MaraSoft

Statement of Applicability

ISO/IEC 27001:2022 | MaraSoft B.V.

Statement of Applicability ISO 27001:2022 (MaraSoft B.V.)

Version: 1.1 (24/06/2024)

Author: Johannes van Urk

Control	Control description	Applicable	Justification / exclusion reason	Control status
5. Organizational controls				
5.1	Policies for information security	Yes	Reducing information security risks	Control implemented
5.2	Information security roles and responsibilities	Yes	Reducing information security risks	Control implemented
5.3	Segregation of duties	Yes	Reducing information security risks	Control implemented
5.4	Management responsibilities	Yes	Reducing information security risks	Control implemented
5.5	Contact with authorities	Yes	Reducing information security risks	Control implemented
5.6	Contact with special interest groups	Yes	Reducing information security risks	Control implemented
5.7	Threat intelligence	Yes	Reducing information security risks	Control implemented
5.8	Information security in project management	Yes	Reducing information security risks	Control implemented
5.9	Inventory of information and other associated assets	Yes	Reducing information security risks	Control implemented
5.10	Acceptable use of information and other associated assets	Yes	Reducing information security risks	Control implemented
5.11	Return of assets	Yes	Reducing information security risks	Control implemented
5.12	Classification of information	Yes	Reducing information security risks	Control implemented
5.13	Labelling of information	Yes	Reducing information security risks	Control implemented
5.14	Information transfer	Yes	Reducing information security risks	Control implemented
5.15	Access control	Yes	Reducing information security risks	Control implemented

5.16	Identity management	Yes	Reducing information security risks	Control implemented
5.17	Authentication information	Yes	Reducing information security risks	Control implemented
5.18	Access rights	Yes	Reducing information security risks	Control implemented
5.19	Information security in supplier relationships	Yes	Reducing information security risks	Control implemented
5.20	Addressing information security within supplier agreements	Yes	Reducing information security risks	Control implemented
5.21	Managing information security in the information and communication technology (ICT) supply chain	Yes	Reducing information security risks	Control implemented
5.22	Monitoring, review and change management of supplier services	Yes	Reducing information security risks	Control implemented
5.23	Information security for use of cloud services	Yes	Reducing information security risks	Control implemented
5.24	Information security incident management planning and preparation	Yes	Reducing information security risks	Control implemented
5.25	Assessment and decision on information security events	Yes	Reducing information security risks	Control implemented
5.26	Response to information security incidents	Yes	Reducing information security risks	Control implemented
5.27	Learning from information security incidents	Yes	Reducing information security risks	Control implemented
5.28	Collection of evidence	Yes	Reducing information security risks	Control implemented
5.29	Information security during disruption	Yes	Reducing information security risks	Control implemented
5.30	ICT readiness for business continuity	Yes	Reducing information security risks	Control implemented
5.31	Legal, statutory, regulatory and contractual agreements	Yes	Reducing information security risks	Control implemented
5.32	Intellectual property rights	Yes	Reducing information security risks	Control implemented
5.33	Protection of records	Yes	Reducing information security risks	Control implemented
5.34	Privacy and protection of personal identifiable information (PII)	Yes	Reducing information security risks	Control implemented

