

ISO 27001 – Kudos Research (Lumanity)
Statement of Applicability ("comply or explain" principle), version 2.0 February 2022

Group	Topic	Control Description	Justification for Inclusion
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	<i>Control</i> A set of policies for information security shall be defined, approved by management, published and communicated to employees and relevant external parties.	Policies across the ISMS provide guidance for how the ISMS is to be implemented and adopted
A.5.1.2	Review of the policies for information security	<i>Control</i> The policies for information security shall be reviewed at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.	Policy Reviews will be conducted
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	<i>Control</i> All information security responsibilities shall be defined and allocated.	Applicable to the ISMS within this organisation.

A.6.1.2	Segregation of duties	<i>Control</i>	
		Conflicting duties and areas of responsibility shall be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.	Applicable to the ISMS within this organisation.
A.6.1.3	Contact with authorities	<i>Control</i>	
		Appropriate contacts with relevant authorities shall be maintained.	Applicable to the ISMS within this organisation.
A.6.1.4	Contact with special interest groups	<i>Control</i>	
		Appropriate contacts with special interest groups or other specialist security forums and professional associations shall be maintained.	Applicable to the ISMS within this organisation.
A.6.1.5	Information security in project management	<i>Control</i>	
		Information security shall be addressed in project management, regardless of the type of the project.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	
		A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Applicable to the ISMS within this organisation.
A.6.2.2	Teleworking	<i>Control</i>	

		A policy and supporting security measures shall be implemented to protect information accessed, processed or stored at teleworking sites.	Applicable to the ISMS within this organisation.
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	<i>Control</i> Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.	Applicable to the ISMS within this organisation.
A.7.1.2	Terms and conditions of employment	<i>Control</i> The contractual agreements with employees and contractors shall state their and the organization's responsibilities for information security.	Applicable to the ISMS within this organisation.
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	<i>Control</i> Management shall require all employees and contractors to apply information security in accordance with the established policies and procedures of the organization.	Applicable to the ISMS within this organisation.

A.7.2.2	Information security awareness, education and training	<i>Control</i>	Applicable to the ISMS within this organisation.
		All employees of the organization and, where relevant, contractors shall receive appropriate awareness education and training and regular updates in organizational policies and procedures, as relevant for their job function.	
A.7.2.3	Disciplinary process	<i>Control</i>	Applicable to the ISMS within this organisation.
		There shall be a formal and communicated disciplinary process in place to take action against employees who have committed an information security breach.	
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	<i>Control</i>	Applicable to the ISMS within this organisation.
		Information security responsibilities and duties that remain valid after termination or change of employment shall be defined, communicated to the employee or contractor and enforced.	
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	<i>Control</i>	Applicable to the ISMS within this organisation.
		Assets associated with information and information processing facilities shall be identified and an inventory of these assets shall be drawn up and maintained.	
A.8.1.2	Ownership of assets	<i>Control</i>	

		Assets maintained in the inventory shall be owned.	Applicable to the ISMS within this organisation.
A.8.1.3	Acceptable use of assets	<i>Control</i>	
		Rules for the acceptable use of information and of assets associated with information and information processing facilities shall be identified, documented and implemented.	Applicable to the ISMS within this organisation.
A.8.1.4	Return of assets	<i>Control</i>	
		All employees and external party users shall return all of the organizational assets in their possession upon termination of their employment, contract or agreement.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	
		Information shall be classified in terms of legal requirements, value, criticality and sensitivity to unauthorised disclosure or modification.	Applicable to the ISMS within this organisation.
A.8.2.2	Labelling of information	<i>Control</i>	
		An appropriate set of procedures for information labelling shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable to the ISMS within this organisation.
A.8.2.3	Handling of assets	<i>Control</i>	

		Procedures for handling assets shall be developed and implemented in accordance with the information classification scheme adopted by the organization.	Applicable to the ISMS within this organisation.
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	<i>Control</i> Procedures shall be implemented for the management of removable media in accordance with the classification scheme adopted by the organization.	Applicable to the ISMS within this organisation.
A.8.3.2	Disposal of media	<i>Control</i> Media shall be disposed of securely when no longer required, using formal procedures.	Applicable to the ISMS within this organisation.
A.8.3.3	Physical media transfer	<i>Control</i>	

