Statement of Applicability

ISO/IEC 27001:2013 | MaraSoft B.V.

Statement of Applicability (MaraSoft B.V.)

Version: 1.0 (17/08/2022)

Author: Johannes van Urk

ISO/IEC 27001:2013 Annex A controls			Control applicable	Justification	Control status
Clause	Section	Control			
A.5 Information security policies	**5.1**	**Management direction for information security**			
	5.1.1	Policies for information security	Yes	Reducing information security risks	Control implemented
	5.1.2	Review of the policies for information security	Yes	Reducing information security risks	Control implemented
A.6 Organization of information security	**6.1**	**Internal organization**			
	6.1.1	Information security roles and responsibilities	Yes	Reducing information security risks	Control implemented
	6.1.2	Segregation of duties	Yes	Reducing information security risks	Control implemented
	6.1.3	Contact with authorities	Yes	Reducing information security risks	Control implemented
	6.1.4	Contact with special interest groups	Yes	Reducing information security risks	Control implemented
	6.1.5	Information security in project management	Yes	Reducing information security risks	Control implemented
	6.2	**Mobile devices and teleworking**			

	6.2.1	Mobile device policy	Yes	Reducing information security risks	Control implemented
	6.2.2	Teleworking	Yes	Reducing information security risks	Control implemented
A.7 Human resource security	**7.1**	**Prior to employment**			
	7.1.1	Screening	Yes	Reducing information security risks	Control implemented
	7.1.2	Terms and conditions of employment	Yes	Reducing information security risks	Control implemented
	7.2	**During employment**			
	7.2.1	Management responsibilities	Yes	Reducing information security risks	Control implemented
	7.2.2	Information security awareness, education and training	Yes	Reducing information security risks	Control implemented
	7.2.3	Disciplinary process	Yes	Reducing information security risks	Control implemented
	7.3	**Termination and change of employment**			
	7.3.1	Termination or change of employment responsibilities	Yes	Reducing information security risks	Control implemented
A.8 Asset management	**8.1**	**Responsibility for assets**			
	8.1.1	Inventory of assets	Yes	Reducing information security risks	Control implemented
	8.1.2	Ownership of assets	Yes	Reducing information security risks	Control implemented
	8.1.3	Acceptable use of assets	Yes	Reducing information security risks	Control implemented
	8.1.4	Return of assets	Yes	Reducing information security risks	Control implemented
	8.2	**Information classification**			
	8.2.1	Classification of information	Yes	Reducing information security risks	Control implemented
	8.2.2	Labeling of information	Yes	Reducing information security risks	Control implemented
	8.2.3	Handling of assets	Yes	Reducing information security risks	Control implemented

	8.3	**Media handling**			
	8.3.1	Management of removable media	Yes	Reducing information security risks	Control implemented
	8.3.2	Disposal of media	Yes	Reducing information security risks	Control implemented
	8.3.3	Physical media transfer	Yes	Reducing information security risks	Control implemented
A.9 Access control	**9.1**	**Business requirements of access control**			
	9.1.1	Access control policy	Yes	Reducing information security risks	Control implemented
	9.1.2	Access to networks and network services	Yes	Reducing information security risks	Control implemented
	9.2	**User access management**			
	9.2.1	User registration and de-registration	Yes	Reducing information security risks	Control implemented
	9.2.2	User access provisioning	Yes	Reducing information security risks	Control implemented
	9.2.3	Management of privileged access rights	Yes	Reducing information security risks	Control implemented
	9.2.4	Management of secret authentication information of users	Yes	Reducing information security risks	Control implemented
	9.2.5	Review of user access rights	Yes	Reducing information security risks	Control implemented
	9.2.6	Removal or adjustment of access rights	Yes	Reducing information security risks	Control implemented
	9.3	**User responsibilities**			
	9.3.1	Use of secret authentication information	Yes	Reducing information security risks	Control implemented
	9.4	System and application access control			

