Exported on: 7/1/2022

Statement of Applicability

Justification

Applicable - implemented	This control is deemed to be applicable based on risk assessment and the control has been implemented.
Applicable - not implemented	This control is deemed to be applicable based on risk assessment but the level of risk has been deemed acceptable and the control has not been implemented.
Not Applicable	This control has been identified as "Not Applicable" and is not relevant to the scope of the ISMS. This has been confirmed through risk assessment.

Version: 2.0

This report includes essential information for Statement of Applicability. For full policy information please visit https://isms.online.

Applicability	Activity reference	Control / Activity	Objective / Deliverable
Applicable - implemented	A.5.1.1	Policies for information security	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.
Applicable - implemented	A.5.1.2	Review of the policies for information security	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.
Applicable - implemented	A.6.1.1	Information security roles and responsibilities	A.6.1 Internal organization. Objective: To establish a management framework to initiate and control implementation and operation of information security within the organization.
Applicable - implemented	A.6.1.2	Segregation of duties	A.6.1 Internal organization. Objective: To establish a management framework to initiate and control implementation and operation of information security within the organization.
Applicable - implemented	A.6.1.3	Contact with authorities	A.6.1 Internal organization. Objective: To establish a management framework to initiate and control implementation and operation of information security within the organization.
Applicable - implemented	A.6.1.4	Contact with special interest groups	A.6.1 Internal organization. Objective: To establish a management framework to initiate and control implementation and operation of information security within the organization.
Applicable - implemented	A.6.1.5	Information security in project management	A.6.1 Internal organization. Objective: To establish a management framework to initiate and control implementation and operation of information security within the organization.
Applicable - implemented	A.6.2.1	Mobile device policy	A.6.2 Mobile devices and teleworking. Objective: To ensure the security of teleworking and use of mobile devices.
Applicable - implemented	A.6.2.2	Teleworking	A.6.2 Mobile devices and teleworking. Objective: To ensure the security of teleworking and use of mobile devices.
Applicable - implemented	A.7.1.1	Screening	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.
Applicable - implemented	A.7.1.2	Terms and conditions of employment	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.
Applicable - implemented	A.7.2.1	Management responsibilities	A.7.2 During employment. Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
Applicable - implemented	A.7.2.2	Information security awareness, education and training	A.7.2 During employment. Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
Applicable - implemented	A.7.2.3	Disciplinary process	A.7.2 During employment. Objective: To ensure that employees and contractors are aware of and fulfil their information security responsibilities.
Applicable - implemented	A.7.3.1	Termination or change of employment responsibilities	A.7.3 Termination or change of employment. Objective: To protect the organization's interests as part of the process of changing or terminating employment.
Applicable - implemented	A.8.1.1	Inventory of assets	A.8.1 Responsibility for assets. Objective: To identify organizational assets and define appropriate protection responsibilities.
Applicable - implemented	A.8.1.2	Ownership of assets	A.8.1 Responsibility for assets. Objective: To identify organizational assets and define appropriate protection responsibilities.
Applicable - implemented	A.8.1.3	Acceptable use of assets	A.8.1 Responsibility for assets. Objective: To identify organizational assets and define appropriate protection responsibilities.
Applicable - implemented	A.8.1.4	Return of assets	A.8.1 Responsibility for assets. Objective: To identify organizational assets and define appropriate protection responsibilities.
Applicable - implemented	A.8.2.1	Classification of information	A.8.2 Classification of information. Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
Applicable - implemented	A.8.2.2	Labelling of information	A.8.2 Classification of information. Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
Applicable - implemented	A.8.2.3	Handling of assets	A.8.2 Classification of information. Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.
Applicable - implemented	A.8.3.1	Management of removable media	A.8.3 Media handling. Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.
Applicable - implemented	A.8.3.2	Disposal of media	A.8.3 Media handling. Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.
Applicable - implemented	A.8.3.3	Physical media transfer	A.8.3 Media handling. Objective: To prevent unauthorised disclosure, modification, removal or destruction of information stored on media.
Applicable - implemented	A.9.1.1	Access control policy	A.9.1 Business requirements of access control. Objective: To limit access to information and information processing facilities.
Applicable - implemented	A.9.1.2	Access to networks and network services	A.9.1 Business requirements of access control. Objective: To limit access to information and information processing facilities.
Applicable - implemented	A.9.2.1	User registration and de-registration	A.9.2 User access management. Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.
Applicable - implemented	A.9.2.2	User access provisioning	A.9.2 User access management. Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.
Applicable - implemented	A.9.2.3	Management of privileged access rights	A.9.2 User access management. Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.
Applicable - implemented	A.9.2.4	Management of secret authentication information of users	A.9.2 User access management. Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.
Applicable - implemented	A.9.2.5	Review of user access rights	A.9.2 User access management. Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.
Applicable - implemented	A.9.2.6	Removal or adjustment of access rights	A.9.2 User access management. Objective: To ensure authorised user access and to prevent unauthorised access to systems and services.