		Media containing information shall be protected against unauthorized access, misuse or corruption during transportation.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	
		An access control policy shall be established, documented and reviewed based on business and information security requirements.	Applicable to the ISMS within this organisation.
A.9.1.2	Access to networks and network services	<i>Control</i>	
		Users shall only be provided with access to the network and network services that they have been specifically authorized to use.	Applicable to the ISMS within this organisation.
A.9.2 User access management			
Objective: To ensure authorized user access and to prevent unauthorized access to systems and services.			
A.9.2.1	User registration and de-registration	<i>Control</i>	
		A formal user registration and de-registration process shall be implemented to enable assignment of access rights.	Applicable to the ISMS within this organisation.
A.9.2.2	User access provisioning	<i>Control</i>	
		A formal user access provisioning process shall be implemented to assign or revoke access rights for all user types to all systems and services.	Applicable to the ISMS within this organisation.
A.9.2.3	Management of privileged access rights	<i>Control</i>	
		The allocation and use of privileged access rights shall be restricted and controlled.	Applicable to the ISMS within this organisation.
A.9.2.4	Management of secret authentication information of users	<i>Control</i>	
		The allocation of secret authentication information shall be controlled through a formal management process.	Applicable to the ISMS within this organisation.

A.9.2.5	Review of user access rights	<i>Control</i>	
		Asset owners shall review users' access rights at regular intervals.	Applicable to the ISMS within this organisation.
A.9.2.6	Removal or adjustment of access rights	<i>Control</i>	
		The access rights of all employees and external party users to information and information processing facilities shall be removed upon termination of their employment, contract or agreement, or adjusted upon change.	Applicable to the ISMS within this organisation.
A.9.3 User responsibilities			
Objective: To make users accountable for safeguarding their authentication information.			
A.9.3.1	Use of secret authentication information	<i>Control</i>	
		Users shall be required to follow the organization's practices in the use of secret authentication information.	Applicable to the ISMS within this organisation.
A.9.4 System and application access control			
Objective: To prevent unauthorized access to systems and applications.			
A.9.4.1	Information access restriction	<i>Control</i>	
		Access to information and application system functions shall be restricted in accordance with the access control policy.	Applicable to the ISMS within this organisation.
A.9.4.2	Secure log-on procedures	<i>Control</i>	
		Where required by the access control policy, access to systems and applications shall be controlled by a secure log-on procedure.	Applicable to the ISMS within this organisation.
A.9.4.3	Password management system	<i>Control</i>	
		Password management systems shall be interactive and shall ensure quality passwords.	Applicable to the ISMS within this organisation.
A.9.4.4	Use of privileged utility programs	<i>Control</i>	
		The use of utility programs that might be capable of overriding system and application controls shall be restricted and tightly controlled.	Applicable to the ISMS within this organisation.
A.9.4.5		<i>Control</i>	

	Access control to program source code	Access to program source code shall be restricted.	Applicable to the ISMS within this organisation.
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	<i>Control</i> A policy on the use of cryptographic controls for protection of information shall be developed and implemented.	Applicable to the ISMS within this organisation.
A.10.1.2	Key management	<i>Control</i> A policy on the use, protection and lifetime of cryptographic keys shall be developed and implemented through their whole lifecycle.	Applicable to the ISMS within this organisation.
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	<i>Control</i> Security perimeters shall be defined and used to protect areas that contain either sensitive or critical information and information processing facilities.	Applicable to the ISMS within this organisation.
A.11.1.2	Physical entry controls	<i>Control</i> Secure areas shall be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	Applicable to the ISMS within this organisation.
A.11.1.3		<i>Control</i>	

	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed and applied.	Applicable to the ISMS within this organisation.
A.11.1.4	Protecting against external and environmental threats	<i>Control</i>	
		Physical protection against natural disasters, malicious attack or accidents shall be designed and applied.	Applicable to the ISMS within this organisation.
A.11.1.5	Working in secure areas	<i>Control</i>	
		Procedures for working in secure areas shall be designed and applied.	Applicable to the ISMS within this organisation.
A.11.1.6	Delivery and loading areas	Control	
		Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.	Not applicable
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	<i>Control</i>	
		Equipment shall be sited and protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.	Applicable to the ISMS within this organisation.
A.11.2.2	Supporting utilities	Control	

		Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Applicable to the ISMS within this organisation.
A.11.2.3	Cabling security	<i>Control</i>	
		Power and telecommunications cabling carrying data or supporting information services shall be protected from interception, interference or damage.	Applicable to the ISMS within this organisation.
A.11.2.4	Equipment maintenance	<i>Control</i>	
		Equipment shall be correctly maintained to ensure its continued availability and integrity.	Applicable to the ISMS within this organisation.
A.11.2.5	Removal of assets	<i>Control</i>	
		Equipment, information or software shall not be taken off-site without prior authorization.	Applicable to the ISMS within this organisation.
A.11.2.6	Security of equipment and assets off-premises	<i>Control</i>	
		Security shall be applied to off-site assets taking into account the different risks of working outside the organization's premises.	Applicable to the ISMS within this organisation.
A.11.2.7	Secure disposal or reuse of equipment	<i>Control</i>	
		All 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.	Applicable to the ISMS within this organisation.
A.11.2.8	Unattended user equipment	<i>Control</i>	

		Users shall ensure that unattended equipment has appropriate protection.	Applicable to the ISMS within this organisation.
A.11.2.9	Clear desk and clear screen policy	Control	
		A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities shall be adopted.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	
		Operating procedures shall be documented and made available to all users who need them.	Applicable to the ISMS within this organisation.
A.12.1.2	Change management	<i>Control</i>	
		Changes to the organization, business processes, information processing facilities and systems that affect information security shall be controlled.	Applicable to the ISMS within this organisation.
A.12.1.3	Capacity management	<i>Control</i>	
		The use of resources shall be monitored, tuned and projections made of future capacity requirements to ensure the required system performance.	Applicable to the ISMS within this organisation.
A.12.1.4	Separation of development, testing and operational environments	<i>Control</i>	
		Development, testing, and operational environments shall be separated to reduce the risks of unauthorized access or changes to the operational environment.	Applicable to the ISMS within this organisation.
A.12.2 Protection from malware			

Objective: To ensure that information and information processing facilities are protected against malware.			
A.12.2.1	Controls against malware	<i>Control</i>	
		Detection, prevention and recovery controls to protect against malware shall be implemented, combined with appropriate user awareness.	Applicable to the ISMS within this organisation.
A.12.3 Backup			
Objective: To protect against loss of data.			
A.12.3.1	Information backup	<i>Control</i>	
		Backup copies of information, software and system images shall be taken and tested regularly in accordance with an agreed backup policy.	Applicable to the ISMS within this organisation.
A.12.4 Logging and monitoring			
Objective: To record events and generate evidence.			
A.12.4.1	Event logging	<i>Control</i>	
		Event logs recording user activities, exceptions, faults and information security events shall be produced, kept and regularly reviewed.	Applicable to the ISMS within this organisation.
A.12.4.2	Protection of log information	<i>Control</i>	
		Logging facilities and log information shall be protected against tampering and unauthorized access.	Applicable to the ISMS within this organisation.
A.12.4.3	Administrator and operator logs	<i>Control</i>	

		System administrator and system operator activities shall be logged and the logs protected and regularly reviewed.	Applicable to the ISMS within this organisation.
A.12.4.4	Clock synchronisation	<i>Control</i>	
		The clocks of all relevant information processing systems within an organization or security domain shall be synchronised to a single reference time source.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	
		Procedures shall be implemented to control the installation of software on operational systems.	Applicable to the ISMS within this organisation.
A.12.6 Technical vulnerability management			
Objective: To prevent exploitation of technical vulnerabilities.			
A.12.6.1	Management of technical vulnerabilities	<i>Control</i>	
		Information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk.	Applicable to the ISMS within this organisation.
A.12.6.2	Restrictions on software installation	<i>Control</i>	
		Rules governing the installation of software by users shall be established and implemented.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	

		Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	
		Networks shall be managed and controlled to protect information in systems and applications.	Applicable to the ISMS within this organisation.
A.13.1.2	Security of network services	<i>Control</i>	
		Security mechanisms, service levels and management requirements of all network services shall be identified and included in network services agreements, whether these services are provided in-house or outsourced.	Applicable to the ISMS within this organisation.
A.13.1.3	Segregation in networks	<i>Control</i>	
		Groups of information services, users and information systems shall be segregated on networks.	Applicable to the ISMS within this organisation.
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		<i>Control</i>	