	9.4.1	Information access restriction	Yes	Reducing information security risks	Control implemented
	9.4.2	Secure log-on procedures	Yes	Reducing information security risks	Control implemented
	9.4.3	Password management system	Yes	Reducing information security risks	Control implemented
	9.4.4	Use of privileged utility programs	Yes	Reducing information security risks	Control implemented
	9.4.5	Access control to program source code	Yes	Reducing information security risks	Control implemented
A.10 Cryptography	**10.1**	**Cryptographic controls**			
	10.1.1	Policy on the use of cryptographic controls	Yes	Reducing information security risks	Control implemented
	10.1.2	Key management	Yes	Reducing information security risks	Control implemented
A.11 Physical and environmental security	**11.1**	**Secure areas**			
	11.1.1	Physical security perimeter	Yes	Reducing information security risks	Control implemented
	11.1.2	Physical entry controls	Yes	Reducing information security risks	Control implemented
	11.1.3	Securing office, room and facilities	Yes	Reducing information security risks	Control implemented
	11.1.4	Protecting against external end environmental threats	Yes	Reducing information security risks	Control implemented
	11.1.5	Working in secure areas	No	MaraSoft does not have secure areas	Not applicable
	11.1.6	Delivery and loading areas	No	MaraSoft does not have delivery and loading areas	Not applicable
	11.2	**Equipment**			
	11.2.1	Equipment siting and protection	Yes	Reducing information security risks	Control implemented
	11.2.2	Supporting utilities	Yes	Reducing information security risks	Control implemented

	11.2.3	Cabling security	Yes	Reducing information security risks	Control implemented
	11.2.4	Equipment maintenance	Yes	Reducing information security risks	Control implemented
	11.2.5	Removal of assets	Yes	Reducing information security risks	Control implemented
	11.2.6	Security of equipment and assets off-premises	Yes	Reducing information security risks	Control implemented
	11.2.7	Secure disposal or re-use of equipment	Yes	Reducing information security risks	Control implemented
	11.2.8	Unattended user equipment	Yes	Reducing information security risks	Control implemented
	11.2.9	Clear desk and clear screen policy	Yes	Reducing information security risks	Control implemented
A.12 Operations security	**12.1**	**Operational procedures and responsibilities**			
	12.1.1	Documented operating procedures	Yes	Reducing information security risks	Control implemented
	12.1.2	Change management	Yes	Reducing information security risks	Control implemented
	12.1.3	Capacity management	Yes	Reducing information security risks	Control implemented
	12.1.4	Separation of development, testing and operational environments	Yes	Reducing information security risks	Control implemented
	12.2	**Protection from malware**			
	12.2.1	Controls against malware	Yes	Reducing information security risks	Control implemented
	12.3	**Backup**			
	12.3.1	Information backup	Yes	Reducing information security risks	Control implemented
	12.4	**Logging and monitoring**			
	12.4.1	Event logging	Yes	Reducing information security risks	Control implemented
	12.4.2	Protection of log information	Yes	Reducing information security risks	Control implemented

	12.4.3	Administrator and operator logs	Yes	Reducing information security risks	Control implemented
	12.4.4	Clock synchronization	Yes	Reducing information security risks	Control implemented
	12.5	**Control of operational software**			
	12.5.1	Installation of software on operational systems	Yes	Reducing information security risks	Control implemented
	12.6	**Technical vulnerability management**			
	12.6.1	Management of technical vulnerabilities	Yes	Reducing information security risks	Control implemented
	12.6.2	Restrictions on software installation	Yes	Reducing information security risks	Control implemented
	12.7	**Information systems audit considerations**			
	12.7.1	Information systems audit controls	Yes	Reducing information security risks	Control implemented
A.13 Communications security	**13.1**	**Network security management**			
	13.1.1	Network controls	Yes	Reducing information security risks	Control implemented
	13.1.2	Security of network services	Yes	Reducing information security risks	Control implemented
	13.1.3	Segregation in networks	Yes	Reducing information security risks	Control implemented
	13.2	**Information transfer**			
	13.2.1	Information transfer policies and procedures	Yes	Reducing information security risks	Control implemented
	13.2.2	Agreements on information transfer	Yes	Reducing information security risks	Control implemented

