Quantios

Statement of Applicability

ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
Sec	Name	Yes /No	Yes/No		LR	CO	BR / BP	RRA
A.5	**Organisational Controls**							
5.1	Policies for information security	Yes	Yes	N/A		Yes	Yes	Yes
5.2	Information security roles and responsibilities	Yes	Yes	N/A			Yes	Yes
5.3	Segregation of duties	Yes	Yes	N/A				Yes
5.4	Management responsibilities	Yes	Yes	N/A			Yes	Yes
5.5	Contact with authorities	Yes	Yes	N/A	Yes			Yes
5.6	Contact with special interest groups	Yes	Yes	N/A			Yes	Yes
5.7	Threat Intelligence	Yes	Yes	N/A			Yes	Yes
5.8	Information security in project management	Yes	Yes	N/A			Yes	Yes
5.9	Inventory of information and other associated assets	Yes	Yes	N/A			Yes	Yes

Statement of Applicability

ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
Sec	Name	Yes /No	Yes/No		LR	CO	BR / BP	RRA
5.10	Acceptable use of information and other associated assets	Yes	Yes	N/A			Yes	Yes
5.11	Return of assets	Yes	Yes	N/A				Yes
5.12	Classification of information	Yes	Yes	N/A			Yes	Yes
5.13	Labelling of information	Yes	Yes	N/A			Yes	Yes
5.14	Information transfer	Yes	Yes	N/A				Yes
5.15	Access control	Yes	Yes	N/A			Yes	Yes
5.16	Identity management	Yes	Yes	N/A				Yes
5.17	Authentication information	Yes	Yes	N/A				Yes
5.18	Access rights	Yes	Yes	N/A			Yes	Yes

Statement of Applicability								

ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
Sec	Name	Yes /No	Yes/No		LR	CO	BR / BP	RRA
5.19	Information security in supplier relationships	Yes	Yes	N/A			Yes	Yes
5.20	Addressing information security within supplier agreements	Yes	Yes	N/A				Yes
5.21	Managing information security in the ICT supply chain	Yes	Yes	N/A				Yes
5.22	Monitoring, review and change management of supplier services	Yes	Yes	N/A				Yes
5.23	Information security for use of cloud services	Yes	Yes	N/A			Yes	
5.24	Information security incident management planning and preparation	Yes	Yes	N/A			Yes	Yes
5.25	Assessment and decision on information security events	Yes	Yes	N/A				Yes
5.26	Response to information security incidents	Yes	Yes	N/A				Yes
5.27	Learning from information security incidents	Yes	Yes	N/A			Yes	Yes

	Statement of Applicability							
Legend LR: Legal Requirements, CO: Contractual Obligations, BR / BP: Business Requirement / Adopted Best Practice, RRA: Results of Risk Assessment								
ISO 27001:2022 Controls		**Controls Required**	**Control Implemented**	**Justification for Full Exclusion (If Applicable)**	**Justification for Selection of Controls (Yes / No)**			
					LR	**CO**	**BR / BP**	**RRA**
Sec	**Name**	**Yes /No**	**Yes/No**					
5.28	Collection of evidence	Yes	Yes	N/A				Yes
5.29	Information security during disruption	Yes	Yes	N/A				Yes
5.30	ICT readiness for business continuity	Yes	Yes	N/A				Yes
5.31	Legal, statutory, regulatory and contractual requirements	Yes	Yes	N/A	Yes			Yes
5.32	Intellectual property rights	Yes	Yes	N/A	Yes			Yes
5.33	Protection of records	Yes	Yes	N/A	Yes			Yes
5.34	Privacy and protection of PII	Yes	Yes	N/A	Yes			Yes
5.35	Independent review of information security	Yes	Yes	N/A			Yes	
5.36	Compliance with policies, rules and standards for information security	Yes	Yes	N/A				Yes

Statement of Applicability								
Legend LR: Legal Requirements, CO: Contractual Obligations, BR / BP: Business Requirement / Adopted Best Practice, RRA: Results of Risk Assessment								
ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
					LR	CO	BR / BP	RRA
Sec	Name	Yes /No	Yes/No					
5.37	Documented operating procedures	Yes	Yes	N/A				Yes
A.6	**People Controls**							
6.1	Screening	Yes	Yes	N/A			Yes	Yes
6.2	Terms and conditions of employment	Yes	Yes	N/A	Yes			Yes
6.3	Information security awareness, education and training	Yes	Yes	N/A				Yes
6.4	Disciplinary process	Yes	Yes	N/A			Yes	
6.5	Responsibilities after termination or change of employment	Yes	Yes	N/A				Yes
6.6	Confidentiality or non–disclosure agreements	Yes	Yes	N/A				Yes