Applicable - implemented	A.9.3.1	Use of secret authentication information	A.9.3 User Responsibilities. Objective: To make users accountable for safeguarding their authentication information.
Applicable - implemented	A.9.4.1	Information access restriction	A.9.4 System and application access control
Applicable - implemented	A.9.4.2	Secure log-on procedures	A.9.4 System and application access control
Applicable - implemented	A.9.4.3	Password management system	A.9.4 System and application access control
Applicable - implemented	A.9.4.4	Use of privileged utility programmes	A.9.4 System and application access control
Applicable - implemented	A.9.4.5	Access control to programme source code	A.9.4 System and application access control
Applicable - implemented	A.10.1.1	Policy on the use of cryptographic controls	A.10.1 Cryptographic controls. Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Applicable - implemented	A.10.1.2	Key management	A.10.1 Cryptographic controls. Objective: To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.
Applicable - implemented	A.11.1.1	Physical security perimeter	A.11.1 Secure areas. Objective: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.
Applicable - implemented	A.11.1.2	Physical entry controls	A.11.1 Secure areas. Objective: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.
Applicable - implemented	A.11.1.3	Securing offices, rooms and facilities	A.11.1 Secure areas. Objective: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.
Applicable - implemented	A.11.1.4	Protecting against external and environmental threats	A.11.1 Secure areas. Objective: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.
Applicable - implemented	A.11.1.5	Working in secure areas	A.11.1 Secure areas. Objective: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.
Applicable - implemented	A.11.1.6	Delivery and loading areas	A.11.1 Secure areas. Objective: To prevent unauthorised physical access, damage and interference to the organization's information and information processing facilities.
Applicable - implemented	A.11.2.1	Equipment siting and protection	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.11.2.2	Supporting utilities	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.11.2.3	Cabling security	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.11.2.4	Equipment maintenance	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.11.2.5	Removal of assets	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.11.2.6	Security of equipment and assets off-premises	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.11.2.7	Secure disposal or reuse of equipment	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.11.2.8	Unattended user equipment	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.11.2.9	Clear desk and clear screen policy	A.11.2 Equipment. Objective: To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.
Applicable - implemented	A.12.1.1	Documented operating procedures	A.12.1 Operational procedures and responsibilities. Objective: To ensure correct and secure operations of information processing facilities.
Applicable - implemented	A.12.1.2	Change management	A.12.1 Operational procedures and responsibilities. Objective: To ensure correct and secure operations of information processing facilities.
Applicable - implemented	A.12.1.3	Capacity management	A.12.1 Operational procedures and responsibilities. Objective: To ensure correct and secure operations of information processing facilities.
Applicable - implemented	A.12.1.4	Separation of development, testing and operational environments	A.12.1 Operational procedures and responsibilities. Objective: To ensure correct and secure operations of information processing facilities.
Applicable - implemented	A.12.2.1	Controls against malware	A.12.2 Protection from malware. Objective: To ensure that information and information processing facilities are protected from malware.
Applicable - implemented	A.12.3.1	Information backup	A.12.3 Backup. Objective: To protect against loss of data.
Applicable - implemented	A.12.4.1	Event logging	A.12.4 Logging and monitoring. Objective: To record events and generate evidence.
Applicable - implemented	A.12.4.2	Protection of log information	A.12.4 Logging and monitoring. Objective: To record events and generate evidence.
Applicable - implemented	A.12.4.3	Administrator and operator logs	A.12.4 Logging and monitoring. Objective: To record events and generate evidence.
Applicable - implemented	A.12.4.4	Clock synchronization	A.12.4 Logging and monitoring. Objective: To record events and generate evidence.
Applicable - implemented	A.12.5.1	Installation of software on operational systems	A.12.5 Control of operational software. Objective: To ensure the integrity of operational systems.
Applicable - implemented	A.12.6.1	Management of technical vulnerabilities	A.12.6 Technical vulnerability management. Objective: To prevent exploitation of technical vulnerabilities.
Applicable - implemented	A.12.6.2	Restrictions on software installation	A.12.6 Technical vulnerability management. Objective: To prevent exploitation of technical vulnerabilities.
Applicable - implemented	A.12.7.1	Information systems audit controls	A.12.7 Information systems audit considerations. Objective: To minimise the impact of audit activities on operational systems.
Applicable - implemented	A.13.1.1	Network controls	A.13.1 Network security management. Objective: To ensure the protection of information in networks and its supporting information processing facilities.
Applicable - implemented	A.13.1.2	Security of network services	A.13.1 Network security management. Objective: To ensure the protection of information in networks and its supporting information processing facilities.
Applicable - implemented	A.13.1.3	Segregation in networks	A.13.1 Network security management. Objective: To ensure the protection of information in networks and its supporting information processing facilities.
Applicable - implemented	A.13.2.1	Information transfer policies and procedures	A.13.2 Information transfer. Objective: To maintain the security of information transferred within an organization and any external entity.
Applicable - implemented	A.13.2.2	Agreements on information transfer	A.13.2 Information transfer. Objective: To maintain the security of information transferred within an organization and any external entity.
