	Verklaring van Toepasselijkheid V1.2, Key Groep, 13 april 2026					Reden voor opname			Uitbesteed	Reden voor uitsluiting
#	Titel maatregel		Beheersmaatregel	Van toepassing?	Geïmplementeerd?	Wet	Contract	Risico register		Onderbouwing waarom niet van toepassing
5	Organisatorische maatregelen									
5.1	Beleidsregels voor informatiebeveiliging	Beheersmaatregel ISO 27001	Informatiebeveiligingsbeleid en onderwerpspecifieke beleidsregels moeten worden gedefinieerd, goedgekeurd door het management, gepubliceerd, gecommuniceerd aan en erkend door relevant personeel en relevante belanghebbenden en met geplande tussenpozen en als zich significante wijzigingen voordoen, worden beoordeeld.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Het informatiebeveiligingsbeleid behoort de aanpak voor het beheer van informatiebeveiliging te beschrijven en te zijn goedgekeurd door het topmanagement, vervolgens ten minste eenmaal per jaar en daarna telkens als er zich een ernstige beveiligingsgebeurtenis voordoet te worden beoordeeld.	Ja	Ja			X		
5.2	Rollen en verantwoordelijkheden op het gebied van informatiebeveiliging	Beheersmaatregel ISO 27001	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Er behoort ten minste één persoon verantwoordelijk te zijn voor informatiebeveiliging.	Ja	Ja			X		
5.3	Functiescheiding	Beheersmaatregel ISO 27001	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja	Ja	X		X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.4	Managementverantwoordelijkheden	Beheersmaatregel ISO 27001	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerpspecifieke beleidsregels en procedures van de organisatie.	Ja	Ja		X	X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.5	Contact met overheidsinstanties	Beheersmaatregel ISO 27001	De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja	Ja	X		X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.6	Contact met speciale belangengroepen	Beheersmaatregel ISO 27001	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.7	Informatie en analyses over dreigingen	Beheersmaatregel ISO 27001	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn, overig	N.v.t.	N.v.t					
5.8	Informatiebeveiliging in projectmanagement	Beheersmaatregel ISO 27001	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn, overig	N.v.t.	N.v.t					
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Beheersmaatregel ISO 27001	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Alle informatiestromen (zowel binnen als tussen organisaties) en de interfaces daarvan (waaronder integratieplatforms) behoren te worden opgenomen in de inventarisatie.	Ja	Ja			X		
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Beheersmaatregel ISO 27001	Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	Ja	Ja	X		X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.11	Retourneren van bedrijfsmiddelen	Beheersmaatregel ISO 27001	Personeel en andere belanghebbenden, al naargelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Er behoort beleid te zijn dat vereist dat personen schriftelijk bevestigen dat alle bedrijfsmiddelen in hun bezit in alle formaten op veilige wijze zijn geretourneerd of verwijderd, indien van toepassing.	Ja	Ja			X		
5.12	Classificeren van informatie	Beheersmaatregel ISO 27001	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Persoonlijke gezondheidsinformatie behoort uniform als vertrouwelijk te worden geclassificeerd.	Ja	Ja			X		
5.13	Labelen van informatie	Beheersmaatregel ISO 27001	Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.14	Overdragen van informatie	Beheersmaatregel ISO 27001	Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn ingesteld voor alle soorten van communicatiefaciliteiten binnen de organisatie en tussen de organisatie en andere partijen.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Vóórdat enige overdracht plaatsvindt, behoren er regels, procedures en overeenkomsten te zijn ingesteld.	Ja	Ja			X		
5.15	Toegangsbeveiliging	Beheersmaatregel ISO 27001	Er moeten regels op basis van bedrijfs- en informatiebeveiligingseisen worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen.	Ja	Ja			X	Deels	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Er behoort beleid voor op rollen gebaseerde toegangsbeveiliging te gelden voor de toegang tot persoonlijke gezondheidsinformatie.	Ja	Ja			X	Deels	
5.16	Identiteitsbeheer	Beheersmaatregel ISO 27001	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Gebruikers die toegang willen hebben tot persoonlijke gezondheidsinformatie en andere vertrouwelijke informatie, behoren formeel te zijn geregistreerd.	Ja	Ja			X	Ja	
