

Statement of Applicability as of 08/27/2020

ISO 27001:2013 Annex A Controls			Current Controls	Justification
Clause	Sec	Control Objective/Control		
Information Security Policies	5.1	Information Security Policy		
	Objective:	To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.		
	5.1.1	Policies for information security	■	
	5.1.2	Review of the policies for information security	■	
Organization of Information security	6.1	Internal Organization		
	Objective:	To establish a management framework to initiate and control the implementation and operation of information security within the organization.		
	6.1.1	Information security roles and responsibilities	■	
	6.1.2	Segregation of duties	■	
	6.1.3	Contact with authorities	■	
	6.1.4	Contact with special interest groups	■	
	6.1.5	Information security in project management	■	
	6.2	Mobile devices and teleworking		
	Objective:	To ensure the security of teleworking and use of mobile devices.		
	6.2.1	Mobile device policy	■	
6.2.2	Teleworking	■		
Human Resources Security	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.		
	7.1.1	Screening	■	
	7.1.2	Terms and conditions of employment	■	
	7.2	During Employment		
	Objective:	To ensure that employees and contractors are aware of and fulfil their information security responsibilities.		
	7.2.1	Management Responsibility	■	
	7.2.2	Information security awareness, education and training	■	
	7.2.3	Disciplinary process	■	
	7.3	Termination or change of employment		
Objective:	To protect the organization's interests as part of the process of changing or terminating employment.			
7.3.1	Termination or change of employment responsibilities	■		
Asset Management	8.1	Responsibility for assets		
	Objective:	To achieve and maintain appropriate protection of organizational assets.		
	8.1.1	Inventory of assets	■	
	8.1.2	Ownership of assets	■	
	8.1.3	Acceptable use of assets	■	
	8.1.4	Return of assets	■	
	8.2	Information classification		
	Objective:	To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.		
8.2.1	Classification of information	■		
8.2.2	Labelling of information	■		

	8.2.3	Handling of assets	■	
	8.3	Media Handling		
	Objective:	To prevent unauthorized disclosure, modification, removal or destruction of information stored on media.		
	8.3.1	Management of removable media	■	
	8.3.2	Disposal of media	■	
	8.3.3	Physical media transfer	■	
Access Control	9.1	Business Requirements of Access Control		
	Objective:	To limit access to information and information processing facilities.		
	9.1.1	Access control policy	■	
	9.1.2	Access to networks and network services	■	
	9.2	User Access Management		
	Objective:	To ensure authorized user access and to prevent unauthorized access to systems and services.		
	9.2.1	User Registration and de-registration	■	
	9.2.2	User access provisioning	■	
	9.2.3	Management of privileged access rights	■	
	9.2.4	Management of secret authentication information of users	■	
	9.2.5	Review of user access rights	■	
	9.2.6	Removal or adjustment of access rights	■	
	9.3	User Responsibilities		
	Objective:	To make users accountable for safeguarding their authentication information.		
	9.3.1	Use of secret authentication information	■	
	9.4	System and application access control		
	Objective:	To prevent unauthorized access to systems and applications.		
	9.4.1	Information access restriction	■	
	9.4.2	Secure log-on procedures	■	
	9.4.3	Password management system	■	
9.4.4	Use of privileged utility programs	■		
9.4.5	Access control to program source code	■		
Cryptography	10.1	Cryptographic controls		
	Objective:	To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.		
	10.1.1	Policy on the use of cryptographic controls	■	
	10.1.2	Key management	■	
Physical and Environmental Security	11.1	Secure Areas		
	Objective:	To prevent unauthorized physical access, damage and interference to the organization's information and information processing facilities.		
	11.1.1	Physical security perimeter	■	
	11.1.2	Physical entry controls	■	
	11.1.3	Securing offices, rooms and facilities	■	
	11.1.4	Protecting against external and environmental threats	■	

11.1.5	Working in secure areas	■	
11.1.6	Delivery and loading areas	■	
11.2	Equipment security		
Objective:	To prevent loss, damage, theft or compromise of assets and interruption to the organization's operations.		
11.2.1	Equipment sitting and protection	■	
11.2.2	Support utilities	■	
11.2.3	Cabling security	■	
11.2.4	Equipment Maintenance	■	
11.2.5	Removal of assets	■	
11.2.6	Security of equipment and assets off-premises	■	
11.2.7	Secure disposal or reuse of equipment	■	
11.2.8	Unattended user equipment	■	
11.2.9	Clear desk and clear screen policy	■	

