Statement of Applicability and status of information security controls

Section	Information security control	Included	Implemented	Justification for inclusion or exclusion
A5	Organizational controls			
A.5.1	Policies for information security	✓	✓	Business requirement derived from risk assessment Adopted best practice
A.5.2	Information security roles and responsibilities	✓	✓	Business requirement derived from risk assessment
A.5.3	Segregation of duties	✓	✓	Business requirement derived from risk assessment
A.5.4	Management responsibilities	✓	✓	Adopted best practice
A.5.5	Contact with authorities	✓	✓	Adopted best practice
A.5.6	Contact with special interest groups	✓	✓	Adopted best practice
A.5.7	Threat intelligence	✓	✓	Business requirement derived from risk assessment Adopted best practice
A.5.8	Information security in projectmanagement	✓	✓	Adopted best practice
A.5.9	Inventory of information and other associated assets	✓	✓	Business requirement derived from risk assessment
A.5.10	Acceptable use of information and other associated assets	✓	✓	Adopted best practice
A.5.11	Return of assets	✓	✓	Business requirement derived from risk assessment
A.5.12	Classification of information	✓	✓	Business requirement derived from risk assessment Adopted best practice

A.5.13	Labelling of information	✓	✓	Adopted best practice
A.5.14	Information transfer	✓	✓	Business requirement derived from risk assessment
A.5.15	Access control	✓	✓	Business requirement derived from risk assessment
A.5.16	Identity management	✓	✓	Business requirement derived from risk assessment
A.5.17	Authentication information	✓	✓	Adopted best practice
A.5.18	Access rights	✓	✓	Adopted best practice
A.5.19	Information security in supplier relationships	✓	✓	Business requirement derived from risk assessment
A.5.20	Addressing information security within supplier agreements	✓	✓	Business requirement derived from risk assessment
A.5.21	Managing information security in the information and communication technology (ICT) supply-chain	✓	✓	Business requirement derived from risk assessment
A.5.22	Monitoring, review and change management of supplier services	✓	✓	Business requirement derived from risk assessment
A.5.23	Information security for use of cloud services	✓	✓	Adopted best practice
A.5.24	Information security incident management planning and preparation	✓	✓	Business requirement derived from risk assessment
A.5.25	Assessment and decision on information security events	✓	✓	Adopted best practice
A.5.26	Response to information security incidents	✓	✓	Adopted best practice
A.5.27	Learning from information security incidents	✓	✓	Adopted best practice
A.5.28	Collection of evidence	✓	✓	Adopted best practice

A.5.29	Information security during disruption	✓	✓	Adopted best practice
A.5.30	ICT readiness for business continuity	✓	✓	Adopted best practice
A.5.31	Legal, statutory, regulatory and contractual requirements	✓	✓	Legal requirement
A.5.32	Intellectual property rights	✓	✓	Legal requirement
A.5.33	Protection of records	✓	✓	Legal requirement
A.5.34	Privacy and protection of personal identifiable information (PII)	✓	✓	Legal requirement
A.5.35	Independent review of information security	✓	✓	Adopted best practice
A.5.36	Compliance with policies, rules and standards for information security	✓	✓	Legal requirement
A.5.37	Documented operating procedures	✓	✓	Adopted best practice
A6	People controls			
A.6.1	Screening	✓	✓	Legal requirement
A.6.2	Terms and conditions of employment	✓	✓	Legal requirement
A.6.3	Information security awareness, education and training	✓	✓	Adopted best practice
A.6.4	Disciplinary process	✓	✓	Adopted best practice
A.6.5	Responsibilities after termination or change of employment	✓	✓	Legal requirement
A.6.6	Confidentiality or non-disclosure agreements	✓	✓	Legal requirement
A.6.7	Remote working	✓	✓	Adopted best practice
A.6.8	Information security event reporting	✓	✓	Adopted best practice
A7	Physical controls			
A.7.1	Physical security perimeters	✓	✓	Business requirement derived from risk assessment Adopted best practice

A.7.2	Physical entry	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.7.3	Securing offices, rooms and facilities	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.7.4	Physical security monitoring	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.7.5	Protecting against physical and environmental threats	✓	✓	Adopted best practice
A.7.6	Working in secure areas	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.7.7	Clear desk and clear screen	✓	✓	Adopted best practice
A.7.8	Equipment siting and protection	✓	✓	Adopted best practice
A.7.9	Security of assets off-premises	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.7.10	Storage media	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.7.11	Supporting utilities	✗	✗	Control not applicable to ISMS scope
A.7.12	Cabling security	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.7.13	Equipment maintenance	✓	✓	Adopted best practice
A.7.14	Secure disposal or re-use of equipment	✓	✓	Adopted best practice

A8	Technological controls			
A.8.1	User end point devices	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.8.2	Privileged access rights	✓	✓	Adopted best practice Business requirement derived from risk assessment
A.8.3	Information access restriction	✓	✓	Contractual obligation Legal requirement
A.8.4	Access to source code	✓	✓	Legal requirement Business requirement derived from risk assessment
A.8.5	Secure authentication	✓	✓	Adopted best practice
A.8.6	Capacity management	✓	✓	Business requirement derived from risk assessment
A.8.7	Protection against malware	✓	✓	Business requirement derived from risk assessment
A.8.8	Management of technical vulnerabilities	✓	✓	Adopted best practice
A.8.9	Configuration management	✓	✓	Adopted best practice
A.8.10	Information deletion	✓	✓	Legal requirement
A.8.11	Data masking	✓	✓	Adopted best practice
A.8.12	Data leakage prevention	✓	✓	Business requirement derived from risk assessment
A.8.13	Information backup	✓	✓	Adopted best practice
A.8.14	Redundancy of information processing facilities	✓	✓	Adopted best practice
A.8.15	Logging	✓	✓	Adopted best practice
A.8.16	Monitoring activities	✓	✓	Adopted best practice
A.8.17	Clock synchronization	✓	✓	Adopted best practice

A.8.18	Use of privileged utility programs	✓	✓	Adopted best practice
A.8.19	Installation of software on operational systems	✓	✓	Adopted best practice
A.8.20	Networks security	✓	✓	Adopted best practice
A.8.21	Security of network services	✓	✓	Adopted best practice
A.8.22	Segregation of networks	✓	✓	Adopted best practice
A.8.23	Web filtering	✓	✓	Adopted best practice
A.8.24	Use of cryptography	✓	✓	Adopted best practice
A.8.25	Secure development life cycle	✓	✓	Adopted best practice
A.8.26	Application security requirements	✓	✓	Adopted best practice
A.8.27	Secure system architecture and engineering principles	✓	✓	Adopted best practice
A.8.28	Secure coding	✓	✓	Adopted best practice
A.8.29	Security testing in development and acceptance	✓	✓	Adopted best practice
A.8.30	Outsourced development	✗	✗	Control not applicable to ISMS scope
A.8.31	Separation of development, test and production environments	✓	✓	Adopted best practice
A.8.32	Change management	✓	✓	Adopted best practice
A.8.33	Test information	✓	✓	Business requirement derived from risk assessment Adopted best practice
A.8.34	Protection of information systems during audit testing	✓	✓	Adopted best practice