Verklaring van toepasselijkheid

Actueel sinds: 26-08-2024

Legenda (voor Geselecteerde maatregelen en motivatie)
WV: **wettelijke verplichting**,CV: **contractuele verplichting**,RRB: **resultaat van risicobeoordeling**

ISO/IEC 27001:2022 Annex A maatregelen			Huidige maatregelen	Opmerkingen (met verklaring van uitsluiting)	Geselecteerde maatregelen en motivatie		
					WV	CV	RRB
Clausule	**Sec**	**Maatregel**					
A5 - Organisatorische beheersmaatregelen	A.5.1	Beleidsregels voor informatiebeveiliging	Beheerst		x	x	x
	A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Beheerst			x	x
	A.5.3	Functiescheiding	Beheerst			x	
	A.5.4	Managementverantwoordelijkheden	Beheerst		x	x	x
	A.5.5	Contact met overheidsinstanties	Beheerst		x	x	
	A.5.6	Contact met speciale belangengroepen	Beheerst		x		x
	A.5.7	Informatie en analyses over dreigingen	Beheerst		x	x	x
	A.5.8	Informatiebeveiliging in projectmanagement	Beheerst		x	x	x
	A.5.9	Inventarisatie van informatie en andere gerelateerde	Beheerst		x		x
	A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde	Beheerst		x	x	x
	A.5.11	Retourneren van bedrijfsmiddelen	Beheerst		x	x	x
	A.5.12	Classificeren van informatie	Beheerst				x
	A.5.13	Labelen van informatie	Beheerst				x
	A.5.14	Overdragen van informatie	Beheerst		x	x	x
	A.5.15	Toegangsbeveiliging	Beheerst		x	x	x
	A.5.16	Identiteitsbeheer	Beheerst		x	x	
	A.5.17	Authenticatie-informatie	Beheerst		x	x	x
	A.5.18	Toegangsrechten	Beheerst		x	x	x
	A.5.19	Informatiebeveiliging in leveranciersrelaties	Beheerst		x	x	x
	A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomste	Beheerst		x	x	x
	A.5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Beheerst		x	x	x
	A.5.22	Monitoren, beoordelen en het beheren van wijzigingen van	Beheerst				x
	A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Beheerst			x	x
	A.5.24	Plannen en voorbereiden van het beheer van	Beheerst		x	x	
	A.5.25	Beoordelen van en besluiten over	Beheerst		x	x	x
	A.5.26	Reageren op informatiebeveiligingsincidenten	Beheerst		x	x	x
	A.5.27	Leren van informatiebeveiligingsincidenten	Beheerst		x	x	
	A.5.28	Verzamelen van bewijsmateriaal	Beheerst		x	x	
	A.5.29	Informatiebeveiliging tijdens een verstoring	Beheerst			x	
	A.5.30	ICT-gereedheid voor bedrijfscontinuïteit	Beheerst			x	x
	A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Beheerst		x	x	x
	A.5.32	Intellectuele-eigendomsrechten	Beheerst		x	x	x
	A.5.33	Beschermen van registraties	Beheerst			x	x
	A.5.34	Privacy en bescherming van persoonsgegevens	Beheerst		x	x	x
	A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	Beheerst		x	x	
	A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Beheerst		x	x	x
	A.5.37	Gedocumenteerde bedieningsprocedures	Beheerst		x	x	x
A6 - Mensgerichte beheersmaatregelen	A.6.1	Screening	Beheerst			x	x
	A.6.2	Arbeidsovereenkomst	Beheerst			x	x
	A.6.3	Bewustwording van, opleiding en training in informatiebeveiligin	Beheerst			x	x
	A.6.4	Disciplinaire procedure	Beheerst			x	x
