

Verklaring van Toepasselijkheid ISO 27001

HealthConnected

- versie: 1.1 - datum: 7-1-2026



ISO 27001:2022 Beveiligingsdoelstellingen				Argumentatie				Maatregelen	
Annex	Ref	Titel	Van toe-passing	WR	RA	Argumenten voor uitsluiting	Geimple-menteerd	Beleid, maatregel of cluster van maatregelen	Omschrijving uit te voeren beheersmaatregel
Organisatorische beheersmaatregelen	5.1	Beleidsregels voor informatiebeveiliging	Ja	NIS2	✓		Ja	Privacy- en Informatiebeveiligingsbeleid Onderliggend beleid	Opstellen, onderhouden en uitvoeren beleid Opstellen, onderhouden en uitvoeren onderliggend beleid Evaluatie tijdens managementreview
	5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Ja	NIS2	✓		Ja	Privacy- en Informatiebeveiligingsbeleid	Opstellen beleid
	5.3	Functiescheiding	Ja		✓		Ja	Privacy- en Informatiebeveiligingsbeleid Personeel en organisatie Functieprofielen	Opstellen beleid Opstellen functieprofielen
	5.4	Managementverantwoordelijkheden	Ja		✓		Ja	Privacy- en Informatiebeveiligingsbeleid Handboek privacy en informatiebeveiliging Awareness policy Functieprofielen	Ondertekenen Contract Ondertekenen Handboek privacy en informatiebeveiliging Overhandigen Privacy- en Informatiebeveiligingsbeleid Overhandigen functieprofiel
	5.5	Contact met overheidsinstanties	Ja		✓		Ja	ISMS: Context van de organisatie ISMS: Bronnen	Up-to-date houden
	5.6	Contact met speciale belangengroepen	Ja		✓		Ja	ISMS: Context van de organisatie ISMS: Bronnen	Up-to-date houden
	5.7	Informatie en analyses over dreigingen	Ja	NIS2	✓		Ja	Risk management	Up-to-date houden
	5.8	Informatiebeveiliging in projectmanagement	Ja		✓		Ja	Change management Relationship management	Opstellen, onderhouden en uitvoeren beleid
	5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Ja		✓		Ja	Risk management ICT Operations	Up-to-date houden
	5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Ja		✓		Ja	Handboek privacy en informatiebeveiliging Personeel en organisatie Control of documents and records Risk management Access management ICT Operations	Opstellen, onderhouden en uitvoeren beleid
	5.11	Retourneren van bedrijfsmiddelen	Ja		✓		Ja	Personeel en organisatie Handboek privacy en informatiebeveiliging ICT Operations	Uitvoeren beleid
	5.12	Classificeren van informatie	Ja		✓		Ja	Control of documents and records	Opstellen, onderhouden en uitvoeren beleid
	5.13	Labelen van informatie	Ja		✓		Ja	Control of documents and records Risk management	Opstellen, onderhouden en uitvoeren beleid
	5.14	Overdragen van informatie	Ja	AVG	✓		Ja	Relationship management Handboek privacy en informatiebeveiliging ICT Operations Verwerkersovereenkomsten Evt. template Uitwisselingsovereenkomst faciliteren Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider Aansturen van netwerk provider Meewerken aan uitwisselingsovereenkomst
	5.15	Toegangsbeveiliging	Ja	NIS2 BEIS	✓		Ja	Access management	Opstellen, onderhouden en uitvoeren beleid
	5.16	Identiteitsbeheer	Ja	NIS2 BEIS AVG	✓		Ja	Access management	Opstellen, onderhouden en uitvoeren beleid
	5.17	Authenticatie-informatie	Ja		✓		Ja	Handboek privacy en informatiebeveiliging Access management ICT Operations	Uitvoeren beleid
	5.18	Toegangsrechten	Ja	NIS2 BEIS	✓		Ja	Access management Periodieke controle	Opstellen, onderhouden en uitvoeren beleid
	5.19	Informatiebeveiliging in leveranciersrelaties	Ja	NIS2	✓		Ja	Relationship management ICT Operations Supplier and software assessment Contract en SLA met leverancier	Opstellen, onderhouden en uitvoeren beleid
	5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Ja	NIS2	✓		Ja	Relationship management Supplier and software assessment Contract en SLA met leverancier	Opstellen, onderhouden en uitvoeren beleid

