Bron: NEN-EN-ISO/IEC 27002:2022 **versie 2, dec '22**

Hoofdstuk Hfd gebied bijlage A	Nr	**ISO 27002:2022 Annex A** **5 Organisatorische beheersmaatregelen**	**5 Organizational controls**	**Gekoppelde maatregelen (controls)**	**ISO verwijzing(en)**	**Lijkt op Ann. A 2013** Beheersmaatregel	**Document status**
Organisatorische maatregelen	5.1	Beleidregels voor informatiebeveiliging	Policies for information security	n.v.t.	n.v.t.	A5.1.1, A5.1.2	onderhanden
	5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Information security roles and responsibilities	5.1	n.v.t.	A6.1.1	-
	5.3	Functiescheiding	Segregation of duties	n.v.t.	n.v.t.	A6.1.2	-
	5.4	Managementverantwoordelijkheden	Management responsibilities	6.3	n.v.t.	A7.2.1	-
	5.5	Contact met overheidsinstanties	Contact with authorities	5.24 t/m 5.30	n.v.t.	A6.1.3	-
	5.6	Contact met speciale belangengroepen	Contact with special interest groups	5.24 t/m 5.28	n.v.t.	A6.1.4	-
	5.7	Informatie en analyses over dreigingen	Threat intelligence	5.25, 8.7, 8.16 of 8.23	n.v.t.	**Nieuw / new**	-
	5.8	Informatiebeveiliging in projectmanagement	Information security in project management	8.26, 5.32, 5.12	ISO 21500 en ISO 21502 ISO 27005	A6.1.5, A14.1.1	-
	5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen (assets)	Inventory of information and other associated assets	5.12, 5.13, 5.10	ISO 19770-1, ISO 55001	A8.1.1, A8.1.2	-
	5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Acceptable use of information and other associated assets	5.12, 7.8, 7.10, 8.10	n.v.t.	A8.1.3, A8.2.3	-
	5.11	Retourneren van bedrijfsmiddelen (assets)	Return of assets	7.14, 5.18, 8.24	n.v.t.	A8.1.4	-
	5.12	Classificeren van informatie	Classification of information	5.1	n.v.t.	A8.2.1	-
	5.13	Labelen van informatie	Labelling of information	5.12	n.v.t.	A8.2.2	-
	5.14	Overdragen van informatie	Information transfer	5.10, 8.24, 5.13, 5.10, 5.31 t/m 5.34, 8.7	n.v.t.	A13.2.1, A13.2.2, A13.2.3	-
	5.15	Toegangsbeveiliging	Access control	8.26, 7.7 t/m 7.4, 5.10, 5.12, 5.13, 8.2, 5.3, 5.31 t/m 5.34, 8.3, 5.16, 5.18, 8.15, 5.16, 5.1, 5.17, 5.18, 8.3, 8.4, 8.5	n.v.t.	A9.1.1, A9.1.2	-
	5.16	Identiteitsbeheer	Identity management	5.19, 5.17, 5.18	n.v.t.	A9.2.1	-
	5.17	Beheren van authenticatie-informatie	Identity management	6.2, 8.24	ISO 24760-reeks	A9.2.4, A9.3.1, A9.4.3	-
	5.18	Toegangsrechten	Access rights	5.9, 5.15, 5.3, 6.1 t/m 6.5, 5.20, 6.6	n.v.t.	A9.2.2, A9.2.5, A9.2.6	-
	5.19	Informatiebeveiliging in leveranciersrelaties	Information security in supplier relationships	n.v.t.	ISO 27036-2	A15.1.1	-
	5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Addressing information security within supplier agreements	5.10, 5.12, 5.13	ISO 27036-reeks, ISO 19086-reeks	A15.1.2	-
	5.21	Beheer van informatiebeveiliging in de ICT-toeleveringsketen	Managing information security in the ICT supply chain	n.v.t.	ISO 27036-3, ISO 19770-2	A15.1,3	-
	5.22	Monitoring, beoordeling en het beheren van wijzigingen van leveranciersdiensten	Monitoring, review and change management of supplier services	5.29, .5.30, 5.35, 5.36, 8.14	ISO 27036-3	A15.2.1, A15.2.2	-
	5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Information security for use of cloud services	5.21, 5.22	ISO 17788, ISO 17789, ISO 22123-1, ISO 19941, ISO 27017, ISO 27018, ISO 27036-4, ISO 19086-reeks	**Nieuw / new**	-
	5.24	Planning en voorbereiding van het beheer van informatiebeveiligingsincidenten	Information security incident management planning and preparation	6.8, 8.15, 8.16, 5.25, 5.26, 5.5, 5.6, 5.28	ISO 27035	A16.1.1	-
	5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Assessment and decision on information security events	n.v.t.	ISO 27035	A16.1.4	-
	5.26	Reactie op informatiebeveiligingsincidenten	Response to information security incidents	5.24, 5.28, 5.29, 5.30, 5.27	ISO 27035	A16.1.5	-
	5.27	Leren van informatiebeveiligingsincidenten	Learning from information security incidents	5.24, 6.3	ISO 27035	A16.1.6	-
	5.28	Verzamelen van bewijsmateriaal	Collection of evidence	n.v.t.	ISO 27037, ISO 27050	A16.1.7	-
	5.29	Informatiebeveiliging tijdens een verstoring	Information security during disruption	n.v.t.	ISO 22301, ISO 22313, ISO 22317	A17.1.1, A17.1.2, A17.1.3	-
	5.30	ICT-gereedheid voor bedrijfscontinuïteit	ICT readiness for business continuity	n.v.t.	ISO 27031, ISO 22301, ISO 22313	**Nieuw / new**	-
	5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Identification of legal, statutory, regulatory and contractual requirements	5.20	n.v.t.	A18.1.1, A18.1.5	-
	5.32	Intellectuele-eigendomsrechten	Intellectual property rights	n.v.t.	ISO 19770, ISO 23751	A18.1.2	-
	5.33	Beschermen van registraties	Protection of records	8.24	ISO 15489	A18.1.3	-
	5.34	Privacy en bescherming van persoonsgegevens	Privacy and protection of PII	n.v.t.	ISO 29100, ISO 27701, ISO 27018, ISO 29134, ISO 27005	A18.1.4	-
	5.35	Onafhankelijke beoordeling van informatiebeveiliging	Independent review of information security	5.1	ISO 27007, ISO 27008	A18.2.1	-
	5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Compliance with policies and standards for information security	5.35, 8.15, 8.16, 8.17	n.v.t.	A18.2.2, A18.2.3	-
	5.37	Gedocumenteerde bedieningsprocedures	Documented operating procedures	8.13, 8.18, 7.10, 7.14, 8.15, 8.17, 7.4, 8.6, 8.16	n.v.t.	A12.1.1	-