Applicable - implemented	A.13.2.3	Electronic messaging	A.13.2 Information transfer. Objective: To maintain the security of information transferred within an organization and any external entity.
Applicable - implemented	A.13.2.4	Confidentiality or non-disclosure agreements	A.13.2 Information transfer. Objective: To maintain the security of information transferred within an organization and any external entity.
Applicable - implemented	A.14.1.1	Information security requirements analysis and specification	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 networks.
Applicable - implemented	A.14.1.2	Securing application services on public networks	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 networks.
Applicable - implemented	A.14.1.3	Protecting application services transactions	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 networks.
Applicable - implemented	A.14.2.1	Secure development policy	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.
Applicable - implemented	A.14.2.2	System change control procedures	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.
Applicable - implemented	A.14.2.3	Technical review of applications after operating platform changes	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.
Applicable - implemented	A.14.2.4	Restrictions on changes to software packages	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.
Applicable - implemented	A.14.2.5	Secure system engineering principles	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.
Applicable - implemented	A.14.2.6	Secure development environment	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.
Applicable - implemented	A.14.2.7	Outsourced development	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.
Applicable - implemented	A.14.2.8	System security testing	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.
Applicable - implemented	A.14.2.9	System acceptance testing	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.
Applicable - implemented	A.14.3.1	Protection of test data	A.14.3 Test data. Objective: To ensure the protection of data used for testing.
Applicable - implemented	A.15.1.1	Information security policy for supplier (and other important) relationships	A.15.1 Information security in supplier and other important relationships. Objective: To ensure protection of the organization's assets that is accessible by suppliers (and other important relationships affecting delivery).
Applicable - implemented	A.15.1.2	Addressing security within supplier (and other important relationships) agreements	A.15.1 Information security in supplier and other important relationships. Objective: To ensure protection of the organization's assets that is accessible by suppliers (and other important relationships affecting delivery).
Applicable - implemented	A.15.1.3	Information and communication technology supply chain	A.15.1 Information security in supplier and other important relationships. Objective: To ensure protection of the organization's assets that is accessible by suppliers (and other important relationships affecting delivery).
Applicable - implemented	A.15.2.1	Monitoring and review of supplier services (and other important delivery relationships)	A.15.2 Supplier and other important relationship service delivery management. Objective: To maintain an agreed level of information security and service delivery in line with supplier (and other important delivery relationships) agreements.
Applicable - implemented	A.15.2.2	Managing changes to supplier (and other important delivery relationships) services	A.15.2 Supplier and other important relationship service delivery management. Objective: To maintain an agreed level of information security and service delivery in line with supplier (and other important delivery relationships) agreements.
Applicable - implemented	A.16.1.1	Responsibilities and procedures	A.16.1 Management of 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.
Applicable - implemented	A.16.1.2	Reporting information security events	A.16.1 Management of 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.
Applicable - implemented	A.16.1.3	Reporting information security weaknesses	A.16.1 Management of 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.
Applicable - implemented	A.16.1.4	Assessment of and decision on information security events	A.16.1 Management of 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.
Applicable - implemented	A.16.1.5	Response to information security events	A.16.1 Management of 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.
Applicable - implemented	A.16.1.6	Learning from information security incidents	A.16.1 Management of 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.
Applicable - implemented	A.16.1.7	Collection of evidence	A.16.1 Management of 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.
Applicable - implemented	A.17.1.1	Planning information security continuity	A.17.1 Information security continuity
Applicable - implemented	A.17.1.2	Implementing information security continuity	A.17.1 Information security continuity
Applicable - implemented	A.17.1.3	Verify, review and evaluate information security continuity	A.17.1 Information security continuity
Applicable - implemented	A.17.2.1	Availability of information processing facilities	A.17.2 Redundancies. Objective: To ensure availability of information processing facilities.
Applicable - implemented	A.18.1.1	Identification of applicable legislation and contractual requirements	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.
Applicable - implemented	A.18.1.2	Intellectual property rights	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.
Applicable - implemented	A.18.1.3	Protection of records	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.
Applicable - implemented	A.18.1.4	Privacy and protection of personally identifiable information	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.
Applicable - implemented	A.18.1.5	Regulation of cryptographic controls	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.
Applicable - implemented	A.18.2.1	Independent review of information security	A.18.2 Information security reviews. Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.
Applicable - implemented	A.18.2.2	Compliance with security policies and standards	A.18.2 Information security reviews. Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.
Applicable - implemented	A.18.2.3	Technical compliance review	A.18.2 Information security reviews. Objective: To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.