	Information transfer policies and procedures	Formal transfer policies, procedures and controls shall be in place to protect the transfer of information through the use of all types of communication facilities.	Applicable to the ISMS within this organisation.
A.13.2.2	Agreements on information transfer	<i>Control</i> Agreements shall address the secure transfer of business information between the organization and external parties.	Applicable to the ISMS within this organisation.
A.13.2.3	Electronic messaging	<i>Control</i> Information involved in electronic messaging shall be appropriately protected.	Applicable to the ISMS within this organisation.
A.13.2.4	Confidentiality or nondisclosure agreements	<i>Control</i> Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Applicable to the ISMS within this organisation.
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 networks.			
A.14.1.1	Information security requirements analysis and specification	<i>Control</i> The information security related requirements shall be included in the requirements for new information systems or enhancements to existing information systems.	Applicable to the ISMS within this organisation.
A.14.1.2		<i>Control</i>	

	Securing application services on public networks	Information involved in application services passing over public networks shall be protected from fraudulent activity, contract dispute and unauthorized disclosure and modification.	Applicable to the ISMS within this organisation.
A.14.1.3	Protecting application services transactions	<i>Control</i>	
		Information involved in application service transactions shall be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	
		Rules for the development of software and systems shall be established and applied to developments within the organization.	Applicable to the ISMS within this organisation.
A.14.2.2	System change control procedures	<i>Control</i>	
		Changes to systems within the development lifecycle shall be controlled by the use of formal change control procedures.	Applicable to the ISMS within this organisation.
A.14.2.3	Technical review of applications after operating platform changes	<i>Control</i>	
		When operating platforms are changed, business critical applications shall be reviewed and tested to ensure there is no adverse impact on organizational operations or security.	Applicable to the ISMS within this organisation.
A.14.2.4	Restrictions on changes to software packages	<i>Control</i>	
		Modifications to software packages shall be discouraged, limited to necessary changes and all changes shall be strictly controlled.	Applicable to the ISMS within this organisation.

A.14.2.5	Secure system engineering principles	<i>Control</i>	
		Principles for engineering secure systems shall be established, documented, maintained and applied to any information system implementation efforts.	Applicable to the ISMS within this organisation.
A.14.2.6	Secure development environment	<i>Control</i>	
		Organizations shall establish and appropriately protect secure development environments for system development and integration efforts that cover the entire system development lifecycle.	Applicable to the ISMS within this organisation.
A.14.2.7	Outsourced development	<i>Control</i>	
		The organization shall supervise and monitor the activity of outsourced system development.	Applicable to the ISMS within this organisation.
A.14.2.8	System security testing	<i>Control</i>	
		Testing of security functionality shall be carried out during development.	Applicable to the ISMS within this organisation.
A.14.2.9	System acceptance testing	<i>Control</i>	
		Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Applicable to the ISMS within this organisation.
A.14.3 Test data			
Objective: To ensure the protection of data used for testing.			
A.14.3.1	Protection of test data	<i>Control</i>	

		Test data shall be selected carefully, protected and controlled.	Applicable to the ISMS within this organisation.
A.15 Supplier relationships			
A.15.1 Information security in supplier relationships			
Objective: To ensure protection of the organization's assets that is accessible by suppliers.			
A.15.1.1	Information security policy for supplier relationships	<i>Control</i> Information security requirements for mitigating the risks associated with supplier's access to the organization's assets shall be agreed with the supplier and documented.	Applicable to the ISMS within this organisation.
A.15.1.2	Addressing security within supplier agreements	<i>Control</i> All relevant information security requirements shall be established and agreed with each supplier that may access, process, store, communicate, or provide IT infrastructure components for, the organization's information.	Applicable to the ISMS within this organisation.
A.15.1.3		<i>Control</i>	