	A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het	Beheerst			x	x
	A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Beheerst				x
	A.6.7	Werken op afstan	Beheerst		x		x
	A.6.8	Melden van informatiebeveiligingsgebeurtenisse	Beheerst				x
A7 - Fysieke beheersmaatregelen	A.7.1	Fysieke beveiligingszones	Beheerst		x	x	x
	A.7.2	Fysieke toegangsbeveiliging	Beheerst		x	x	x
	A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Beheerst		x	x	x
	A.7.4	Monitoren van de fysieke beveiliging	Beheerst		x	x	x
	A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Beheerst		x	x	x
	A.7.6	Werken in beveiligde zones	Beheerst		x	x	x
	A.7.7	Clear desk' en 'clear screen'	Beheerst		x	x	x
	A.7.8	Plaatsen en beschermen van apparatuur	Beheerst		x	x	
	A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Beheerst		x	x	x
	A.7.10	Opslagmedia	Beheerst		x		x
	A.7.11	Nutsvoorzieningen	Beheerst			x	x
	A.7.12	Beveiligen van bekabeling	Beheerst		x	x	x
	A.7.13	Onderhoud van apparatuur	Beheerst		x		x
	A.7.14	Veilig verwijderen of hergebruiken van apparatuur	Beheerst		x		
A8 - Technologische beheersmaatregelen	A.8.1	User endpoint devices'	Beheerst		x		x
	A.8.2	Speciale toegangsrechten	Beheerst		x	x	x
	A.8.3	Beperking toegang tot informatie	Beheerst		x	x	x
	A.8.4	Toegangsbeveiliging op broncode	Beheerst		x	x	x
	A.8.5	Beveiligde authenticatie	Beheerst				x
	A.8.6	Capaciteitsbeheer	Beheerst		x	x	x
	A.8.7	Bescherming tegen malware	Beheerst				x
	A.8.8	Beheer van technische kwetsbaarheden	Beheerst		x	x	x
	A.8.9	Configuratiebeheer	Beheerst			x	x
	A.8.10	Wissen van informatie	Beheerst		x	x	x
	A.8.11	Maskeren van gegevens	Beheerst		x	x	
	A.8.12	Voorkomen van gegevenslekken (data leakage prevention)	Beheerst		x	x	x
	A.8.13	Back-up van informatie	Beheerst			x	x
	A.8.14	Redundantie van informatieverwerkende faciliteiten	Beheerst			x	x
	A.8.15	Logging	Beheerst		x		x
	A.8.16	Monitoren van activiteiten	Beheerst		x	x	x
	A.8.17	Kloksynchronisatie	Beheerst			x	
	A.8.18	Gebruik van speciale systeemhulpmiddelen	Beheerst		x	x	x
	A.8.19	Installeren van software op operationele systemen	Beheerst			x	x
	A.8.20	Beveiliging netwerkcomponenten	Beheerst		x	x	x
	A.8.21	Beveiliging van netwerkdiensten	Beheerst		x	x	x
	A.8.22	Netwerksegmentatie	Beheerst		x	x	x
	A.8.23	Toepassen van webfilters	Beheerst				x
	A.8.24	Gebruik van cryptografie	Beheerst		x	x	x
	A.8.25	Beveiligen tijdens de ontwikkelcyclus	Beheerst		x	x	x
	A.8.26	Toepassingsbeveiligingseisen	Beheerst		x	x	x
	A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Beheerst		x	x	x
	A.8.28	Veilig coderen	Beheerst		x	x	x
	A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Beheerst		x	x	x
	A.8.30	Uitbestede systeemontwikkeling	Beheerst		x	x	x
	A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Beheerst		x	x	
	A.8.32	Wijzigingsbeheer	Beheerst			x	x
	A.8.33	Testgegevens	Beheerst		x	x	
	A.8.34	Bescherming van informatiesystemen tijdens audits	Beheerst		x	x	

