infomaniak

Statement of Applicability ISO 27001 : 2022

Chapter Name	ID	Article Name	Article Description	Applicable
Organizational Security Measures	A.5.1	Information security policies	An information security policy and topic-specific policies should be defined, approved by management, published, communicated and requested for confirmation from relevant personnel and stakeholders, and reviewed at planned intervals and if significant changes occur.	Yes
Organizational Security Measures	A.5.10	Correct use of information and other associated assets	Rules for the correct use and procedures for handling information and other associated assets must be identified, documented and implemented.	Yes
Organizational Security Measures	A.5.11	Return of assets	Staff and other interested parties, as applicable, must return all assets of the organization in their possession at the time of the change or termination of their employment, contract or agreement.	Yes
Organizational Security Measures	A.5.12	Classification of information	Information should be classified in accordance with the organization's information security needs, based on confidentiality, integrity, availability requirements, and significant stakeholder requirements.	Yes
Organizational Security Measures	A.5.13	Marking information	An appropriate set of procedures for marking information should be developed and implemented in accordance with the information classification scheme adopted by the organization.	Yes
Organizational Security Measures	A.5.14	Transfer of information	Rules, procedures or agreements on the transfer of information must be in place for all types of transfer means within the organization and between the organization and third parties.	Yes
Organizational Security Measures	A.5.15	Access control	Rules to control physical and logical access to information and other associated assets must be defined and implemented, based on business and information security requirements.	Yes
Organizational Security Measures	A.5.16	Identity management	The complete lifecycle of identities must be managed.	Yes
Organizational Security Measures	A.5.17	Authentication information	The allocation and management of authentication information must be controlled by a management process, including guidance to staff on the appropriate use of authentication information.	Yes
Organizational Security Measures	A.5.18	Access rights	Access rights to information and other associated assets must be provided, reviewed, modified and removed in accordance with the organization's subject-specific access control policy and access control rules.	Yes
Organizational Security Measures	A.5.19	Information security in supplier relationships	Processes and procedures to manage information security risks associated with the use of the supplier's products or services must be defined and implemented	Yes
Organizational Security Measures	A.5.2	Information Security Functions and Responsibilities	Information security functions and responsibilities should be defined and assigned according to the needs of the organization.	Yes
Organizational Security Measures	A.5.20	Information security in agreements with suppliers	Appropriate information security requirements should be put in place and agreed with each supplier, depending on the type of relationship with the supplier.	Yes
Organizational Security Measures	A.5.21	Information Security Management in the Information and Communication Technology (ICT) Supply Chain	Processes and procedures to manage information security risks associated with the supply chain of ICT products and services must be defined and implemented.	Yes
Organizational Security Measures	A.5.22	Monitoring, review and change management of supplier services	The organization shall regularly monitor, review, evaluate and manage changes to the provider's information security and service delivery practices.	Yes
Organizational Security Measures	A.5.23	Information security in the use of cloud services	Processes for acquiring, using, managing and terminating cloud services must be established in accordance with the organization's information security requirements.	Yes

Organizational Security Measures	A.5.24	Planning and preparation for information security incident management	The organization must plan and prepare for information security incident management by defining, establishing and communicating the processes, functions and responsibilities related to information security incident management.	Yes
Organizational Security Measures	A.5.25	Information security event assessment and decision making	The organization must assess information security events and decide whether they should be categorized as information security incidents.	Yes
Organizational Security Measures	A.5.26	Information Security Incident Response	Response to information security incidents must be in accordance with documented procedures.	Yes
Organizational Security Measures	A.5.27	Learning from information security incidents	Knowledge gained from information security incidents should be used to strengthen and improve information security measures.	Yes
Organizational Security Measures	A.5.28	Evidence collection	The organization shall establish and implement procedures for the identification, collection, acquisition and preservation of evidence relating to information security events.	Yes
Organizational Security Measures	A.5.29	Information Security During a Disruption	The organization must plan how to maintain information security at the appropriate level during a disruption.	Yes
Organizational Security Measures	A.5.3	Separation of duties	Incompatible tasks and areas of responsibility should be separated.	Yes
Organizational Security Measures	A.5.30	ICT Preparation for Business Continuity	ICT preparedness should be planned, implemented, maintained and tested based on business continuity objectives and ICT continuity requirements.	Yes
Organizational Security Measures	A.5.31	Legal, statutory, regulatory and contractual requirements	The relevant legal, statutory, regulatory and contractual requirements for information security, as well as the organization's approach to meeting these requirements, must be identified, documented and kept up to date.	Yes
Organizational Security Measures	A.5.32	Intellectual Property Rights	The organization must implement appropriate procedures to protect intellectual property rights.	Yes
Organizational Security Measures	A.5.33	Protection of recordings	Recordings must be protected from loss, destruction, falsification, unauthorized access and unauthorized dissemination.	Yes
Organizational Security Measures	A.5.34	Protection of privacy and personal data (DCP)	The organization must identify and comply with privacy and personal data protection requirements in accordance with applicable laws, regulations and contractual requirements.	Yes
Organizational Security Measures	A.5.35	Independent Information Security Review	The organization's approach to managing information security and its implementation, including people, processes, and technologies, should be independently reviewed at planned intervals, or when significant changes occur.	Yes
Organizational Security Measures	A.5.36	Compliance with information security policies, rules and standards	Compliance with the organization's information security policy, topic-specific policies, rules and standards should be regularly verified	Yes
Organizational Security Measures	A.5.37	Documented operating procedures	Operating procedures for information processing facilities must be documented and made available to personnel who need them.	Yes
Organizational Security Measures	A.5.4	Management Responsibilities	Management should require all staff to implement information security measures in accordance with the organization's information security policy, topic-specific policies and established procedures.	Yes
Organizational Security Measures	A.5.5	Contacts with the authorities	The organization must establish and maintain contact with the appropriate authorities.	Yes
Organizational Security Measures	A.5.6	Contacts with specific interest groups	The organization should establish and maintain contacts with specific interest groups or other specialized security forums and professional associations.	Yes