	Information and communication technology supply chain	Agreements with suppliers shall include requirements to address the information security risks associated with information and communications technology services and product supply chain.	Applicable to the ISMS within this organisation.
A.15.2 Supplier service delivery management			
Objective: To maintain an agreed level of information security and service delivery in line with supplier agreements.			
A.15.2.1	Monitoring and review of supplier services	<i>Control</i> Organizations shall regularly monitor, review and audit supplier service delivery.	Applicable to the ISMS within this organisation.
A.15.2.2	Managing changes to supplier services	<i>Control</i> Changes to the provision of services by suppliers, including maintaining and improving existing information security policies, procedures and controls, shall be managed, taking account of the criticality of business information, systems and processes involved re-assessment of risks.	Applicable to the ISMS within this organisation.
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	<i>Control</i> Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Applicable to the ISMS within this organisation.
A.16.1.2	Reporting information security events	<i>Control</i> Information security events shall be reported through appropriate management channels as quickly as possible.	Applicable to the ISMS within this organisation.

A.16.1.3	Reporting information security weaknesses	<i>Control</i>	
		Employees and contractors using the organization's information systems and services shall be required to note and report any observed or suspected information security weaknesses in systems or services.	Applicable to the ISMS within this organisation.
A.16.1.4	Assessment of and decision on information security events	<i>Control</i>	
		Information security events shall be assessed and it shall be decided if they are to be classified as information security incidents.	Applicable to the ISMS within this organisation.
A.16.1.5	Response to information security incidents	<i>Control</i>	
		Information security incidents shall be responded to in accordance with the documented procedures.	Applicable to the ISMS within this organisation.
A.16.1.6	Learning from information security incidents	<i>Control</i>	
		Knowledge gained from analysing and resolving information security incidents shall be used to reduce the likelihood or impact of future incidents.	Applicable to the ISMS within this organisation.
A.16.1.7	Collection of evidence	<i>Control</i>	
		The organization shall define and apply procedures for the identification, collection, acquisition and preservation of information, which can serve as evidence.	Applicable to the ISMS within this organisation.
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	<i>Control</i>	
		The organization shall determine its requirements for information security and the continuity of information security management in adverse situations, e.g. during a crisis or disaster.	Applicable to the ISMS within this organisation.
A.17.1.2		<i>Control</i>	

	Implementing information security continuity	The organization shall establish, document, implement and maintain processes, procedures and controls to ensure the required level of continuity for information security during an adverse situation.	Applicable to the ISMS within this organisation.
A.17.1.3	Verify, review and evaluate information security continuity	<i>Control</i>	
		The organization shall verify the established and implemented information security continuity controls at regular intervals in order to ensure that they are valid and effective during adverse situations.	Applicable to the ISMS within this organisation.
A.17.2 Redundancies			
Objective: To ensure availability of information processing facilities.			
A.17.2.1	Availability of information processing facilities	<i>Control</i>	
		Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Applicable to the ISMS within this organisation.
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 legislation and contractual requirements	<i>Control</i>	
		All relevant legislative statutory, regulatory, contractual requirements and the organization's approach to meet these requirements shall be explicitly identified, documented and kept up to date for each information system and the organization.	Applicable to the ISMS within this organisation.
A.18.1.2	Intellectual property rights	<i>Control</i>	
		Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products.	Applicable to the ISMS within this organisation.
A.18.1.3	Protection of records	<i>Control</i>	

		Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.	Applicable to the ISMS within this organisation.
A.18.1.4	Privacy and protection of personally identifiable information	<i>Control</i> Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Applicable to the ISMS within this organisation.
A.18.1.5	Regulation of cryptographic controls	<i>Control</i> Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Applicable to the ISMS within this organisation.
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	<i>Control</i> The organization's approach to managing information security and its implementation (i.e. control objectives, controls, policies, processes and procedures for information security) shall be reviewed independently at planned intervals or when significant changes occur.	Applicable to the ISMS within this organisation.
A.18.2.2	Compliance with security policies and standards	<i>Control</i> Managers shall regularly review the compliance of information processing and procedures within their area of responsibility with the appropriate security policies, standards and any other security requirements.	Applicable to the ISMS within this organisation.
A.18.2.3	Technical compliance review	<i>Control</i>	

		Information systems shall be regularly reviewed for compliance with the organization's information security policies and standards.	Applicable to the ISMS within this organisation.
--	--	---	--

Reviewed and authorised:

Date: 18/01/2023

A handwritten signature in black ink, appearing to read 'ahsahim'.