Statement of Applicability

Current as of: 2024-08-26

Legend (for Selected Controls and Reasons for controls selection)
LR: **legal requirements**,CO: **contractual obligations**,RRA: **results of risk assessment**

ISO/IEC 27001:2022 Annex A controls			Current controls	Remarks (with justification for exclusions)	Selected controls and reasons for selection		
					LR	CO	RRA
Clause	**Sec**	**Control Objective/Control**					
A5 - Organizational controls	A.5.1	Policies for information security	Managed		x	x	x
	A.5.2	Information security roles and responsibilities	Managed			x	x
	A.5.3	Segregation of duties	Managed			x	
	A.5.4	Management responsibilities	Managed		x	x	x
	A.5.5	Contact with authorities	Managed		x	x	
	A.5.6	Contact with special interest groups	Managed		x		x
	A.5.7	Threat intelligence	Managed		x	x	x
	A.5.8	Information security in projectmanagement	Managed		x	x	x
	A.5.9	Inventory of information and other associated assets	Managed		x		x
	A.5.10	Acceptable use of information and other associated assets	Managed		x	x	x
	A.5.11	Return of assets	Managed		x	x	x
	A.5.12	Classification of information	Managed				x
	A.5.13	Labelling of information	Managed				x
	A.5.14	Information transfer	Managed		x	x	x
	A.5.15	Access control	Managed		x	x	x
	A.5.16	Identity management	Managed		x	x	
	A.5.17	Authentication information	Managed		x	x	x
	A.5.18	Access rights	Managed		x	x	x
	A.5.19	Information security in supplier relationships	Managed		x	x	x
	A.5.20	Addressing information security within supplier agreements	Managed		x	x	x
	A.5.21	Managing information security in the information	Managed		x	x	x
	A.5.22	Monitoring, review and change management of supplier services	Managed				x
	A.5.23	Information security for use of cloud services	Managed			x	x
	A.5.24	Information security incident management planning and preparation	Managed		x	x	
	A.5.25	Assessment and decision on information security events	Managed		x	x	x
	A.5.26	Response to information security incidents	Managed		x	x	x
	A.5.27	Learning from information security incidents	Managed		x	x	
	A.5.28	Collection of evidence	Managed		x	x	
	A.5.29	Information security during disruption	Managed			x	
	A.5.30	ICT readiness for business continuity	Managed			x	x
	A.5.31	Legal, statutory, regulatory and contractual requirements	Managed		x	x	x
	A.5.32	Intellectual property rights	Managed		x	x	x
	A.5.33	Protection of records	Managed			x	x
	A.5.34	Privacy and protection of personal identifiable information (PII)	Managed		x	x	x
	A.5.35	Independent review of information security	Managed		x	x	
	A.5.36	Compliance with policies, rules and standards for information	Managed		x	x	x
	A.5.37	Documented operating procedures	Managed		x	x	x
A6 - People controls	A.6.1	Screening	Managed			x	x
	A.6.2	Terms and conditions of employment	Managed			x	x
	A.6.3	Information security awareness, education and training	Managed			x	x
	A.6.4	Disciplinary process	Managed			x	x
	A.6.5	Responsibilities after termination or change of employment	Managed			x	x
	A.6.6	Confidentiality or non-disclosure agreements	Managed				x
	A.6.7	Remote working	Managed		x		x
	A.6.8	Information security event reporting	Managed				x
A7 - Physical controls	A.7.1	Physical security perimeters	Managed		x	x	x
	A.7.2	Physical entry	Managed		x	x	x
	A.7.3	Securing offices, rooms and facilities	Managed		x	x	x
	A.7.4	Physical security monitoring	Managed		x	x	x
	A.7.5	Protecting against physical and environmental threats	Managed		x	x	x
	A.7.6	Working in secure areas	Managed		x	x	x
	A.7.7	Clear desk and clear screen	Managed		x	x	x
	A.7.8	Equipment siting and protection	Managed		x	x	
	A.7.9	Security of assets off-premises	Managed		x	x	x
	A.7.10	Storage media	Managed		x		x
	A.7.11	Supporting utilities	Managed			x	x
	A.7.12	Cabling security	Managed		x	x	x
	A.7.13	Equipment maintenance	Managed		x		x
	A.7.14	Secure disposal or re-use of equipment	Managed		x		
A8 - Technological controls	A.8.1	User end point devices	Managed		x		x
	A.8.2	Privileged access rights	Managed		x	x	x
	A.8.3	Information access restriction	Managed		x	x	x
	A.8.4	Access to source code	Managed		x	x	x
	A.8.5	Secure authentication	Managed				x
	A.8.6	Capacity management	Managed		x	x	x
	A.8.7	Protection against malware	Managed				x
	A.8.8	Management of technical vulnerabilities	Managed		x	x	x
	A.8.9	Configuration management	Managed			x	x
	A.8.10	Information deletion	Managed		x	x	x
	A.8.11	Data masking	Managed		x	x	
	A.8.12	Data leakage prevention	Managed		x	x	x
	A.8.13	Information backup	Managed			x	x
	A.8.14	Redundancy of information processing facilities	Managed			x	x
	A.8.15	Logging	Managed		x		x
	A.8.16	Monitoring activities	Managed		x	x	x
	A.8.17	Clock synchronization	Managed			x	
	A.8.18	Use of privileged utility programs	Managed		x	x	x
	A.8.19	Installation of software on operational systems	Managed			x	x
	A.8.20	Networks security	Managed		x	x	x
	A.8.21	Security of network services	Managed		x	x	x
	A.8.22	Segregation of networks	Managed		x	x	x
	A.8.23	Web filtering	Managed				x
	A.8.24	Use of cryptography	Managed		x	x	x
	A.8.25	Secure development life cycle	Managed		x	x	x
	A.8.26	Application security requirements	Managed		x	x	x
	A.8.27	Secure system architecture and engineering principles	Managed		x	x	x
	A.8.28	Secure coding	Managed		x	x	x
	A.8.29	Security testing in development and acceptance	Managed		x	x	x
	A.8.30	Outsourced development	Managed		x	x	x
	A.8.31	Separation of development, test and production environments	Managed		x	x	
	A.8.32	Change management	Managed			x	x
	A.8.33	Test information	Managed		x	x	
	A.8.34	Protection of information systems during audit testing	Managed		x	x	