Classificatie	Extern - Beperkt
Auteur	Vincent Bougeatre
Laatste review	22 mei 2023
Versie	v1
Eigenaar	ISO

Applicable?	Standard	Control	Implemented?	Justification for applicable or not applicable
	5	Organizational controls		
Yes	5.1	Policies for information security		Compliance, risk mitigation
Yes	5.2	Information security roles and responsibilities		Best practice
Yes	5.2	Segregation of duties		Best practice
Yes	5.4	Management responsibilities		Compliance
Yes	5.5	Contact with authorities		Best practice
Yes	5.6	Contact with special interest groups		Best practice
Yes	5.7	Threat intelligence		Best practice
Yes	5.8	Information security in project management		Best practice
Yes	5.9	Inventory of information and other associated assets		Best practice
Yes	5.10	Acceptable use of information and other associated assets		Best practice
Yes	5.11	Return of assets		Best practice
Yes	5.12	Classification of information		Risk mitigation
Yes	5.13	Labelling of information		Risk mitigation
Yes	5.14	Information transfer		Best practice
Yes	5.15	Access control		Risk mitigation
Yes	5.16	Identity management		Risk mitigation
Yes	5.17	Authentication information		Risk mitigation
Yes	5.18	Access rights		Risk mitigation
Yes	5.19	Information security in supplier relationships		Risk mitigation
Yes	5.20	Addressing information security within supplier agreements		Risk mitigation
Yes	5.21	Managing information security in the ICT supply chain		Best practice
Yes	5.22	Monitoring, review and change management of supplier services		Risk mitigation
Yes	5.23	Information security for use of cloud services		Risk mitigation
Yes	5.24	Information security incident management planning and preparation		Risk mitigation
Yes	5.25	Assessment and decision on information security events		Risk mitigation
Yes	5.26	Response to information security incidents		Risk mitigation
Yes	5.27	Learning from information security incidents		Risk mitigation
Yes	5.28	Collection of evidence		Risk mitigation
Yes	5.29	Information security during disruption		Best practice
Yes	5.30	ICT readiness for business continuity		Risk mitigation
Yes	5.31	Identification of legal, statutory, regulatory and contractual requirements		Best practice
Yes	5.32	Intellectual property rights		Compliance
Yes	5.33	Protection of records		Compliance
Yes	5.34	Privacy and protection of PII		Compliance
Yes	5.35	Independent review of information security		Best practice
Yes	5.36	Compliance with policies and standards of information security		Best practice
Yes	5.37	Documented operating procedures		Best practice
	6	People controls		
Yes	6.1	Screening		Best practice
Yes	6.2	Terms and conditions of employment		Risk mitigation
Yes	6.3	Information security awareness, education and training		Risk mitigation
Yes	6.4	Disciplinary process		Risk mitigation
Yes	6.5	Responsibilities after termination or change of employment		Risk mitigation
Yes	6.6	Confidentiality or non-disclosure agreements		Best practice
Yes	6.7	Remote working		Best practice
Yes	6.8	Information security event reporting		Risk mitigation
	7	Physical controls		
Yes	7.1	Physical security perimeter		Risk mitigation
Yes	7.2	Physical entry controls		Risk mitigation
Yes	7.3	Securing offices, rooms and facilities		Risk mitigation
Yes	7.4	Physical security monitoring		Risk mitigation
Yes	7.5	Protecting against physical and environmental threats		Best practice
Yes	7.6	Working in secure areas		Best practice
Yes	7.7	Clear desk and clear screen		Risk mitigation
Yes	7.8	Equipment siting and protection		Best practice
Yes	7.9	Security of assets off-premises		Best practice
Yes	7.10	Storage media		Best practice
Yes	7.11	Supporting utilities		Best practice
Yes	7.12	Cabling security		Best practice
Yes	7.13	Equipment maintenance		Best practice
Yes	7.14	Secure disposal or re-use of equipment		Best practice
	8	Technological Controls		
Yes	8.1	User endpoint devices		Risk mitigation
Yes	8.2	Privileged access rights		Risk mitigation
Yes	8.3	Information access restriction		Risk mitigation
Yes	8.4	Access to source code		Best practice
Yes	8.5	Secure authentication		Risk mitigation
Yes	8.6	Capacity management		Best practice
Yes	8.7	Protection against malware		Best practice
Yes	8.8	Management of technical vulnerabilities		Best practice
Yes	8.9	Configuration management		Risk mitigation
Yes	8.10	Information deletion		Risk mitigation
Yes	8.11	Data masking		Best practice
Yes	8.12	Data leakage prevention		Best practice
Yes	8.13	Information backup		Risk mitigation
Yes	8.14	Redundancy of information processing facilities		Best practice
Yes	8.15	Logging		Risk mitigation
Yes	8.16	Monitoring activities		Risk mitigation
Yes	8.17	Clock synchronization		Best practice
Yes	8.18	Use of privileged utility programs		Best practice
Yes	8.19	Installation of software on operational systems		Risk mitigation
Yes	8.20	Networks security		Risk mitigation
Yes	8.21	Security of network services		Best practice
Yes	8.22	Segregation in networks		Risk mitigation
Yes	8.23	Web filtering		Best practice
Yes	8.24	Use of cryptography		Best practice
No	8.25	Secure development lifecycle		Out of scope
Yes	8.26	Application security requirements		Best practice
Yes	8.27	Secure system architecture and engineering principles		Best practice
No	8.28	Secure coding		Out of scope
No	8.29	Security testing in development		Out of scope
No	8.30	Outsourced development		Out of scope
No	8.31	Separation of development, test and production environments		Out of scope
Yes	8.32	Change management		Best practice

Yes	8.33	Test information	Best practice
Yes	8.34	Protection of information systems during audit and testing	Best practice