subparagraaf; Gekoppelde documenten, voorbeeldtekst t.b.v. maatregel

In de beleidsdocumenten Organisatorische maatregelen (H5), item 5.30 "ICT-gereedheid voor bedrijfscontinuïteit" item 5.37 "Gedocumenteerde bedieningsprocedures" en Technologische maatregelen en (H8) item 8.31 "Scheiding van ontwikkel-, test- en productieomgevingen" wordt beschreven hoe dit binnen de organisatie is ingeregeld.

Bron: NEN-EN-ISO/IEC 27002:2022 **versie 2, dec '22**

Hoofdstuk Hfd gebied bijlage A	Nr	**ISO 27002:2022 Annex A** **6 Beheersmaatregel t.a.v. mensen**	**6 People controls**	**Gekoppelde maatregelen (controls)**	**ISO verwijzing(en)**	**Lijkt op Ann. A 2013** Beheersmaatregel	**Document status**
Maatregelen tav mensen	6.1	Screening	Screening	n.v.t	n.v.t.	A7.1.1	-
	6.2	Arbeidsovereenkomst	Terms and conditions of employment	6.6, 5.32, 5.34, 5.9 t/m 5.13, 6.4	n.v.t.	A7.1.2	-
	6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Information security awareness, education and training	5.17	n.v.t.	A7.2.2	-
	6.4	Disciplinaire procedure	Disciplinary process	5.28	n.v.t.	A7.2.3	-
	6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Responsibilities after termination or change of employment	6.6, 6.2	n.v.t.	A7.3.1	-
	6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Confidentiality or non-disclosure agreements	5.31 t/m 5.34	n.v.t.	A.13.2.4	-
	6.7	Werken op afstand	Remote working	n.v.t	n.v.t.	A6.2.2	-
	6.8	Melden van informatiebeveiligingsgebeurtenissen	Information security event reporting	n.v.t	ISO 27035	A16.1.2, A16.1.3	-

subparagraaf; Gekoppelde documenten, voorbeeldtekst t.b.v. maatregel

In de beleidsdocumenten Organisatorische maatregelen (H5), item 5.30 "ICT-gereedheid voor bedrijfscontinuïteit" item 5.37 "Gedocumenteerde bedieningsprocedures" en Technologische maatregelen en (H8) item 8.31 "Scheiding van ontwikkel-, test- en productieomgevingen" wordt beschreven hoe dit binnen de organisatie is ingeregeld.

