Statement Of Applicability

Nr.	Clause	Title	Description	Applicable	Implemented
	A.5	Information security policies			
	A.5.1	Management direction for information	To provide management direction and support for information security		
1	A.5.1.1	Policies for information security	A set of policies for information security shall be defined, approved by	Yes	Yes
2	A.5.1.2	Review of the policies for information	The policies for information security shall be reviewed at planned	Yes	Yes
	A.6	Organization of information security			
	A.6.1	Internal organization	To establish a management framework to initiate and control the		
3	A.6.1.1	Information security roles and	All information security responsibilities shall be defined and allocated.	Yes	Yes
4	A.6.1.2	Segregation of duties	Conflicting duties and areas of responsibility shall be segregated to	Yes	Yes
5	A.6.1.3	Contact with authorities	Appropriate contacts with relevant authorities shall be maintained.	Yes	Yes
6	A.6.1.4	Contact with special interest groups	Appropriate contacts with special interest groups or other specialist	Yes	Yes
7	A.6.1.5	Information security in project management	Information security shall be addressed in project management, regardless of the type of the project.	Yes	Yes
	A.6.2	Mobile devices and teleworking	To ensure the security of teleworking and use of mobile devices.		
8	A.6.2.1	Mobile device policy	A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.	Yes	Yes
9	A.6.2.2	Teleworking	A policy and supporting security measures shall be implemented to	Yes	Yes
	A.7	Human resource security			
	A.7.1	Prior to employment	To ensure that employees and contractors understand their		
10	A.7.1.1	Screening	Background verification checks on all candidates for employment	Yes	Yes
11	A.7.1.2	Terms and conditions of employment	The contractual agreements with employees and contractors shall	Yes	Yes
	A.7.2	During employment	To ensure that employees and contractors are aware of and fulfil their		
12	A.7.2.1	Management responsibilities	Management shall require all employees and contractors to apply	Yes	Yes
13	A.7.2.2	Information security awareness,	All employees of the organization and, where relevant, contractors	Yes	Yes
14	A.7.2.3	Disciplinary process	There shall be a formal and communicated disciplinary process in	Yes	Yes
	A.7.3	Termination and change of employment	To protect the organization's interests as part of the process of		
15	A.7.3.1	Termination or change of employment responsibilities	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.	Yes	Yes
	A.8	Asset management			
	A.8.1	Responsibility for assets	To identify organizational assets and define appropriate protection		
16	A.8.1.1	Inventory of assets	Assets associated with information and information processing	Yes	Yes
17	A.8.1.2	Ownership of assets	Assets maintained in the inventory shall be owned.	Yes	Yes
18	A.8.1.3	Acceptable use of assets	Rules for the acceptable use of information and of assets associated	Yes	Yes
19	A.8.1.4	Return of assets	All employees and external party users shall return all of the	Yes	Yes
	A.8.2	Information classification	To ensure that information receives an appropriate level of protection		
20	A.8.2.1	Classification of information	Information shall be classified in terms of legal requirements, value,	Yes	Yes
21	A.8.2.2	Labelling of information	An appropriate set of procedures for information labelling shall be	Yes	Yes
22	A.8.2.3	Handling of assets	Procedures for handling assets shall be developed and implemented	Yes	Yes
	A.8.3	Media handling	To prevent unauthorized disclosure, modification, removal or		
23	A.8.3.1	Management of removable media	Procedures shall be implemented for the management of removable	Yes	Yes
24	A.8.3.2	Disposal of media	Media shall be disposed of securely when no longer required, using	Yes	Yes
25	A.8.3.3	Physical media transfer	Media containing information shall be protected against unauthorized	Yes	Yes
	A.9	Access control			
	A.9.1	Business requirements of access	To limit access to information and information processing facilities.		