	13.2.3	Electronic messaging	Yes	Reducing information security risks	Control implemented
	13.2.4	Confidentiality or non-disclosure agreements	Yes	Reducing information security risks	Control implemented
A.14 System acquisition, development and maintenance	**14.1**	**Security requirements of information systems**			
	14.1.1	Information security requirements analysis and specification	Yes	Reducing information security risks	Control implemented
	14.1.2	Securing applications services on public networks	Yes	Reducing information security risks	Control implemented
	14.1.3	Protecting application services transactions	Yes	Reducing information security risks	Control implemented
	14.2	**Security in development and support processes**			
	14.2.1	Secure development policy	Yes	Reducing information security risks	Control implemented
	14.2.2	System change control procedures	Yes	Reducing information security risks	Control implemented
	14.2.3	Technical review of applications after operating platform changes	Yes	Reducing information security risks	Control implemented
	14.2.4	Restrictions on changes to software packages	Yes	Reducing information security risks	Control implemented
	14.2.5	Secure system engineering principles	Yes	Reducing information security risks	Control implemented
	14.2.6	Secure development environment	Yes	Reducing information security risks	Control implemented
	14.2.7	Outsourced development	Yes	Reducing information security risks	Control implemented
	14.2.8	System security testing	Yes	Reducing information security risks	Control implemented

	14.2.9	System acceptance testing	Yes	Reducing information security risks	Control implemented
	14.3	**Test data**			
	14.3.1	Protection of test data	Yes	Reducing information security risks	Control implemented
A.15 Supplier relationships	**15.1**	**Information security in supplier relationships**			
	15.1.1	Information security policy for supplier relationships	Yes	Reducing information security risks	Control implemented
	15.1.2	Addressing security within supplier agreements	Yes	Reducing information security risks	Control implemented
	15.1.3	Information and communication technology supply chain	Yes	Reducing information security risks	Control implemented
	15.2	**Supplier service delivery management**			
	15.2.1	Monitoring and review of supplier services	Yes	Reducing information security risks	Control implemented
	15.2.2	Managing changes to supplier services	Yes	Reducing information security risks	Control implemented
A.16 Information security incident management	**16.1**	**Management of information security incidents and improvements**			
	16.1.1	Responsibilities and procedures	Yes	Reducing information security risks	Control implemented
	16.1.2	Reporting information security events	Yes	Reducing information security risks	Control implemented
	16.1.3	Reporting information security weaknesses	Yes	Reducing information security risks	Control implemented

	16.1.4	Assessment of and decision on information security events	Yes	Reducing information security risks	Control implemented
	16.1.5	Response to information security incidents	Yes	Reducing information security risks	Control implemented
	16.1.6	Learning from information security incidents	Yes	Reducing information security risks	Control implemented
	16.1.7	Collection of evidence	Yes	Reducing information security risks	Control implemented
A.17 Information security aspects of business continuity management	**17.1**	**Information security continuity**			
	17.1.1	Planning information security continuity	Yes	Reducing information security risks	Control implemented
	17.1.2	Implementing information security continuity	Yes	Reducing information security risks	Control implemented
	17.1.3	Verify, review and evaluate information security continuity	Yes	Reducing information security risks	Control implemented
	17.2	**Redundancies**			
	17.2.1	Availability of information processing facilities	Yes	Reducing information security risks	Control implemented
A.18 Compliance	**18.1**	**Compliance with legal and contractual requirements**			
	18.1.1	Identification of applicable legislation and contractual requirements	Yes	Reducing information security risks	Control implemented
	18.1.2	Intellectual property rights	Yes	Reducing information security risks	Control implemented
	18.1.3	Protection of records	Yes	Reducing information security risks	Control implemented

	18.1.4	Privacy and protection of personally identifiable information	Yes	Reducing information security risks	Control implemented
	18.1.5	Regulation of cryptographic controls	Yes	Reducing information security risks	Control implemented
	18.2	**Information security reviews**			
	18.2.1	Independent review of information security	Yes	Reducing information security risks	Control implemented
	18.2.2	Compliance with security policies and standards	Yes	Reducing information security risks	Control implemented
	18.2.3	Technical compliance review	Yes	Reducing information security risks	Control implemented