Bron: NEN-EN-ISO/IEC 27002:2022 **versie 2, dec '22**

Hoofdstuk Hfd gebied bijlage A	Nr	**ISO 27002:2022 Annex A** **7. Fysieke beheersmaatregelen**	**7 Physical controls**	**Gekoppelde maatregelen (controls)**	**ISO verwijzing(en)**	**Lijkt op Ann. A 2013** Beheersmaatregel	**Document status**
Fysieke maatregelen	7.1	Fysieke beveiligingszone	Physical security perimeter	n.v.t.	n.v.t.	A11.1.1	-
	7.2	Fysieke toegangsbeveiliging	Physical entry controls	5.18, 5.33, 5.17, 5.9, 7.10	n.v.t.	A11.1.2, A11.1.6	-
	7.3	Beveiligen van kantoren, ruimten en faciliteiten	Securing offices, rooms and facilities	n.v.t.	n.v.t.	A11.1.3	-
	7.4	Monitoren van de fysieke beveiliging	Physical security monitoring	n.v.t.	n.v.t.	**Nieuw**	-
	7.5	Bescherming tegen fysieke en omgevingsbedreigingen	Protecting against physical and environmental threats	n.v.t.	n.v.t.	A11.1.4	-
	7.6	Werken in beveiligde zones	Working in secure areas	n.v.t.	n.v.t.	A11.1.5	-
	7.7	Clear desk' en 'clear screen'	Clear desk and clear screen	n.v.t.	n.v.t.	A11.2.9	-
	7.8	Plaatsen en beschermen van apparatuur	Equipment siting and protection	n.v.t.	n.v.t.	A11.2.1	-
	7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Security of assets off-premises	5.14, 7.4, 7.5, 8.1, 6.7	n.v.t.	A11.2.6	-
	7.10	Opslagmedia	Storage media	5.14, 8.10, 7.14	n.v.t.	A8.3.1, A8.3.2, A8.3.3, A8.11.2.5	-
	7.11	Nutsvoorzieningen	Supporting utilities	n.v.t.	n.v.t.	A11.2.2	-
	7.12	Beveiligen van bekabeling	Cabling security	n.v.t.	n.v.t.	A11.2.3	-
	7.13	Onderhoud van apparatuur	Equipment maintenance	7.9, 7.14	n.v.t.	A11.2.4	-
	7.14	Veilig verwijderen of hergebruiken van apparatuur	Secure disposal or re-use of equipment	7.19, 8.10, 8.24	ISO 27040	A11.2.7	-

subparagraaf; Gekoppelde documenten, voorbeeldtekst t.b.v. maatregel
In de beleidsdocumenten Organisatorische maatregelen (H5), item 5.30 "ICT-gereedheid voor bedrijfscontinuïteit" item 5.37 "Gedocumenteerde bedieningsprocedures" en Technologische maatregelen en (H8) item 8.31 "Scheiding van ontwikkel-, test- en productieomgevingen" wordt beschreven hoe dit binnen de organisatie is ingeregeld.