26	A.9.1.1	Access control policy	An access control policy shall be established, documented and	Yes	Yes
27	A.9.1.2	Access to networks and network	Users shall only be provided with access to the network and network	Yes	Yes
	A.9.2	User access management	To ensure authorized user access and to prevent unauthorized		
28	A.9.2.1	User registration and de-registration	A formal user registration and de-registration process shall be	Yes	Yes
29	A.9.2.2	User access provisioning	A formal user access provisioning process shall be implemented to	Yes	Yes
30	A.9.2.3	Management of privileged access	The allocation and use of privileged access rights shall be restricted	Yes	Yes
31	A.9.2.4	Management of secret authentication	The allocation of secret authentication information shall be controlled	Yes	Yes
32	A.9.2.5	Review of user access rights	Asset owners shall review users' access rights at regular intervals.	Yes	Yes
33	A.9.2.6	Removal or adjustment of access rights	The access rights of all employees and external party users to	Yes	Yes
	A.9.3	User responsibilities	To make users accountable for safeguarding their authentication		
34	A.9.3.1	Use of secret authentication	Users shall be required to follow the organization's practices in the	Yes	Yes
	A.9.4	System and application access control	To prevent unauthorized access to systems and applications.		
35	A.9.4.1	Information access restriction	Access to information and application system functions shall be	Yes	Yes
36	A.9.4.2	Secure log-on procedures	Where required by the access control policy, access to systems and	Yes	Yes
37	A.9.4.3	Password management system	Password management systems shall be interactive and shall ensure	Yes	Yes
38	A.9.4.4	Use of privileged utility programs	The use of utility programs that might be capable of overriding system	Yes	Yes
39	A.9.4.5	Access control to program source code	Access to program source code shall be restricted.	Yes	Yes
	A.10	Cryptography			
	A.10.1	Cryptographic controls	To ensure proper and effective use of cryptography to protect the		
40	A.10.1.1	Policy on the use of cryptographic	A policy on the use of cryptographic controls for protection of	Yes	Yes
41	A.10.1.2	Key management	A policy on the use, protection and lifetime of cryptographic keys shall	Yes	Yes
	A.11	Physical and environmental security			
	A.11.1	Secure areas	To prevent unauthorized physical access, damage and interference to		
42	A.11.1.1	Physical security perimeter	Security perimeters shall be defined and used to protect areas that	Yes	Yes
43	A.11.1.2	Physical entry controls	Secure areas shall be protected by appropriate entry controls to	Yes	Yes
44	A.11.1.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be designed	Yes	Yes
45	A.11.1.4	Protecting against external and	Physical protection against natural disasters, malicious attack or	Yes	Yes
46	A.11.1.5	Working in secure areas	Procedures for working in secure areas shall be designed and	Yes	Yes
47	A.11.1.6	Delivery and loading areas	Access points such as delivery and loading areas and other points	Yes	Yes
	A.11.2	Equipment	To prevent loss, damage, theft or compromise of assets and		
48	A.11.2.1	Equipment siting and protection	Equipment shall be sited and protected to reduce the risks from	Yes	Yes

49	A.11.2.2	Supporting utilities	Equipment shall be protected from power failures and other disruptions caused by failures in supporting utilities.	Yes	Yes
50	A.11.2.3	Cabling security	Power and telecommunications cabling carrying data or supporting	Yes	Yes
51	A.11.2.4	Equipment maintenance	Equipment shall be correctly maintained to ensure its continued	Yes	Yes
52	A.11.2.5	Removal of assets	Equipment, information or software shall not be taken off-site without	Yes	Yes
53	A.11.2.6	Security of equipment and assets off-	Security shall be applied to off-site assets taking into account the	Yes	Yes
54	A.11.2.7	Secure disposal or reuse of equipment	All items of equipment containing storage media shall be verified to	Yes	Yes
55	A.11.2.8	Unattended user equipment	Users shall ensure that unattended equipment has appropriate	Yes	Yes
56	A.11.2.9	Clear desk and clear screen policy	A clear desk policy for papers and removable storage media and a	Yes	Yes
	A.12	Operations security			
	A.12.1	Operational procedures and	To ensure correct and secure operations of information processing		
57	A.12.1.1	Documented operating procedures	Operating procedures shall be documented and made available to all	Yes	Yes
58	A.12.1.2	Change management	Changes to the organization, business processes, information	Yes	Yes
59	A.12.1.3	Capacity management	The use of resources shall be monitored, tuned and projections made	Yes	Yes
60	A.12.1.4	Separation of development, testing and	Development, testing, and operational environments shall be	Yes	Yes
	A.12.2	Protection from malware	To ensure that information and information processing facilities are		
61	A.12.2.1	Controls against malware	Detection, prevention and recovery controls to protect against	Yes	Yes
	A.12.3	Backup	To protect against loss of data.		