Organizational Security Measures	A.5.7	Threat Intelligence	Information related to information security threats must be collected and analyzed to produce threat intelligence.	Yes
Organizational Security Measures	A.5.8	Information security in project management	Information security must be integrated into project management.	Yes
Organizational Security Measures	A.5.9	Inventory of information and other associated assets	An inventory of information and other associated assets, including their owners, must be developed and maintained.	Yes
People Security Measures	A.6	Safety measures applicable to individuals		Yes
People Security Measures	A.6.1	Selection of candidates	Reference checks on all job applicants should be conducted prior to joining the organization and on an ongoing basis, taking into account applicable laws, regulations and ethics, and should be commensurate with the business requirements, the classification of the information to which they will have access and the identified risks.	Yes
People Security Measures	A.6.2	Terms and conditions of the employment contract	Employment contracts should state the responsibilities of staff and the organization regarding information security.	Yes
People Security Measures	A.6.3	Information security awareness, education and training	Organizational personnel and relevant stakeholders must receive appropriate information security awareness, education and training, as well as regular updates to the organization's information security policy, topic-specific policies and procedures relevant to their role.	Yes
People Security Measures	A.6.4	Disciplinary process	A disciplinary process for taking action against staff and other interested parties who have committed a violation of the information security policy must be formalized and communicated.	Yes
People Security Measures	A.6.5	Responsibilities after ending or changing employment	Responsibilities and obligations relating to information security that remain in force after the end or change of employment must be defined, applied and communicated to staff and other relevant stakeholders.	Yes
People Security Measures	A.6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements, representing the organization's needs for protecting information, must be identified, documented, regularly reviewed and signed.	Yes
People Security Measures	A.6.7	Remote work	Security measures must be implemented when staff are working remotely, to protect information accessed, processed or stored outside the organization's premises.	Yes
People Security Measures	A.6.8	Information Security Event Reporting	The organization shall provide a mechanism for personnel to promptly report observed or suspected information security events through appropriate channels.	Yes
People Security Measures	A.7	Physical security measures		Yes
Physical Security Measures	A.7.1	Physical security perimeters	Security perimeters must be defined and used to protect areas that contain information and other associated assets.	Yes
Physical Security Measures	A.7.10	Storage media	Storage media must be managed throughout their lifecycle of acquisition, use, transport and disposal in accordance with the organization's classification scheme and processing requirements.	Yes

Physical Security Measures	A.7.11	Support services	Information processing facilities must be protected against power outages and other disruptions caused by failures of support services.	Yes
Physical Security Measures	A.7.12	Wiring Safety	Electrical cables carrying data or supporting information services must be protected against interception, interference or damage.	Yes
Physical Security Measures	A.7.13	Hardware maintenance	Equipment must be properly maintained to ensure the availability, integrity and confidentiality of information.	Yes
Physical Security Measures	A.7.14	Secure disposal or recycling of equipment	Hardware items containing storage media should be checked to ensure that any sensitive data and licensed software have been securely deleted or overwritten, prior to disposal or reuse.	Yes
Physical Security Measures	A.7.2	Physical entrances	Secure areas must be protected by appropriate access security measures and access points.	Yes
Physical Security Measures	A.7.3	Securing offices, rooms and facilities	Physical security measures for offices, rooms and facilities must be designed and implemented.	Yes
Physical Security Measures	A.7.4	Physical security monitoring	The premises must be continuously monitored to prevent unauthorized physical access.	Yes
Physical Security Measures	A.7.5	Protection against physical and environmental threats	Protection against physical and environmental threats, such as natural disasters and other physical threats, intentional or unintentional, impacting infrastructure, must be designed and implemented.	Yes
Physical Security Measures	A.7.6	Work in secure areas	Safety measures for working in secure areas must be designed and implemented.	Yes
Physical Security Measures	A.7.7	Clean desk and blank screen	Rules for an empty desk, clear of paper documents and removable storage media, and rules for a blank screen for information processing means, must be defined and applied appropriately.	Yes
Physical Security Measures	A.7.8	Location and protection of equipment	A secure location for the equipment must be chosen and protected.	Yes
Physical Security Measures	A.7.9	Security of assets off premises	Off-site assets must be protected.	Yes
Technological Security Measures	A.8	Technological security measures		Yes
Technological Security Measures	A.8.1	User end terminals	Information stored, processed or accessible via users' end devices must be protected.	Yes
Technological Security Measures	A.8.10	Deletion of information	Information stored in information systems, terminals or any other storage media must be deleted when it is no longer needed.	Yes
Technological Security Measures	A.8.11	Data masking	Data masking should be used in accordance with the organization's subject-specific access control policy and other associated subject-specific policies, as well as business requirements, while taking into account applicable legislation.	Yes
Technological Security Measures	A.8.12	Data Leak Prevention	Data leak prevention measures must be applied to systems, networks and all other terminals that process, store or transmit sensitive information.	Yes
Technological Security Measures	A.8.13	Saving information	Backup copies of information, software and systems must be maintained and tested regularly according to the agreed backup policy specific to the topic.	Yes
Technological Security Measures	A.8.14	Redundancy of information processing resources	Information processing means must be implemented with sufficient redundancy to meet availability requirements.	Yes