--	--	--	--

Operations Security

12.1	Operational procedures and responsibilities		
Objective:	To ensure correct and secure operations of information processing facilities.		
12.1.1	Documented operating procedures	■	
12.1.2	Change Management	■	
12.1.3	Capacity management	■	
12.1.4	Separation of development, testing and operational environments	■	
12.2	Protection from malware		
Objective:	To ensure that information and information processing facilities are protected against malware.		
12.2.1	Controls against malware	■	
12.3	Backup		
Objective:	To protect against loss of data.		
12.3.1	Information backup	■	
12.4	Logging and monitoring		
Objective:	To record events and generate evidence.		
12.4.1	Event logging	■	
12.4.2	Protection of log information	■	
12.4.3	Administrator and operator logs	■	
12.4.4	Clock synchronization	■	
12.5	Control of operational software		
Objective:	To ensure the integrity of operational systems.		
12.5.1	Installation of software on operational systems	■	
12.6	Technical Vulnerability Management		

	Objective:	To prevent exploitation of technical vulnerabilities.		
	12.6.1	Management of technical vulnerabilities	■	
	12.6.2	Restrictions on software installation	■	
	12.7	Information systems audit considerations		
	Objective:	To minimise the impact of audit activities on operational systems.		
	12.7.1	Information systems audit controls	■	
Communications Security	13.1	Network Security Management		
	Objective:	To ensure the protection of information in networks and its supporting information processing facilities.		
	13.1.1	Network controls	■	
	13.1.2	Security of network services	■	
	13.1.3	Security of network services	■	
	13.2	Information transfer		
	Objective:	To maintain the security of information transferred within an organization and with any external entity.		
	13.2.1	Information transfer policies and procedures	■	
	13.2.2	Agreements on information transfer	■	
	13.2.3	Electronic messaging	■	
	13.2.4	Confidentiality or nondisclosure agreements	■	
Systems Acquisition, Development and Maintenance	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.		
	14.1.1	Information security requirements analysis and specification	■	
	14.1.2	Securing application services on public networks	■	
	14.1.3	Protecting application services transactions	■	
	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.		
	14.2.1	Secure development policy		Not in scope
	14.2.2	System change control procedures	■	
	14.2.3	Technical review of applications after operating platform changes	■	
	14.2.4	Restrictions on changes to software packages	■	
	14.2.5	Secure system engineering principles	■	
	14.2.6	Secure development environment	■	
	14.2.7	Outsourced development	■	
	14.2.8	System security testing		Not in scope
14.2.9	System acceptance		Not in scope	
14.3	Test data			

	Objective:	To ensure the protection of data used for testing.		
	14.3.1	Protection of system test data	■	
Supplier Relationships	15.1	Supplier relationships		
	Objective:	To ensure the protection of data used for testing.		
	15.1.1	Information security policy for supplier relationships	■	
	15.1.2	Addressing security within supplier agreements	■	
	15.1.3	Information and communication technology supply chain	■	
	15.2	Supplier service delivery management		
	Objective:	To maintain an agreed level of information security and service delivery in line with supplier agreements.		
	15.2.1	Monitoring and review of supplier services	■	
15.2.2	Managing changes to supplier services	■		
Information Security Incident Management	16.1	Management of information security incidents and improvements		
	Objective:	Objective: To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.		
	16.1.1	Responsibilities and procedures	■	
	16.1.2	Reporting Information security events	■	
	16.1.3	Reporting information security weaknesses	■	
	16.1.4	Assessment of and decision on information security events	■	
	16.1.5	Response to information security incidents	■	
	16.1.6	Learning from information security incidents	■	
	16.1.7	Collection of evidence	■	
Business Continuity Management	17.1	Information security continuity		
	Objective:	Information security continuity shall be embedded in the organization's business continuity management systems.		
	17.1.1	Planning information security continuity	■	
	17.1.2	Implementing information security continuity	■	
	17.1.3	Verify, review and evaluate information security continuity	■	
	17.2	Redundancies		
	Objective:	To ensure availability of information processing facilities.		
17.2.1	Availability of information processing facilities	■		
Compliance	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.		
	18.1.1	Identification of applicable legislation and contractual requirements	■	
	18.1.2	Intellectual property rights	■	

18.1.3	Protection of records	■	
18.1.4	Privacy and protection of personally identifiable information	■	
18.1.5	Regulation of cryptographic controls	■	
18.2	Information security reviews		
Objective:	To ensure that information security is implemented and operated in accordance with the organizational policies and procedures.		
18.2.1	Independent review of information security	■	
18.2.2	Compliance with security policies and standards	■	
18.2.3	Technical compliance review	■	