62	A.12.3.1	Information backup	Backup copies of information, software and system images shall be	Yes	Yes
	A.12.4	Logging and monitoring	To record events and generate evidence.		
63	A.12.4.1	Event logging	Event logs recording user activities, exceptions, faults and	Yes	Yes
64	A.12.4.2	Protection of log information	Logging facilities and log information shall be protected against	Yes	Yes
65	A.12.4.3	Administrator and operator logs	System administrator and system operator activities shall be logged	Yes	Yes
66	A.12.4.4	Clock synchronisation	The clocks of all relevant information processing systems within an	Yes	Yes
	A.12.5	Control of operational software	To ensure the integrity of operational systems.		
67	A.12.5.1	Installation of software on operational	Procedures shall be implemented to control the installation of	Yes	Yes
	A.12.6	Technical vulnerability management	To prevent exploitation of technical vulnerabilities.		
68	A.12.6.1	Management of technical vulnerabilities	Information about technical vulnerabilities of information systems	Yes	Yes
69	A.12.6.2	Restrictions on software installation	Rules governing the installation of software by users shall be	Yes	Yes
	A.12.7	Information systems audit	To minimise the impact of audit activities on operational systems.		
70	A.12.7.1	Information systems audit controls	Audit requirements and activities involving verification of operational systems shall be carefully planned and agreed to minimise disruptions to business processes.	Yes	Yes
	A.13	Communications security			
	A.13.1	Network security management	To ensure the protection of information in networks and its supporting		
71	A.13.1.1	Network controls	Networks shall be managed and controlled to protect information in	Yes	Yes
72	A.13.1.2	Security of network services	Security mechanisms, service levels and management requirements	Yes	Yes
73	A.13.1.3	Segregation in networks	Groups of information services, users and information systems shall	Yes	Yes
	A.13.2	Information transfer	To maintain the security of information transferred within an		
74	A.13.2.1	Information transfer policies and	Formal transfer policies, procedures and controls shall be in place to	Yes	Yes
75	A.13.2.2	Agreements on information transfer	Agreements shall address the secure transfer of business information	Yes	Yes
76	A.13.2.3	Electronic messaging	Information involved in electronic messaging shall be appropriately	Yes	Yes
77	A.13.2.4	Confidentiality or nondisclosure agreements	Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information shall be identified, regularly reviewed and documented.	Yes	Yes
	A.14	System acquisition, development and			
	A.14.1	Security requirements of information	To ensure that information security is an integral part of information		
78	A.14.1.1	Information security requirements	The information security related requirements shall be included in the	Yes	Yes
79	A.14.1.2	Securing application services on public	Information involved in application services passing over public	Yes	Yes
80	A.14.1.3	Protecting application services	Information involved in application service transactions shall be	Yes	Yes
	A.14.2	Security in development and support	To ensure that information security is designed and implemented		
81	A.14.2.1	Secure development policy	Rules for the development of software and systems shall be	Yes	Yes
82	A.14.2.2	System change control procedures	Changes to systems within the development lifecycle shall be	Yes	Yes
83	A.14.2.3	Technical review of applications after	When operating platforms are changed, business critical applications	Yes	Yes
84	A.14.2.4	Restrictions on changes to software	Modifications to software packages shall be discouraged, limited to	Yes	Yes
85	A.14.2.5	Secure system engineering principles	Principles for engineering secure systems shall be established,	Yes	Yes
86	A.14.2.6	Secure development environment	Organizations shall establish and appropriately protect secure	Yes	Yes
87	A.14.2.7	Outsourced development	The organization shall supervise and monitor the activity of	No	No
88	A.14.2.8	System security testing	Testing of security functionality shall be carried out during	Yes	Yes
89	A.14.2.9	System acceptance testing	Acceptance testing programs and related criteria shall be established for new information systems, upgrades and new versions.	Yes	Yes
	A.14.3	Test data	To ensure the protection of data used for testing.		
