Annex	Control	Description	Applicability
A.5	**Organisational Controls**		
A.5.1	Policies for information security	Information security policy and topic-specific policies	Applicable
A.5.2	Information security roles and responsibilities	Information security roles and responsibilities shall be	Applicable
A.5.3	Segregation of duties	Conflicting duties and conflicting areas of responsibility	Applicable
A.5.4	Management responsibilities	Management shall require all personnel to apply	Applicable
A.5.5	Contact with authorities	The organization shall establish and maintain contact	Applicable
A.5.6	Contact with special interest groups	The organization shall establish and maintain contact	Applicable
A.5.7	Threat intelligence	Information relating to information security threats shall	Applicable
A.5.8	Information security in project management	Information security shall be integrated into project	Applicable
A.5.9	Inventory of information and other associated assets	An inventory of information and other associated assets,	Applicable
A.5.10	Acceptable use of information and other associated	Rules for the acceptable use and procedures for	Applicable
A.5.11	Return of assets	Personnel and other interested parties as appropriate	Applicable
A.5.12	Classification of information	Information shall be classified according to the	Applicable
A.5.13	Labelling of information	An appropriate set of procedures for information	Applicable
A.5.14	Information transfer	Information transfer rules, procedures, or agreements	Applicable
A.5.15	Access control	Rules to control physical and logical access to	Applicable
A.5.16	Identity management	The full life cycle of identities shall be managed.	Applicable
A.5.17	Authentication information	Allocation and management of authentication	Applicable
A.5.18	Access rights	Access rights to information and other associated assets	Applicable
A.5.19	Information security in supplier relationships	Processes and procedures shall be defined and	Applicable
A.5.20	Addressing information security within supplier	Relevant information security requirements shall be	Applicable
A.5.21	Managing information security in the ICT supply chain	Processes and procedures shall be defined and	Applicable
A.5.22	Monitoring, review and change management of supplier	The organization shall regularly monitor, review,	Applicable
A.5.23	Information security for use of cloud services	Processes for acquisition, use, management and exit	Applicable
A.5.24	Information security incident management planning and	The organization shall plan and prepare for managing	Applicable
A.5.25	Assessment and decision on information security events	The organization shall assess information security	Applicable
A.5.26	Response to information security incidents	Information security incidents shall be responded to in	Applicable
A.5.27	Learning from information security incidents	Knowledge gained from information security incidents	Applicable
A.5.28	Collection of evidence	The organization shall establish and implement	Applicable
A.5.29	Information security during disruption	The organization shall plan how to maintain information	Applicable
A.5.30	ICT readiness for business continuity	ICT readiness shall be planned, implemented,	Applicable
A.5.31	Legal statutory regulatory and contractual requirements	Legal, statutory, regulatory and contractual	Applicable
A.5.32	Intellectual property rights	The organization shall implement appropriate	Applicable
A.5.33	Protection of records	Records shall be protected from loss, destruction,	Applicable
A.5.34	Privacy and protection of PII	The organization shall identify and meet the	Applicable
A.5.35	Independent review of information security	The organization's approach to managing information	Applicable
A.5.36	Compliance with policies, rules and standards for	Compliance with the organization's information security	Applicable
A.5.37	Documented operating procedures	Operating procedures for information processing	Applicable
A.6	**People Controls**		
A.6.1	Screening	Background verification checks on all candidates to	Applicable
A.6.2	Terms and conditions of employment	The employment contractual agreements shall state the	Applicable
A.6.3	Information security awareness education and training	Personnel of the organization and relevant interested	Applicable
A.6.4	Disciplinary process	A disciplinary process shall be formalized and	Applicable
A.6.5	Responsibilities after termination or change of	Information security responsibilities and duties that	Applicable
A.6.6	Confidentiality or non-disclosure agreements	Confidentiality or non-disclosure agreements reflecting	Applicable
A.6.7	Remote working	Security measures shall be implemented when	Applicable
A.6.8	Information security event reporting	The organization shall provide a mechanism for	Applicable