5.35	Independent review of information security	Yes	Reducing information security risks	Control implemented
5.36	Compliance with policies, rules and standards for information security	Yes	Reducing information security risks	Control implemented
5.37	Documented operating procedures	Yes	Reducing information security risks	Control implemented
6. People controls				
6.1	Screening	Yes	Reducing information security risks	Control implemented
6.2	Terms and conditions of employment	Yes	Reducing information security risks	Control implemented
6.3	Information security awareness, education and training	Yes	Reducing information security risks	Control implemented
6.4	Disciplinary process	Yes	Reducing information security risks	Control implemented
6.5	Responsibilities after termination of change of employment	Yes	Reducing information security risks	Control implemented
6.6	Confidentiality or non-disclosure agreements	Yes	Reducing information security risks	Control implemented
6.7	Remote working	Yes	Reducing information security risks	Control implemented
6.8	Information security event reporting	Yes	Reducing information security risks	Control implemented
7. Physical controls				
7.1	Physical security perimeters	Yes	Reducing information security risks	Control implemented
7.2	Physical entry	Yes	Reducing information security risks	Control implemented
7.3	Securing offices, rooms and facilities	Yes	Reducing information security risks	Control implemented
7.4	Physical security monitoring	Yes	Reducing information security risks	Control implemented
7.5	Protecting against physical and environmental threats	Yes	Reducing information security risks	Control implemented
7.6	Working in secure areas	Yes	Reducing information security risks	Control implemented
7.7	Clear desk and clear screen	Yes	Reducing information security risks	Control implemented
7.8	Equipment siting and protection	Yes	Reducing information security risks	Control implemented

7.9	Security of assets off-premises	Yes	Reducing information security risks	Control implemented
7.10	Storage media	Yes	Reducing information security risks	Control implemented
7.11	Supporting utilities	Yes	Reducing information security risks	Control implemented
7.12	Cabling security	Yes	Reducing information security risks	Control implemented
7.13	Equipment maintenance	Yes	Reducing information security risks	Control implemented
7.14	Secure disposal or re-use of equipment	Yes	Reducing information security risks	Control implemented
8. Technological controls				
8.1	User end point devices	Yes	Reducing information security risks	Control implemented
8.2	Privileged access rights	Yes	Reducing information security risks	Control implemented
8.3	Information access restriction	Yes	Reducing information security risks	Control implemented
8.4	Access to source code	Yes	Reducing information security risks	Control implemented
8.5	Secure authentication	Yes	Reducing information security risks	Control implemented
8.6	Capacity management	Yes	Reducing information security risks	Control implemented
8.7	Protection against malware	Yes	Reducing information security risks	Control implemented
8.8	Management of technical vulnerabilities	Yes	Reducing information security risks	Control implemented
8.9	Configuration management	Yes	Reducing information security risks	Control implemented
8.10	Information deletion	Yes	Reducing information security risks	Control implemented
8.11	Data masking	Yes	Reducing information security risks	Control implemented
8.12	Data leakage prevention	Yes	Reducing information security risks	Control implemented
8.13	Information backup	Yes	Reducing information security risks	Control implemented
8.14	Redundancy of information processing facilities	Yes	Reducing information security risks	Control implemented
8.15	Logging	Yes	Reducing information security risks	Control implemented
8.16	Monitoring activities	Yes	Reducing information security risks	Control implemented

8.17	Clock synchronization	Yes	Reducing information security risks	Control implemented
8.18	Use of privileged utility programs	Yes	Reducing information security risks	Control implemented
8.19	Installation of software on operational systems	Yes	Reducing information security risks	Control implemented
8.20	Networks security	Yes	Reducing information security risks	Control implemented
8.21	Security of network services	Yes	Reducing information security risks	Control implemented
8.22	Segregation of networks	Yes	Reducing information security risks	Control implemented
8.23	Web filtering	Yes	Reducing information security risks	Control implemented
8.24	Use of cryptography	Yes	Reducing information security risks	Control implemented
8.25	Secure development life cycle	Yes	Reducing information security risks	Control implemented
8.26	Application security requirements	Yes	Reducing information security risks	Control implemented
8.27	Secure system architecture and engineering principles	Yes	Reducing information security risks	Control implemented
8.28	Secure coding	Yes	Reducing information security risks	Control implemented
8.29	Security testing in development and acceptance	Yes	Reducing information security risks	Control implemented
8.30	Outsourced development	Yes	Reducing information security risks	Control implemented
8.31	Separation of development, test and production environments	Yes	Reducing information security risks	Control implemented
8.32	Change management	Yes	Reducing information security risks	Control implemented
8.33	Test information	Yes	Reducing information security risks	Control implemented
8.34	Protection of information systems during audit testing	Yes	Reducing information security risks	Control implemented