice	APPLICABLE

	security			
5.37	Documented operating procedures	Operating procedures for information processing facilities shall be documented and made available to personnel who need them.	Best practice	APPLICABLE
6	People controls			
6.1	Screening	Background verification checks on all candidates to become personnel shall be carried out prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Best practice	APPLICABLE
6.2	Terms and conditions of employment	The employment contractual agreements shall state the personnel's and the organization's responsibilities for information security.	Best practice	APPLICABLE
6.3	Information security awareness, education and training	Personnel of the organization and relevant interested parties shall receive appropriate information security awareness, education and training and regular updates of the organization's information security policy, topic-specific policies and procedures, as relevant for their job function.	Best practice	APPLICABLE
6.4	Disciplinary process	A disciplinary process shall be formalized and communicated to take actions against personnel and other	Best practice	APPLICABLE

		relevant interested parties who have committed an information security policy violation.		
6.5	Responsibilities after termination or change of employment	Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, enforced and communicated to relevant personnel and other interested parties.	Best practice	APPLICABLE
6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, documented, regularly reviewed and signed by personnel and other relevant interested parties.	Best practice	APPLICABLE
6.7	Remote working	Security measures shall be implemented when personnel are working remotely to protect information accessed, processed or stored outside the organization's premises.	Best practice	APPLICABLE
6.8	Information security event reporting	The organization shall provide a mechanism for personnel to report observed or suspected information security events through appropriate channels in a timely manner.	Best practice	APPLICABLE
7	Physical controls			
7.1	Physical security perimeters	Security perimeters shall be defined and used to protect areas that contain information and other associated assets.	Best practice	APPLICABLE

7.2	Physical entry	Secure areas shall be protected by appropriate entry controls and access points.	Best practice	APPLICABLE
7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and implemented.	Best practice	APPLICABLE
7.4	Physical security monitoring	Premises shall be continuously monitored for unauthorized physical access.	Best practice	APPLICABLE
7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure shall be designed and implemented.	Best practice	APPLICABLE
7.6	Working in secure areas	Security measures for working in secure areas shall be designed and implemented.	Best practice	APPLICABLE
7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage media and clear screen rules for information processing facilities shall be defined and appropriately enforced.	Best practice	APPLICABLE
7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Best practice	APPLICABLE
7.9	Security of assets off-premises	Off-site assets shall be protected.	Best practice	APPLICABLE
7.10	Storage media	Storage media shall be managed	Best practice	APPLICABLE

		through their life cycle of acquisition, use, transportation and disposal in accordance with the organization's classification scheme and handling requirements.		
7.11	Supporting utilities	Information processing facilities shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Best practice	APPLICABLE
7.12	Cabling security	Cables carrying power, data or supporting information services shall be protected from interception, interference or damage.	Best practice	APPLICABLE
7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure availability, integrity and confidentiality of information.	Best practice	APPLICABLE
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 securely overwritten prior to disposal or re-use.	Best practice	APPLICABLE
8	Technological controls			
8.1	User end point devices	Information stored on, processed by or accessible via user end point devices shall be protected.	To protect sensitive data and prevent unauthorized access	APPLICABLE

8.2	Privileged access rights	The allocation and use of privileged access rights shall be restricted and managed.	To minimize the risk of unauthorized access and potential misuse	APPLICABLE
8.3	Information access restriction	Access to information and other associated assets shall be restricted in accordance with the established topic-specific policy on access control.	To ensure confidentiality, integrity, and availability of information	APPLICABLE
8.4	Access to source code	Read and write access to source code, development tools and software libraries shall be appropriately managed.	Restriction of read and write access to the source code and development tools on the "need-to-know" basis for employees responsible for application instance setup & deployment.	APPLICABLE
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.	To prevent unauthorized access and protect user identities	APPLICABLE
8.6	Capacity management	The use of resources shall be monitored and adjusted in line with current and expected capacity requirements.	To optimize system performance and prevent service interruptions	APPLICABLE
8.7	Protection against malware	Protection against malware shall be implemented and supported by appropriate user awareness.	To prevent malware infections and minimize the risk of data breaches	APPLICABLE
8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems in use shall be obtained, the organization's exposure to such vulnerabilities shall be evaluated and appropriate measures shall be taken.	To identify and address vulnerabilities that could be exploited	APPLICABLE