ISO 27001:2022 Beveiligingsdoelstellingen				Argumentatie				Maatregelen	
Annex	Ref	Titel	Van toepassing	WR	RA	Argumenten voor uitsluiting	Geïmplementeerd	Beleid, maatregel of cluster van maatregelen	Omschrijving uit te voeren beheersmaatregel
	5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Ja	NIS2	✓		Ja	Relationship management Supplier and software assessment Contract en SLA met leverancier Verwerkersovereenkomsten	Opstellen, onderhouden en uitvoeren beleid
	5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Ja	NIS2	✓		Ja	Relationship management Supplier and software assessment Periodieke controle	Uitvoeren beleid Aansturen van hosting provider
	5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Ja	NIS2	✓		Ja	Relationship management Supplier and software assessment ICT Operations Access management	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Ja	NIS2	✓		Ja	Privacy- en Informatiebeveiligingsbeleid Incident management	Opstellen beleid
	5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Ja	NIS2	✓		Ja	Incident management	Uitvoeren beleid
	5.26	Reageren op informatiebeveiligingsincidenten	Ja	NIS2	✓		Ja	Incident management	Uitvoeren beleid
	5.27	Leren van informatiebeveiligingsincidenten	Ja	NIS2	✓		Ja	Incident management	Uitvoeren beleid
	5.28	Verzamelen van bewijsmateriaal	Ja	NIS2	✓		Ja	Incident management	Uitvoeren beleid
	5.29	Informatiebeveiliging tijdens een verstoring	Ja	NIS2	✓		Ja	Contraiteitsplan Periodieke controle Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	5.30	ICT-gereedheid voor bedrijfscontinuïteit	Ja	NIS2	✓		Ja	Contraiteitsplan	Opstellen, onderhouden en uitvoeren beleid
	5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Ja		✓		Ja	Privacy- en Informatiebeveiligingsbeleid ISMS- Wet- en regelgeving	Opstellen, onderhouden en uitvoeren beleid
	5.32	Intellectuele-eigendomsrechten	Ja		✓		Ja	Personeel en organisatie Contracten medewerkers Handboek privacy en informatiebeveiliging	Opstellen, onderhouden en uitvoeren beleid
	5.33	Beschermen van registraties	Ja		✓		Ja	Handboek privacy en informatiebeveiliging ICT Operations	Opstellen, onderhouden en uitvoeren beleid
	5.34	Privacy en bescherming van persoonsgegevens	Ja	AVG	✓		Ja	Privacy- en Informatiebeveiligingsbeleid Handboek privacy en informatiebeveiliging	Opstellen, onderhouden en uitvoeren beleid
	5.35	Onafhankelijke beoordeling van informatiebeveiliging	Ja	NIS2	✓		Ja	Privacy- en Informatiebeveiligingsbeleid Internal audit plan External audits	Audits
	5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Ja	NIS2	✓		Ja	Privacy- en Informatiebeveiligingsbeleid IBMF (InformatiebeveiligingsManagementForum) Kwartaalrapportages Management review Periodieke controles PEN testen	Uitvoeren beleid
	5.37	Gedocumenteerde bedieningsprocedures	Ja		✓		Ja	Werkinstructies Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
Mensgerichte beheersmaatregelen	6.1	Screening	Ja	NIS2	✓		Ja	Personeel en organisatie	Uitvoeren screening
	6.2	Arbeidsovereenkomst	Ja		✓		Ja	Personeel en organisatie Arbeidscontracten Functieprofielen Privacy- en Informatiebeveiligingsbeleid Handboek privacy en informatiebeveiliging	Ondertekenen Contract Ondertekenen Handboek privacy en informatiebeveiliging Overhandigen functieprofiel
	6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Ja	NIS2	✓		Ja	Awareness policy	Opstellen, onderhouden en uitvoeren beleid
	6.4	Disciplinaire procedure	Ja	NIS2	✓		Ja	Handboek privacy en informatiebeveiliging	Opstellen, onderhouden en uitvoeren beleid
	6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Ja	NIS2	✓		Ja	Personeel en organisatie	Opstellen, onderhouden en uitvoeren beleid
	6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Ja	NIS2	✓		Ja	Handboek privacy en informatiebeveiliging Personeel en organisatie	Opstellen, onderhouden en uitvoeren beleid
	6.7	Werken op afstand	Ja		✓		Ja	Handboek privacy en informatiebeveiliging	Opstellen, onderhouden en uitvoeren beleid
	6.8	Melden van informatiebeveiligingsgebeurtenissen	Ja	NIS2	✓		Ja	Incident management	Uitvoeren beleid
	7.1	Fysieke beveiligingszones	Ja		✓		Ja	Access management Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider

ISO 27001:2022 Beveiligingsdoelstellingen				Argumentatie				Maatregelen	
Annex	Ref	Titel	Van toe-passing	WR	RA	Argumenten voor uitsluiting	Geimple-menteerd	Beleid, maatregel of cluster van maatregelen	Omschrijving uit te voeren beheersmaatregel
Fysieke beheersmaatregelen	7.2	Fysieke toegangsbeveiliging	Ja		✓		Ja	Access management Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	7.3	Beveiligen van kantoren, ruimten en faciliteiten	Ja		✓		Ja	Access management	Opstellen, onderhouden en uitvoeren beleid
	7.4	Monitoren van de fysieke beveiliging	Ja		✓		Ja	Access management Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	7.5	Beschermen tegen fysieke en omgevingsdreigingen	Ja		✓		Ja	Continuïteitsplan Bedrijfshulpverlening Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	7.6	Werken in beveiligde zones	Ja		✓		Ja	Borging door Outsourcing	Aansturen van hosting provider
	7.7	Clear desk en clear screen	Ja		✓		Ja	Handboek privacy en informatiebeveiliging	Opstellen, onderhouden en uitvoeren beleid
	7.8	Plaatsen en beschermen van apparatuur	Ja		✓		Ja	Borging door Outsourcing	Aansturen van hosting provider
	7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Ja		✓		Ja	Handboek privacy en informatiebeveiliging Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	7.10	Opslagmedia	Ja		✓		Ja	ICT Operations Handboek privacy en informatiebeveiliging Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	7.11	Nutsvoorzieningen	Ja		✓		Ja	Borging door Outsourcing	Aansturen van hosting provider
	7.12	Beveiligen van bekabeling	Ja		✓		Ja	Borging door Outsourcing	Aansturen van hosting provider
	7.13	Onderhoud van apparatuur	Ja		✓		Ja	Borging door Outsourcing	Aansturen van hosting provider
	7.14	Veilig verwijderen of hergebruiken van apparatuur	Ja		✓		Ja	ICT Operations Handboek privacy en informatiebeveiliging Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.1	User endpoint devices	Ja		✓		Ja	Handboek privacy en informatiebeveiliging ICT Operations Werkinstructies	Opstellen, onderhouden en uitvoeren beleid
	8.2	Speciale toegangsrechten	Ja	NIS2	✓		Ja	Access management	Opstellen, onderhouden en uitvoeren beleid
	8.3	Beperking toegang tot informatie	Ja	NIS2	✓		Ja	Access management	Opstellen, onderhouden en uitvoeren beleid
	8.4	Toegangsbeveiliging op broncode	Ja	NIS2	✓		Ja	Access management	Opstellen, onderhouden en uitvoeren beleid
	8.5	Beveiligde authenticatie	Ja	NIS2 AVG	✓		Ja	Access management Handboek privacy en informatiebeveiliging ICT Operations	Opstellen, onderhouden en uitvoeren beleid
	8.6	Capaciteitsbeheer	Ja		✓		Ja	ICT Operations In-house monitoring Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.7	Bescherming tegen malware	Ja	NIS2	✓		Ja	ICT Operations Handboek privacy en informatiebeveiliging Awareness policy Cybersecurity verzekering Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.8	Beheer van technische kwetsbaarheden	Ja	NIS2	✓		Ja	Privacy- en Informatiebeveiligingsbeleid ICT Operations Risk management Incident management Development policy Periodieke controles PEN testen Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.9	Configuratiebeheer	Ja		✓		Ja	ICT Operations Development policy Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.10	Wissen van informatie	Ja	AVG	✓		Ja	ICT Operations Development policy	Opstellen, onderhouden en uitvoeren beleid
	8.11	Maskeren van gegevens	Ja	AVG	✓		Ja	Development policy	Opstellen, onderhouden en uitvoeren beleid
	8.12	Voorkomen van gegevenslekken (Data leakage prevention)	Ja	AVG	✓		Ja	ICT Operations Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.13	Back-up van informatie	Ja	NIS2	✓		Ja	ICT Operations Borging door Outsourcing Periodieke controle	Aansturen van hosting provider
	8.14	Redundantie van informatieverwerkende faciliteiten	Ja	NIS2	✓		Ja	ICT Operations Borging door Outsourcing	Aansturen van hosting provider