Statement of Applicability								
Legend LR: Legal Requirements, CO: Contractual Obligations, BR / BP: Business Requirement / Adopted Best Practice, RRA: Results of Risk Assessment								
ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
					LR	CO	BR / BP	RRA
Sec	Name	Yes /No	Yes/No					
6.7	Remote Working	Yes	Yes	N/A				Yes
6.8	Information security event reporting	Yes	Yes	N/A				Yes
A.7	**Physical Controls**							
7.1	Physical security perimeters	Yes	Yes	N/A				Yes
7.2	Physical entry	Yes	Yes	N/A				Yes
7.3	Securing offices, rooms and facilities	Yes	Yes	N/A				Yes
7.4	Physical security monitoring	Yes	Yes	N/A				Yes
7.5	Protecting against physical and environmental threats	Yes	Yes	N/A				Yes
7.6	Working in secure areas	Yes	Yes	N/A				Yes
7.7	Clear desk and clear screen	Yes	Yes	N/A			Yes	Yes
7.8	Equipment siting and protection	Yes	Yes	N/A				Yes
7.9	Security of assets off-premises	Yes	Yes	N/A				Yes
7.10	Storage media	Yes	Yes	N/A				Yes
7.11	Supporting utilities	Yes	Yes	N/A				Yes

Statement of Applicability								
Legend LR: Legal Requirements, CO: Contractual Obligations, BR / BP: Business Requirement / Adopted Best Practice, RRA: Results of Risk Assessment								
ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
Sec	Name	Yes /No	Yes/No		LR	CO	BR / BP	RRA
7.12	Cabling security	Yes	Yes	N/A				Yes
7.13	Equipment maintenance	Yes	Yes	N/A				Yes
7.14	Secure disposal or re-use of equipment	Yes	Yes	N/A				Yes
A.8	**Technological controls**							
8.1	User endpoint devices	Yes	Yes	N/A				Yes
8.2	Privileged access rights	Yes	Yes	N/A				Yes
8.3	Information access restriction	Yes	Yes	N/A			Yes	Yes
8.4	Access to source code	Yes	Yes	N/A				Yes
8.5	Secure authentication	Yes	Yes	N/A			Yes	
8.6	Capacity management	Yes	Yes	N/A			Yes	
8.7	Protection against malware	Yes	Yes	N/A				Yes
8.8	Management of technical vulnerabilities	Yes	Yes	N/A				Yes
8.9	Configuration management	Yes	Yes	N/A				Yes
8.10	Information deletion	Yes	Yes	N/A	Yes		Yes	

Statement of Applicability							
Legend LR: Legal Requirements, CO: Contractual Obligations, BR / BP: Business Requirement / Adopted Best Practice, RRA: Results of Risk Assessment							
ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
Sec	Name	Yes /No	Yes/No		LR	CO	BR / BP	RRA
8.11	Data masking	Yes	Yes	N/A	Yes			Yes
8.12	Data leakage prevention	Yes	Yes	N/A				Yes
8.13	Information backup	Yes	Yes	N/A				Yes
8.14	Redundancy of information processing facilities	Yes	Yes	N/A			Yes	
8.15	Logging	Yes	Yes	N/A				Yes
8.16	Monitoring activities	Yes	Yes	N/A				Yes
8.17	Clock synchronization	Yes	Yes	N/A				Yes
8.18	Use of privileged utility programs	Yes	Yes	N/A				Yes
8.19	Installation of software on operational systems	Yes	Yes	N/A				Yes
8.20	Networks security	Yes	Yes	N/A				Yes
8.21	Security of network services	Yes	Yes	N/A				Yes
8.22	Segregation of networks	Yes	Yes	N/A				Yes

Statement of Applicability

Legend
LR: Legal Requirements, CO: Contractual Obligations, BR / BP: Business Requirement / Adopted Best Practice, RRA: Results of Risk Assessment

ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
Sec	Name	Yes /No	Yes/No		LR	CO	BR / BP	RRA
8.23	Web filtering	Yes	Yes	N/A			Yes	
8.24	Use of cryptography	Yes	Yes	N/A				Yes
8.25	Secure development life cycle	Yes	Yes	N/A				Yes
8.26	Application security requirements	Yes	Yes	N/A				Yes
8.27	Secure system architecture and engineering principles	Yes	Yes	N/A				Yes
8.28	Secure coding	Yes	Yes	N/A				Yes
8.29	Security testing in development and acceptance	Yes	Yes	N/A				Yes

Statement of Applicability

ISO 27001:2022 Controls		Controls Required	Control Implemented	Justification for Full Exclusion (If Applicable)	Justification for Selection of Controls (Yes / No)			
Sec	Name	Yes /No	Yes/No		LR	CO	BR / BP	RRA
8.30	Outsourced development	Yes	Yes	This control applies only in scenarios where there is a urgent request or need to engage with an outsourced developer. However, this control is currently not applicable as Quantios does not outsource any software development activities. All software development processes are carried out internally, with no involvement of third-party providers.				Yes
8.31	Separation of development, test and production environments	Yes	Yes	N/A				Yes
8.32	Change management	Yes	Yes	N/A				Yes
8.33	Test information	Yes	Yes	N/A	Yes		Yes	Yes
8.34	Protection of information systems during audit testing	Yes	Yes	N/A				Yes