8.9	Configuration management	Configurations, including security configurations, of hardware, software, services and networks shall be established, documented, implemented, monitored and reviewed.	To ensure consistent and secure configurations, minimizing the risk of unauthorized changes and misconfigurations	APPLICABLE
8.10	Information deletion	Information stored in information systems, devices or in any other storage media shall be deleted when no longer required.	To prevent unauthorized access and comply with data privacy regulations	APPLICABLE
8.11	Data masking	Data masking shall be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies, and business requirements, taking applicable legislation into consideration.	To protect sensitive data during testing, development, and analysis	APPLICABLE
8.12	Data leakage prevention	Data leakage prevention measures shall be applied to systems, networks and any other devices that process, store or transmit sensitive information.	To protect sensitive information from unauthorized disclosure	APPLICABLE
8.13	Information backup	Backup copies of information, software and systems shall be maintained and regularly tested in accordance with the agreed topic-specific policy on backup.	To protect against data loss and minimize downtime in the event of system failures	APPLICABLE
8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	To ensure continuous availability and minimize the impact of disruptions	APPLICABLE
8.15	Logging	Logs that record activities, exceptions, faults and other relevant events shall be produced, stored, protected and analysed.	To detect and investigate security incidents, and support forensic analysis	APPLICABLE

8.16	Monitoring activities	Networks, systems and applications shall be monitored for anomalous behaviour and appropriate actions taken to evaluate potential information security incidents.	To identify and mitigate security incidents and vulnerabilities	APPLICABLE
8.17	Clock synchronization	The clocks of information processing systems used by the organization shall be synchronized to approved time sources.	To ensure proper system functioning and accurate event sequencing	APPLICABLE
8.18	Use of privileged utility programs	The use of utility programs that can be capable of overriding system and application controls shall be restricted and tightly controlled.	To prevent unauthorized access and misuse of privileged functions	APPLICABLE
8.19	Installation of software on operational systems	Procedures and measures shall be implemented to securely manage software installation on operational systems.	To ensure secure and authorized software deployments	APPLICABLE
8.20	Networks security	Networks and network devices shall be secured, managed and controlled to protect information in systems and applications.	To protect network assets and prevent unauthorized access	APPLICABLE
8.21	Security of network services	Security mechanisms, service levels and service requirements of network services shall be identified, implemented and monitored.	To prevent unauthorized access, data interception, and service disruptions	APPLICABLE
8.22	Segregation of networks	Groups of information services, users and information systems shall be segregated in the organization's networks.	To prevent unauthorized access and limit the impact of network breaches	APPLICABLE
8.23	Web filtering	Access to external websites shall be	To protect against web-based	APPLICABLE

		managed to reduce exposure to malicious content.	threats and enforce acceptable use policies	
8.24	Use of cryptography	Rules for the effective use of cryptography, including cryptographic key management, shall be defined and implemented.	To ensure confidentiality, integrity, and authenticity of sensitive information	APPLICABLE
8.25	Secure development life cycle	Rules for the secure development of software and systems shall be established and applied.	To identify and mitigate security vulnerabilities in applications	APPLICABLE
8.26	Application security requirements	Information security requirements shall be identified, specified and approved when developing or acquiring applications.	To ensure that applications are designed and developed with security in mind	APPLICABLE
8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be established, documented, maintained and applied to any information system development activities.	To design and build secure and resilient systems	APPLICABLE
8.28	Secure coding	Secure coding principles shall be applied to software development.	To prevent common software vulnerabilities and reduce the risk of exploitation	APPLICABLE
8.29	Security testing in development and acceptance	Security testing processes shall be defined and implemented in the development life cycle.	To identify and remediate security vulnerabilities and ensure secure software deployment	APPLICABLE
8.30	Outsourced development	The organization shall direct, monitor and review the activities related to outsourced system development.	To ensure the security of systems developed by external parties	APPLICABLE
8.31	Separation of development,	Development, testing and production environments shall be separated and	To prevent unauthorized access, accidental data leaks,	APPLICABLE

	test and production environments	secured.	and ensure proper testing	
8.32	Change management	Changes to information processing facilities and information systems shall be subject to change management procedures.	To control and manage changes to systems and minimize the risk of unauthorized modifications	APPLICABLE
8.33	Test information	Test information shall be appropriately selected, protected and managed.	To prevent unauthorized access to sensitive test data and ensure accurate testing	APPLICABLE
8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving assessment of operational systems shall be planned and agreed between the tester and appropriate management.	To maintain system integrity and prevent disruptions during audit processes	APPLICABLE

Table. ISO 27001 Information security controls reference.

References

Normative source	Chapter
ISO/IEC 27001:2022(E)	6.1.3 d); Annex A