5.17	Beheren van authenticatie-informatie	Beheersmaatregel ISO 27001	De toewijzing en het beheer van authenticatie-informatie moet worden beheerst door middel van een beheerproces waarvan het adviseren van het personeel over de juiste manier van omgaan met authenticatie-informatie deel uitmaakt.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.18	Toegangsrechten	Beheersmaatregel ISO 27001	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijderd overeenkomstig het onderwerpspecifieke beleid en de regels inzake toegangsbeveiliging van de organisatie.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.19	Informatiebeveiliging in leveranciersrelaties	Beheersmaatregel ISO 27001	Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen.	Ja	Ja		X	X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	De risico's in verband met toegang door externe partijen tot systemen of de gegevens die zij bevatten behoren te worden beoordeeld en beheersmaatregelen passend bij het geïdentificeerde risico behoren te worden geïmplementeerd.	Ja	Ja			X		
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Beheersmaatregel ISO 27001	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja	Ja		X	X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.21	Beheer van informatiebeveiliging in de ICT-toeleveringsketen	Beheersmaatregel ISO 27001	Er moeten processen en procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en -diensten te beheersen.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn, overig	N.v.t.	N.v.t					
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Beheersmaatregel ISO 27001	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.23	Informatiebeveiliging voor het gebruik van cloud diensten	Beheersmaatregel ISO 27001	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja	Ja		X	X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, overig	N.v.t.	N.v.t					
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Beheersmaatregel ISO 27001	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Beheersmaatregel ISO 27001	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.26	Reageren op informatiebeveiligingsincidenten	Beheersmaatregel ISO 27001	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.27	Leren van informatiebeveiligingsincidenten	Beheersmaatregel ISO 27001	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de en voor informatiebeveiliging te versterken en te verbeteren.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.28	Verzamelen van bewijsmateriaal	Beheersmaatregel ISO 27001	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.29	Informatiebeveiliging tijdens een verstoring	Beheersmaatregel ISO 27001	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.30	ICT-gereedheid voor bedrijfscontinuïteit	Beheersmaatregel ISO 27001	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	Ja	Ja			X	Deels	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					

5.31	Wettelijke, statutaire, regelgevende en contractuele vereisten	Beheersmaatregel ISO 27001	Wettelijke, statutaire, regelgevende en contractuele eisen die relevant zijn voor informatiebeveiliging en de aanpak van de organisatie om aan deze eisen te voldoen, moeten worden geïdentificeerd, gedocumenteerd en actueel gehouden.	Ja	Ja	X	X	X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.32	Intellectuele eigendomsrechten	Beheersmaatregel ISO 27001	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	Ja	Ja	X		X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.33	Beschermen van registraties	Beheersmaatregel ISO 27001	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Ja	X		X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.34	Privacy en bescherming van persoonsgegevens	Beheersmaatregel ISO 27001	De organisatie moet de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen identificeren en eraan voldoen.	Ja	Ja	X		X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn, overig	N.v.t.	N.v.t					
5.35	Onafhankelijke beoordeling van informatiebeveiliging	Beheersmaatregel ISO 27001	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie ervan, met inbegrip van mensen, processen en technologieën, moeten onafhankelijk en met geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Beheersmaatregel ISO 27001	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
5.37	Gedocumenteerde bedieningsprocedures	Beheersmaatregel ISO 27001	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
5.38	HLT - Analyse en specificatie van informatie- beveiligingseisen	Beheersmaatregel ISO 27001	geen	N.v.t.	N.v.t					
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	De informatiebeveiligingsgerelateerde eisen behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen aan bestaande informatiesystemen.	Ja	Ja			X		
5.39	HLT – Zorgontvangers op unieke wijze identificeren	Beheersmaatregel ISO 27001	geen	N.v.t.	N.v.t					
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Beleid en processen behoren te waarborgen dat elke zorgontvanger op unieke wijze binnen het systeem kan worden geïdentificeerd en behoren in staat te zijn dubbele of meervoudige registraties samen te voegen als er dubbele of meervoudige registraties zijn voor een en dezelfde zorgontvanger.	Nee	Nee					We hebben geen toegang tot cliëntinformatiesystemen en er is geen noodzaak om deze cliënten te identificeren. We werken met anonieme data die niet te herleiden is tot een individu.