Bron: NEN-EN-ISO/IEC 27002:2022 **versie 2, dec '22**

Hoofdstuk Hfd gebied bijlage A	Nr	**ISO 27002:2022 Annex A** **8. Technische beheersmaatregelen**	**8 Technological controls**	**Gekoppelde maatregelen (controls)**	**ISO verwijzing(en)**	**Lijkt op Ann. A 2013** Beheersmaatregel	**Document status**
Technische maatregelen	8.1	'User endpoint devices'	User endpoint devices	8.16, 8.9	n.v.t.	A6.2.1, A11.2.8	-
	8.2	Speciale toegangsrechten	Privileged access rights	5.15, 5.18, 5.17	ISO 29146	A9.2.3	-
	8.3	Beperking toegang tot informatie	Information access restriction	n.v.t.	ISO 29146	A9.4.1	-
	8.4	Toegangsbeveiliging op broncode	Access to source code	8.32	n.v.t.	A9.4.5	-
	8.5	Beveiligde authenticatie	Secure authentication	n.v.t.	ISO 29115	A9.4.2	-
	8.6	Capaciteitsbeheer	Capacity management	n.v.t.	ISO 23167	A12.1.3	-
	8.7	Bescherming tegen malware	Protection against malware	8.18, 8.32, 8.13, 6.3	n.v.t.	A12.2.1	-
	8.8	Beheer van technische kwetsbaarheden	Management of technical vulnerabilities	5.9 t/m 5.14, 5.20, 8.28, 8.32, 5.26, 8.20 t/m 8.22, 5.23, 8.32	ISO 27031, ISO 19086, ISO 27017	A12.6.1, A18.2.3	-
	8.9	Configuratiebeheer	Configuration management	5.32, 8.32	n.v.t.	**Nieuw / New**	-
	8.10	Wissen van informatie	Information deletion	7.14	ISO 27017, ISO 27555	**Nieuw / New**	-
	8.11	Maskeren van gegevens	Data leakage prevention	n.v.t.	ISO 27018	**Nieuw / New**	-
	8.12	Voorkomen van gegevenslekken (data leakage prevention)	Data masking	5.12, 5.15	n.v.t.	**Nieuw / New**	-
	8.13	Back-up van informatie	Data leakage prevention	5.30 , 8.10	ISO 27040	A12.3.1	-
	8.14	Redundantie van informatieverwerkende faciliteiten	Redundancy of information processing facilities	5.30	ISO 23167	A17.2.1	-
	8.15	Logging	Logging	8.17, 5.28, 8.11, 5.34, 5.25, 8.16	ISO 27017	A12.4.1, A12.4.2, A12.4.3	-
	8.16	Monitoren van activiteiten	Monitoring activities	5.25, 5.26, 5.7	n.v.t.	**Nieuw / New**	-
	8.17	Kloksynchronisatie	Clock synchronization	n.v.t.	n.v.t.	A12.4.4	-
	8.18	Gebruik van speciale systeemhulpmiddelen	Use of privileged utility programs	8.2	n.v.t.	A9.4.4	-
	8.19	Installeren van software op operationele systemen	Installation of software on operational systems	8.5, 8.29, 8.31, 8.8, 8.19, 5.22	n.v.t.	A12.5.1, A12.6.2	-
	8.20	Beveiliging netwerkcomponenten	Network controls	5.3, 5.22, 8.24, 5.14, 6.6, 8.16, 8.15	ISO 27033-reeks, ISO 23167	A13.1.1	-
	8.21	Beveiliging van netwerkdiensten	Security of network services	n.v.t.	ISO 29146	A13.1.2	-
	8.22	Netwerksegmentatie	Segregation in networks	5.15, 8.20	n.v.t.	A13.1.3	-
	8.23	Toepassen van webfilters	Web filtering	5.7	n.v.t.	**Nieuw / New**	-
	8.24	Gebruik van cryptografie	Use of cryptography	8.24, 5.31, 5.22	ISO 11770	A10.1.1, A10.1.2	-
	8.25	Beveiligen tijdens de ontwikkelcyclus	Secure development lifecycle	8.31, 8.28, 8.27, 5.8, 8.29, 8.4, 8.9, 8.32, 5.32, 8.30	n.v.t.	A14.2.1	-
	8.26	Toepassingsbeveiligingseisen	Application security requirements	5.17, 8.2, 8.5, 5.53 t/m 5.36	ISO 27034	A14.1.1, A14.1.3	-
	8.27	Veilige systeemarchitectuur en technische uitgangspunten	Secure system architecture and engineering principles	5.15, 5.18, 8.2, 5.16, 5.17, 5.12, 8.5	n.v.t.	A14.2.5	-
	8.28	Veilig coderen	Secure coding	8.29, 8.8	ISO 15408-reeks	**Nieuw / New**	-
	8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Security testing in development and acceptance	8.5, 8.3, 8.24, 8.28, 8.9, 8.20, 8.22,5.8, 5.20, 8.31	n.v.t.	A14.2.8, A14.2.9	-
	8.30	Uitbestede systeemontwikkeling	Outsourced development	5.32, 8.25 t/m 8.29, 8.31	ISO 27036	A14.2.7	-
	8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Separation of development, test and production environments	8.29, 8.33	n.v.t.	A12.1.4, A14.2.6	-
	8.32	Wijzigingsbeheer	Change management	8.29, 5.37, 5.30	n.v.t.	A12.1.2, A14.2.2, A14.2.3, A14.2.4	-
	8.33	Testgegevens	Test information	8.31, 8.11, 8.10	n.v.t.	A14.3.1	-
	8.34	Bescherming van informatiesystemen tijdens audits	Protection of information systems during audit and testing	n.v.t.	n.v.t.	A12.7.1	-

subparagraaf; Gekoppelde documenten, voorbeeldtekst t.b.v. maatregel(en)
In de beleidsdocumenten Organisatorische maatregelen (H5), item 5.30 "ICT-gereedheid voor bedrijfscontinuïteit" item 5.37 "Gedocumenteerde bedieningsprocedures" en Technologische maatregelen en (H8) item 8.31 "Scheiding van ontwikkel-, test- en productieomgevingen" wordt beschreven hoe dit binnen de organisatie is ingeregeld.

Disclaimer
Ondanks alle aan de samenstelling van de tekst bestede zorg, kan Management Projects bv. (MPbv) geen aansprakelijkheid aanvaarden voor eventuele schade, die zou kunnen voortvloeien uit enige fout, die in deze uitgave zou kunnen voorkomen. Alle rechten voorbehouden. Niets uit deze uitgave mag worden verveelvoudigd, opgeslagen in geautomatiseerd gegevensbestand, of openbaar gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opname, of op enige andere manier, zonder voorafgaande uitdrukkelijke toestemming van MPbv.

Documentstatussen	
-	
n.v.t.	
niet onderhanden	
gereed voor review	
onder controle	
gecontroleerd	
revisie	

Hieraan kunnen nog statussen worden toegevoegd!