Technological Security Measures	A.8.15	Logging	Logs that record activities, exceptions, failures, and other relevant events must be generated, retained, protected, and analyzed.	Yes
Technological Security Measures	A.8.16	Surveillance activities	Networks, systems and applications should be monitored for abnormal behavior and appropriate measures should be taken to assess potential information security incidents.	Yes
Technological Security Measures	A.8.17	Clock synchronization	Clocks in information processing systems used by the organization must be synchronized with approved time sources.	Yes
Technological Security Measures	A.8.18	Using Privileged Utility Programs	The use of utility programs that have the ability to circumvent system or application security measures should be limited and tightly controlled.	Yes
Technological Security Measures	A.8.19	Installing software on operational systems	Procedures and measures must be implemented to securely manage the installation of software on operational systems.	Yes
Technological Security Measures	A.8.2	Privileged access rights	The allocation and use of privileged access rights must be limited and managed.	Yes
Technological Security Measures	A.8.20	Network security	Networks and network endpoints must be secured, managed, and controlled to protect information in systems and applications.	Yes
Technological Security Measures	A.8.21	Network Services Security	Security mechanisms, service levels and service requirements of network services must be identified, implemented and monitored.	Yes
Technological Security Measures	A.8.22	Network partitioning	Groups of information services, users, and information systems must be partitioned within the organization's networks.	Yes
Technological Security Measures	A.8.23	Web filtering	Access to external websites should be managed to reduce exposure to malicious content.	Yes
Technological Security Measures	A.8.24	Use of cryptography	Rules for the effective use of cryptography, including the management of cryptographic keys, must be defined and implemented.	Yes
Technological Security Measures	A.8.25	Secure Development Lifecycle	Rules for the secure development of software and systems must be defined and enforced.	Yes
Technological Security Measures	A.8.26	Application security requirements	Information security requirements must be identified, specified, and approved when developing or acquiring applications.	Yes
Technological Security Measures	A.8.27	Principles of secure systems engineering and architecture	Secure systems engineering principles must be established, documented, maintained, and applied to all information systems development activities.	Yes
Technological Security Measures	A.8.28	Secure coding	Secure coding principles should be applied to software development.	Yes
Technological Security Measures	A.8.29	Security testing in development and acceptance	Processes for security testing should be defined and implemented during the development lifecycle.	Yes
Technological Security Measures	A.8.3	Restriction of access to information	Access to information and other associated assets must be restricted in accordance with the established access control topic-specific policy.	Yes
Technological Security Measures	A.8.30	Outsourced development	The organization must direct, control and audit activities related to outsourced systems development.	Yes
Technological Security Measures	A.8.31	Separation of development, test and operational environments	Development, test and operational environments must be separated and secure.	Yes
Technological Security Measures	A.8.32	Change management	Changes to information processing facilities and information systems must be subject to change management procedures.	Yes
Technological Security Measures	A.8.33	Test information	Test information must be selected, protected and managed appropriately.	Yes

Technological Security Measures	A.8.34	Protection of information systems during audit tests	Audit testing and other assurance activities involving the evaluation of operational systems should be planned and agreed between the tester and the appropriate level of management.	Yes
Technological Security Measures	A.8.4	Access to source codes	Read and write access to source code, development tools, and software libraries must be managed appropriately.	Yes
Technological Security Measures	A.8.5	Secure authentication	Secure authentication technologies and procedures must be implemented based on information access restrictions and the policy specific to the access control topic.	Yes
Technological Security Measures	A.8.6	Sizing	Resource utilization should be monitored and adjusted according to current and forecasted sizing needs.	Yes
Technological Security Measures	A.8.7	Malware Protection	Malware protection must be implemented and reinforced by appropriate user awareness.	Yes
Technological Security Measures	A.8.8	Technical Vulnerability Management	Information on the technical vulnerabilities of the information systems used must be obtained, the organization's exposure to these vulnerabilities must be assessed and appropriate measures must be taken.	Yes
Technological Security Measures	A.8.9	Configuration management	Configurations, including security, hardware, software, service, and network configurations, must be defined, documented, implemented, monitored, and reviewed.	Yes