ISO 27001:2022 Beveiligingsdoelstellingen				Argumentatie				Maatregelen	
Annex	Ref	Titel	Van toe-passing	WR	RA	Argumenten voor uitsluiting	Geimple-menteerd	Beleid, maatregel of cluster van maatregelen	Omschrijving uit te voeren beheersmaatregel
Technologische beheersmaatregelen	8.15	Logging	Ja	BEIS AVG	✓		Ja	ICT Operations Development policy Access management Periodieke controle Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.16	Monitoren van activiteiten	Ja	NIS2	✓		Ja	ICT Operations In-house monitoring Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.17	Kloksynchronisatie	Ja		✓		Ja	ICT Operations Periodieke controle Borging door Outsourcing	Aansturen van hosting provider
	8.18	Gebruik van speciale systeemhulpmiddelen	Ja	NIS2	✓		Ja	Access management	Opstellen, onderhouden en uitvoeren beleid
	8.19	Installeren van software op operationele systemen	Ja		✓		Ja	ICT Operations Development policy Handboek privacy en informatiebeveiliging Periodieke controle Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.20	Beveiliging netwerkcomponenten	Ja	NIS2	✓		Ja	ICT Operations Borging door Outsourcing	Aansturen van hosting provider Aansturen van netwerk provider
	8.21	Beveiliging van netwerkdiensten	Ja	NIS2	✓		Ja	ICT Operations Borging door Outsourcing	Aansturen van hosting provider Aansturen van netwerk provider
	8.22	Netwerksegmentatie	Ja	NIS2	✓		Ja	ICT Operations Borging door Outsourcing	Aansturen van hosting provider Aansturen van netwerk provider
	8.23	Toepassen van webfilters	Ja		✓		Ja	ICT Operations Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.24	Gebruik van cryptografie	Ja	NIS2 AVG	✓		Ja	ICT Operations Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.25	Beveiligen tijdens de ontwikkelcyclus	Ja	NIS2	✓		Ja	Development policy	Opstellen, onderhouden en uitvoeren beleid
	8.26	Toepassingsbeveiligingseisen	Ja		✓		Ja	ICT Operations Development policy Handboek privacy en informatiebeveiliging Evt. template Uitwisselingsovereenkomst faciliteren Verwerkingsovereenkomsten met derden	Opstellen, onderhouden en uitvoeren beleid Meewerken aan uitwisselingsovereenkomst
	8.27	Veilige systeemarchitectuur en technische uitgangspunten	Ja	NIS2	✓		Ja	Development policy	Opstellen, onderhouden en uitvoeren beleid
	8.28	Veilig coderen	Ja	NIS2	✓		Ja	Development policy	Opstellen, onderhouden en uitvoeren beleid
	8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Ja	NIS2	✓		Ja	Change management Development policy	Opstellen, onderhouden en uitvoeren beleid
	8.30	Uitbestede systeemontwikkeling	Nee			HealthConnected maakt geen gebruik van externe leveranciers voor ontwikkeling	Nvt		
	8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ja	NIS2	✓		Ja	ICT Operations Development policy Borging door Outsourcing	Opstellen, onderhouden en uitvoeren beleid Aansturen van hosting provider
	8.32	Wijzigingsbeheer	Ja		✓		Ja	Change management Development policy	Opstellen, onderhouden en uitvoeren beleid
	8.33	Testgegevens	Ja		✓		Ja	Development policy	Opstellen, onderhouden en uitvoeren beleid
	8.34	Bescherming van informatiesystemen tijdens audits	Ja		✓		Ja	Privacy- en Informatiebeveiligingsbeleid PEN testen	Opstellen, onderhouden en uitvoeren beleid
Legenda voor reden voor selectie:									
WR = Wet en Regelgeving, RA = Risico Analyse									
Eisen aan het ISMS	Hoofdstuk 4	Context van de organisatie	Ja	AVG			Ja	Management review Privacy- en Informatiebeveiligingsbeleid ISMS: Context van de organisatie	Opstellen, onderhouden en uitvoeren beleid
	Hoofdstuk 5	Leiderschap	Ja	AVG			Ja	Privacy- en informatiebeveiligingsbeleid	Opstellen, onderhouden en uitvoeren beleid
	Hoofdstuk 6	Planning	Ja	AVG			Ja	Kwartaalrapportages Management review	Rapporteren PDCA
	Hoofdstuk 7	Ondersteuning	Ja	AVG			Ja	Privacy- en Informatiebeveiligingsbeleid Handboek privacy en informatiebeveiliging Procedures & Werkinstructies	Opstellen, onderhouden en uitvoeren beleid
	Hoofdstuk 8	Uitvoering	Ja	AVG			Ja	Procedures & Werkinstructies	Opstellen, onderhouden en uitvoeren beleid

ISO 27001:2022 Beveiligingsdoelstellingen				Argumentatie				Maatregelen	
Annex	Ref	Titel	Van toe- passing	WR	RA	Argumenten voor uitsluiting	Geimple- menteerd	Beleid, maatregel of cluster van maatregelen	Omschrijving uit te voeren beheersmaatregel
	Hoofdstuk 9	Evaluatie van de prestaties	Ja	AVG			Ja	Kwartaalrapportages Management review	Rapporteren PDCA
	Hoofdstuk 10	Verbetering	Ja	AVG			Ja	Management review	Rapporteren PDCA