90	A.14.3.1	Protection of test data	Test data shall be selected carefully, protected and controlled.	Yes	Yes
	A.15	Supplier relationships			
	A.15.1	Information security in supplier	To ensure protection of the organization's assets that is accessible by		
91	A.15.1.1	Information security policy for supplier	Information security requirements for mitigating the risks associated	Yes	Yes
92	A.15.1.2	Addressing security within supplier	All relevant information security requirements shall be established	Yes	Yes
93	A.15.1.3	Information and communication	Agreements with suppliers shall include requirements to address the	Yes	Yes
	A.15.2	Supplier service delivery management	To maintain an agreed level of information security and service		
94	A.15.2.1	Monitoring and review of supplier	Organizations shall regularly monitor, review and audit supplier	Yes	Yes
95	A.15.2.2	Managing changes to supplier services	Changes to the provision of services by suppliers, including	Yes	Yes
	A.16	Information security incident			
	A.16.1	Management of information security	To ensure a consistent and effective approach to the management of		
96	A.16.1.1	Responsibilities and procedures	Management responsibilities and procedures shall be established to ensure a quick, effective and orderly response to information security incidents.	Yes	Yes
97	A.16.1.2	Reporting information security events	Information security events shall be reported through appropriate	Yes	Yes
98	A.16.1.3	Reporting information security	Employees and contractors using the organization's information	Yes	Yes
99	A.16.1.4	Assessment of and decision on	Information security events shall be assessed and it shall be decided	Yes	Yes

100	A.16.1.5	Response to information security	Information security incidents shall be responded to in accordance	Yes	Yes
101	A.16.1.6	Learning from information security	Knowledge gained from analysing and resolving information security	Yes	Yes
102	A.16.1.7	Collection of evidence	The organization shall define and apply procedures for the	Yes	Yes
	A.17	Information security aspects of			
	A.17.1	Information security continuity	Information security continuity shall be embedded in the		
103	A.17.1.1	Planning information security continuity	The organization shall determine its requirements for information	Yes	Yes
104	A.17.1.2	Implementing information security	The organization shall establish, document, implement and maintain	Yes	Yes
105	A.17.1.3	Verify, review and evaluate information	The organization shall verify the established and implemented	Yes	Yes
	A.17.2	Redundancies	To ensure availability of information processing facilities.		
106	A.17.2.1	Availability of information processing facilities	Information processing facilities shall be implemented with redundancy sufficient to meet availability requirements.	Yes	Yes
	A.18	Compliance			
	A.18.1	Compliance with legal and contractual	To avoid breaches of legal, statutory, regulatory or contractual		
107	A.18.1.1	Identification of applicable legislation	All relevant legislative statutory, regulatory, contractual requirements	Yes	Yes
108	A.18.1.2	Intellectual property rights	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.	Yes	Yes
109	A.18.1.3	Protection of records	Records shall be protected from loss, destruction, falsification,	Yes	Yes
110	A.18.1.4	Privacy and protection of personally identifiable information	Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.	Yes	Yes
111	A.18.1.5	Regulation of cryptographic controls	Cryptographic controls shall be used in compliance with all relevant agreements, legislation and regulations.	Yes	Yes
	A.18.2	Information security reviews	To ensure that information security is implemented and operated in		
112	A.18.2.1	Independent review of information	The organization's approach to managing information security and its	Yes	Yes
113	A.18.2.2	Compliance with security policies and	Managers shall regularly review the compliance of information	Yes	Yes
114	A.18.2.3	Technical compliance review	Information systems shall be regularly reviewed for compliance with	Yes	Yes