ISO 27001:2013 Statement of Applicability
2024-07-18

ISO CONTROL	APPLICABLE	STATUS
A.5 Information security policies		
A.5.1 Management direction for information security Objective: To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
A.5.1.1 Policies for information security	yes	implemented
A.5.1.2 Review of policies for Information security	yes	implemented
A.6 Organization of information security		
A.6.1 Internal organization Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
A.6.1.1 Information Security roles and responsibilities	yes	implemented
A.6.1.2 Segregation of duties	yes	implemented
A.6.1.3 Contact with authorities	yes	implemented
A.6.1.4 Contact with special interest groups	yes	implemented
A.6.1.5 Information security in project management	yes	implemented
A.6.2 Mobile devices and teleworking Objective: To ensure the security of teleworking and use of mobile devices.		
A.6.2.1 Mobile device policy	yes	implemented
A.6.2.2 Teleworking	yes	implemented
A.7 Human resource security		
A.7.1 Prior to employment Objective: To ensure that employees and contractors understand their responsibilities and are suitable for the roles for which they are considered.		
A.7.1.1 Screening	yes	implemented
A.7.1.2 Terms and conditions of employment	yes	implemented
A.7.2 During employment Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
A.7.2.1 Management Responsibilities	yes	implemented
A.7.2.2 Information security awareness, education and training	yes	implemented
A.7.2.3 Disciplinary process	yes	implemented

ISO 27001:2013 Statement of Applicability
2024-07-18

ISO CONTROL	APPLICABLE	STATUS
A.7.3 Termination and change of employment Objective: To protect the organization's interests as part of the process of changing or terminating employment.		
A.7.3.1 Termination or change of employment responsibilities	yes	implemented
A.8 Asset management		
A.8.1 Responsibility for assets Objective: To identify organizational assets and define appropriate protection responsibilities.		
A.8.1.1 Inventory of assets	yes	implemented
A.8.1.2 Ownership of assets	yes	implemented
A.8.1.3 Acceptable use of assets	yes	implemented
A.8.1.4 Return of assets	yes	implemented
A.8.2 Information classification Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
A.8.2.1 Classification of information	yes	implemented
A.8.2.2 Labelling of information	yes	implemented
A.8.2.3 Handling of assets	yes	implemented
A.8.3 Media handling Objective: To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
A.8.3.1 Management of removable media	yes	implemented
A.8.3.2 Disposal of Media	yes	implemented
A.8.3.3 Physical media in transfer	no	N/A
A.9 Access control		
A.9.1 Business requirements of access control Objective: To limit access to information and information processing facilities.		
A.9.1.1 Access control policy	yes	implemented
A.9.1.2 Access to networks and network services	yes	implemented
A.9.2 User access management		
A.9.2.1 User registration and de-registration	yes	implemented
A.9.2.2 User access provisioning	yes	implemented

ISO 27001:2013 Statement of Applicability
2024-07-18

ISO CONTROL	APPLICABLE	STATUS
A.9.2.3 Management of privileged access rights	yes	implemented
A.9.2.4 Management of secret authentication information of users	yes	implemented
A.9.2.5 Review of user access rights	yes	implemented
A.9.2.6 Removal or adjustment of access rights	yes	implemented
A.9.3 User responsibilities Objective: To make users accountable for safeguarding their authentication information.		
A.9.3.1 Use of secret authentication information	yes	implemented
A.9.4 System and application access control Objective: To prevent unauthorized access to systems and applications.		
A.9.4.1 Information access restriction	yes	implemented
A.9.4.2 Secure log-on Procedures	yes	implemented
A.9.4.3 Password Management system	yes	implemented
A.9.4.4 Use of privileged utility programs	yes	implemented
A.9.4.5 Access control to program source code	yes	implemented
A.10 Cryptography		
A.10.1 Cryptographic controls Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.		
A.10.1.1 Policy on the use of cryptographic controls	yes	implemented
A.10.1.2 Key Management	yes	implemented
A.11 Physical and environmental security		
A.11.1 Secure areas Objective: To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.		
A.11.1.1 Physical security perimeter	yes	implemented
A.11.1.2 Physical entry controls	yes	implemented
A.11.1.3 Securing offices, rooms and facilities	yes	implemented
A.11.1.4 Protecting against external and environmental threats	yes	implemented
A.11.1.5 Working in secure areas	yes	implemented

ISO 27001:2013 Statement of Applicability
2024-07-18

ISO CONTROL	APPLICABLE	STATUS
A.11.1.6 Delivery and loading areas	no	N/A
A.11.2 Equipment Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
A.11.2.1 Equipment siting and protection	yes	implemented
A.11.2.2 Supporting utilities	yes	implemented
A.11.2.3 Cabling security	yes	implemented
A.11.2.4 Equipment maintenance	yes	implemented
A.11.2.5 Removal of assets	yes	implemented
A.11.2.6 Security of equipment and assets off premises	yes	implemented
A.11.2.7 Secure disposal or re-use of equipment	yes	implemented
A.11.2.8 Unattended user equipment	yes	implemented
A.11.2.9 Clear Desk and Clear Screen Policy	yes	implemented
A.12 Operations security		
A.12.1 Operational procedures and responsibilities Objective: To ensure correct and secure operations of information processing facilities.		
A.12.1.1 Documented operating procedures	yes	implemented
A.12.1.2 Change management	yes	implemented
A.12.1.3 Capacity management	yes	implemented
A.12.1.4 Separation of development, testing and operational environments	yes	implemented
A.12.2 Protection from malware Objective: To ensure that information and information processing facilities are protected against malware.		
A.12.2.1 Control against malware	yes	implemented
A.12.3 Backup Objective: To protect against loss of data.		
A.12.3.1 Information backup	yes	implemented
A.12.4 Logging and monitoring Objective: To record events and generate evidence.		
A.12.4.2 Protection of log information	yes	implemented