A.7	**Physical Controls**		
A.7.1	Physical security perimeters	Security perimeters shall be defined and used to protect	Applicable
A.7.2	Physical entry	Secure areas shall be protected by appropriate entry	Applicable
A.7.3	Securing offices, rooms and facilities	Physical security for offices, rooms and facilities shall be	Applicable
A.7.4	Physical security monitoring	Premises shall be continuously monitored for	Applicable
A.7.5	Protecting against physical and environmental threats	Protection against physical and environmental threats,	Applicable
A.7.6	Working in secure areas	Security measures for working in secure areas shall be	Applicable
A.7.7	Clear desk and clear screen	Clear desk rules for papers and removable storage	Applicable
A.7.8	Equipment siting and protection	Equipment shall be sited securely and protected.	Applicable
A.7.9	Security of assets off-premises	Off-site assets shall be protected.	Applicable
A.7.10	Storage media	Storage media shall be managed through their life cycle	Not Applicable
A.7.11	Supporting utilities	Information processing facilities shall be protected from	Applicable
A.7.12	Cabling security	Cables carrying power, data or supporting information	Applicable
A.7.13	Equipment maintenance	Equipment shall be maintained correctly to ensure	Applicable
A.7.14	Secure disposal or re-use of equipment	Items of equipment containing storage media shall be	Applicable
A.8	**Tecnical Controls**		
A.8.1	User endpoint devices	Information stored on, processed by or accessible via	Applicable
A.8.2	Privileged access rights	The allocation and use of privileged access rights shall	Applicable
A.8.3	Information access restriction	Access to information and other associated assets shall	Applicable
A.8.4	Access to source code	Read and write access to source code, development	Applicable
A.8.5	Secure authentication	Secure authentication technologies and procedures	Applicable
A.8.6	Capacity management	The use of resources shall be monitored and adjusted	Applicable
A.8.7	Protection against malware	Protection against malware shall be implemented and	Applicable
A.8.8	Management of technical vulnerabilities	Information about technical vulnerabilities of information	Applicable
A.8.9	Configuration management	Configurations, including security configurations, of	Applicable
A.8.10	Information deletion	Information stored in information systems, devices or in	Applicable
A.8.11	Data masking	Data masking shall be used in accordance with the	Applicable
A.8.12	Data leakage prevention	Data leakage prevention measures shall be applied to	Applicable
A.8.13	Information backup	Backup copies of information, software and systems	Applicable
A.8.14	Redundancy of information processing facilities	Information processing facilities shall be implemented	Applicable
A.8.15	Logging	Logs that record activities, exceptions, faults and other	Applicable
A.8.16	Monitoring activities	Networks, systems and applications shall be monitored	Applicable
A.8.17	Clock synchronization	The clocks of information processing systems used by	Applicable
A.8.18	Use of privileged utility programs	The use of utility programs that can be capable of	Applicable
A.8.19	Installation of software on operational systems	Procedures and measures shall be implemented to	Applicable
A.8.20	Network Security	Networks and network devices shall be secured,	Applicable
A.8.21	Security of network services	Security mechanisms, service levels and service	Applicable
A.8.22	Segregation of networks	Groups of information services, users and information	Applicable
A.8.23	Web filtering	Access to external websites shall be managed to	Applicable
A.8.24	Use of cryptography	Rules for the effective use of cryptography, including	Applicable
A.8.25	Secure development lifecycle	Rules for the secure development of software and	Applicable
A.8.26	Application security requirements	Information security requirements shall be identified,	Applicable
A.8.27	Secure system architecture and engineering principles	Principles for engineering secure systems shall be	Applicable
A.8.28	Secure coding	Secure coding principles shall be applied to software	Applicable
A.8.29	Security testing in development and acceptance	Security testing processes shall be defined and	Applicable
A.8.30	Outsourced development	The organization shall direct, monitor and review the	Applicable
A.8.31	Separation of development test and production	Development, testing and production environments shall	Applicable
A.8.32	Change management	Changes to information processing facilities and	Applicable
A.8.33	Test information	Test information shall be appropriately selected,	Applicable
A.8.34	Protection of information systems during audit testing	Audit tests and other assurance activities involving	Applicable