Statement of Applicability

version: 1.1

ISO/IEC 27001:2022 Annex A	Control	Control description	Applicable Yes/No	Reason for exclusion
5 Organization controls	5.1	Policies for information security	Yes	
	5.2	Information security roles and responsibilities	Yes	
	5.3	Segregation of duties	Yes	
	5.4	Management responsibilities	Yes	
	5.5	Contact with authorities	Yes	
	5.6	Contact with special interest groups	Yes	
	5.7	Threat intelligence	Yes	
	5.8	Information security in project management	Yes	
	5.9	Inventory of information and other associated assets	Yes	
	5.10	Acceptable use of information and other associated assets	Yes	
	5.11	Return of assets	Yes	
	5.12	Classification of information	Yes	
	5.13	Labelling of information	Yes	
	5.14	Information transfer	Yes	
	5.15	Access control	Yes	
	5.16	Identity management	Yes	
	5.17	Authentication information	Yes	
	5.18	Access rights	Yes	
	5.19	Information security in supplier relationships	Yes	
	5.20	Addressing information security within supplier agreements	Yes	
	5.21	Managing information security in the information and communication technology (ICT) supply chain	Yes	
	5.22	Monitoring, review and change management of supplier services	Yes	
	5.23	Information security for use of cloud services	Yes	
	5.24	Information security incident management planning and preparation	Yes	
	5.25	Assessment and decision on information security events	Yes	
	5.26	Response to information security incidents	Yes	
	5.27	Learning from information security incidents	Yes	
	5.28	Collection of evidence	Yes	
	5.29	Information security during disruption	Yes	
	5.30	ICT readiness for business continuity	Yes	
	5.31	Legal, statutory, regulatory and contractual requirements	Yes	
	5.32	Intellectual property rights	Yes	

	5.33	Protection of records	Yes	
	5.34	Privacy and protection of personal identifiable information (PII)	Yes	
	5.35	Independent review of information security	Yes	
	5.36	Compliance with policies, rules and standards for information security	Yes	
	5.37	Documented operating procedures	Yes	
6 People controls	6.1	Screening	Yes	
	6.2	Terms and conditions of employment	Yes	
	6.3	Information security awareness, education and training	Yes	
	6.4	Disciplinary process	Yes	
	6.5	Responsibilities after termination or change of employment	Yes	
	6.6	Confidentiality or non-disclosure agreements	Yes	
	6.7	Remote working	Yes	
	6.8	Information security event reporting	Yes	
7 Physical controls	7.1	Physical security perimeters	Yes	
	7.2	Physical entry	Yes	
	7.3	Securing offices, rooms and facilities	Yes	
	7.4	Physical security monitoring	Yes	
	7.5	Protecting against physical and environmental threats	Yes	
	7.6	Working in secure areas	Yes	
	7.7	Clear desk and clear screen	Yes	
	7.8	Equipment siting and protection	Yes	
	7.9	Security of assets off-premises	Yes	
	7.10	Storage media	Yes	
	7.11	Supporting utilities	Yes	
	7.12	Cabling security	Yes	
	7.13	Equipment maintenance	Yes	
	7.14	Secure disposal or re-use of equipment	Yes	
8 Technological controls	8.1	User end point devices	Yes	
	8.2	Privileged access rights	Yes	
	8.3	Information access restriction	Yes	
	8.4	Access to source code	Yes	
	8.5	Secure authentication	Yes	
	8.6	Capacity management	Yes	
	8.7	Protection against malware	Yes	
	8.8	Management of technical vulnerabilities	Yes	

	8.9	Configuration management	Yes	
	8.10	Information deletion	Yes	
	8.11	Data masking	Yes	
	8.12	Data leakage prevention	Yes	
	8.13	Information backup	Yes	
	8.14	Redundancy of information processing facilities	Yes	
	8.15	Logging	Yes	
	8.16	Monitoring activities	Yes	
	8.17	Clock synchronization	Yes	
	8.18	Use of privileged utility programs	Yes	
	8.19	Installation of software on operational systems	Yes	
	8.20	Networks security	Yes	
	8.21	Security of network services	Yes	
	8.22	Segregation of networks	Yes	
	8.23	Web filtering	Yes	
	8.24	Use of cryptography	Yes	
	8.25	Secure development life cycle	Yes	
	8.26	Application security requirements	Yes	
	8.27	Secure system architecture and engineering principles	Yes	
	8.28	Secure coding	Yes	
	8.29	Security testing in development and acceptance	Yes	
	8.30	Outsourced development	No	No outsourced development
	8.31	Separation of development, test and production environments	Yes	
	8.32	Change management	Yes	
	8.33	Test information	Yes	
	8.34	Protection of information systems during audit testing	Yes	