ISO 27001:2013 Statement of Applicability
2024-07-18

ISO CONTROL	APPLICABLE	STATUS
A.12.4.1 Event logging	yes	implemented
A.12.4.3 Administrator and operator logs	yes	implemented
A.12.4.4 Clock synchronisation	yes	implemented
A.12.5 Control of operational software Objective: To ensure the integrity of operational systems.		
A.12.5.1 Installation of software on operational systems	yes	implemented
A.12.6 Technical vulnerability management Objective: To prevent exploitation of technical vulnerabilities.		
A.12.6.1 Management of technical vulnerabilities	yes	implemented
A.12.6.2 Restrictions on software installation	yes	implemented
A.12.7 Information systems audit considerations Objective: To minimise the impact of audit activities on operational systems.		
A.12.7.1 Information systems audit controls	yes	implemented
A.13 Communications security		
A.13.1 Network security management Objective: To ensure the protection of information in networks and its supporting information processing facilities.		
A.13.1.1 Network controls	yes	implemented
A.13.1.2 Security of network services	yes	implemented
A.13.1.3 Segregation in networks	no	N/A
A.13.2 Information transfer Objective: To maintain the security of information transferred within an organization and with any external entity.		
A.13.2.1 Information transfer policies and procedures	yes	implemented
A.13.2.2 Agreements on information transfer	yes	implemented
A.13.2.3 Electronic messaging	yes	implemented
A.13.2.4 Confidentiality or non disclosure agreements	yes	implemented
A.14 System acquisition, development and maintenance		
A.14.1 Security requirements of information systems Objective: To ensure that information security is an integral part of information systems across the entire lifecycle. This also includes the requirements for information systems which provide services over public		

ISO CONTROL	APPLICABLE	STATUS
networks.		
A.14.1.1 Information security requirements analysis and specification	yes	implemented
A.14.1.2 Securing application services on public networks	yes	implemented
A.14.1.3 Protecting application services and transactions	yes	implemented
A.14.2 Security in development and support processes Objective: To ensure that information security is designed and implemented within the development lifecycle of information systems.		
A.14.2.1 Secure development policy	yes	implemented
A.14.2.2 System change control procedures	yes	implemented
A.14.2.3 Technical review of applications after Operating platform changes	yes	implemented
A.14.2.4 Restrictions on changes to software packages	yes	implemented
A.14.2.5 Secure system engineering principles	yes	implemented
A.14.2.6 Secure development environment	yes	implemented
A.14.2.7 Outsourced development	yes	implemented
A.14.2.8 System security testing	yes	implemented
A.14.2.9 System acceptance testing	yes	implemented
A.14.3 Test data Objective: To ensure the protection of data used for testing.		
A.14.3.1 Protection of test data	yes	implemented
A.15 Supplier relationships		
A.15.1 Information security in supplier relationships		
A.15.1.1 Information security policy for supplier relationships	yes	implemented
A.15.1.2 Addressing security within supplier agreements	yes	implemented
A.15.1.3 Information and communication technology supply chain	yes	implemented
A.15.2 Supplier service delivery management Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.		

ISO 27001:2013 Statement of Applicability
2024-07-18

ISO CONTROL	APPLICABLE	STATUS
A.15.2.1 Monitoring and review of supplier services	yes	implemented
A.15.2.2 Managing changes to supplier services	yes	implemented
A.16 Information security incident management		
A.16.1 Management of information security incidents and improvements Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
A.16.1.1 Responsibilities and Procedures	yes	implemented
A.16.1.2 Reporting information security events	yes	implemented
A.16.1.3 Reporting information security weaknesses	yes	implemented
A.16.1.4 Assessment of and decision on information security events	yes	implemented
A.16.1.5 Response to information security incidents	yes	implemented
A.16.1.6 Learning from Information security incidents	yes	implemented
A.16.1.7 Collection of evidence	yes	implemented
A.17 Information security aspects of business continuity management		
A.17.1 Information security continuity Objective: Information security continuity shall be embedded in the organization's business continuity management systems.		
A.17.1.1 Planning information security continuity	yes	implemented
A.17.1.2 Implementation information security continuity.	yes	implemented
A.17.1.3 Verify, review and evaluate information security continuity	yes	implemented
A.17.2 Redundancies Objective: To ensure availability of information processing facilities.		
A.17.2.1 Availability of information processing facilities	yes	implemented
A.18 Compliance		
A.18.1 Compliance with legal and contractual requirements Objective: To avoid breaches of legal, statutory, regulatory or contractual obligations related to information security and of any security requirements.		
A.18.1.1 Identification of applicable legislations and contractual requirements	yes	implemented

ISO 27001:2013 Statement of Applicability
2024-07-18

ISO CONTROL	APPLICABLE	STATUS
A.18.1.2 Intellectual Property Rights (IPR)	yes	implemented
A.18.1.3 Protection of records	yes	implemented
A.18.1.4 Privacy and protection of personally identifiable information	yes	implemented
A.18.1.5 Regulation of cryptographic controls	yes	implemented
A.18.2 Information security reviews Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.		
A.18.2.1 Independent review of information security	yes	implemented
A.18.2.3 Compliance with security policies and standards	yes	implemented
A.18.2.3 Technical compliance review	yes	implemented