5.40	HLT – Validatie van getoonde/geprinte gegevens	Beheersmaatregel ISO 27001	geen	N.v.t.	N.v.t					
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Als er gegevens worden getoond en/of geprint door gezondheidsinformatiesystemen behoren deze gegevens ook informatie te omvatten waarmee de zorgontvanger waarop de gegevens betrekking heeft wordt geïdentificeerd.	Nee	Nee					We hebben geen toegang tot medische gegevens / cliëntinformatie.
5.41	HLT – Openbaar beschikbare gezondheidsinformatie	Beheersmaatregel ISO 27001	geen	N.v.t.	N.v.t					
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Openbaar beschikbare gezondheidsinformatie behoort te worden beschermd, bewaard en beheerd gedurende de volledige levenscyclus.	Nee	Nee					Wij beschikken niet over openbaar beschikbare gezondheidsinformatie.
5.42	HLT – Communicatie in noodsituaties	Beheersmaatregel ISO 27001	geen	N.v.t.	N.v.t					
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Noodcommunicatiekanalen binnen een zorgorganisatie die in werking treden wanneer er een storing is in de continuïteit van de ICT van de organisatie behoren te worden gepland, geïmplementeerd, onderhouden en beproefd.	Nee	Nee					We zijn geen zorgorganisatie.
5.43	HLT – Incidenten extern melden	Beheersmaatregel ISO 27001	geen	N.v.t.	N.v.t					
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Informatiebeveiligingsincidenten behoren volgens juridische of contractuele verplichtingen of verplichtingen uit hoofde van wet- en regelgeving te worden gemeld.	Ja	Ja	X		X		
6	Mensgerichte beheersmaatregelen									
6.1	Screening	Beheersmaatregel ISO 27001	De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie behoort te worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden te worden herhaald. Hierbij behoort rekening te worden gehouden met de toepasselijke wet- en regelgeving, voorschriften en ethische overwegingen, en deze controle behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
6.2	Arbeidsovereenkomst	Beheersmaatregel ISO 27001	In arbeidsovereenkomsten behoort te worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Ja		X	X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	In functiebeschrijvingen behoren de beveiligingsrollen en verantwoordelijkheden te worden vermeld die van toepassing zijn op het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja		X	X		
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Beheersmaatregel ISO 27001	Personeel van de organisatie en relevante belanghebbenden behoren een passend(e) bewustwordingvan, opleiding, training en bijscholing in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, te krijgen.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn, overig	N.v.t.	N.v.t					
6.4	Disciplinaire procedure	Beheersmaatregel ISO 27001	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Beheersmaatregel ISO 27001	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn, overig	N.v.t.	N.v.t					
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Beheersmaatregel ISO 27001	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, behoren te worden geïdentificeerd, gedocumenteerd, regelmatig te worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Ja		X	X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Alle personeel dat bevoegd is tot toegang tot persoonlijke gezondheidsinformatie behoort er formeel toe te worden verplicht die informatie vertrouwelijk te behandelen.	Ja	Ja			X		
6.7	Werken op afstand	Beheersmaatregel ISO 27001	Wanneer personeel op afstand werkt, behoren er beveiligingsmaatregelen te worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezien, verwerkt of opgeslagen.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, overig	N.v.t.	N.v.t					
6.8	Melden van informatiebeveiligingsgebeurteniss en	Beheersmaatregel ISO 27001	De organisatie behoort te voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
6.9	HLT – Managementtraining	Beheersmaatregel ISO 27001	geen	N.v.t.	N.v.t					
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Het management van de organisatie behoort passende training te krijgen, naarmate relevant is voor hun rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en hoe het wordt beheerd.	Ja	Ja			X		
7	Fysieke maatregelen									
7.1	Fysieke beveiligingszones	Beheersmaatregel ISO 27001	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
7.2	Fysieke toegangsbeveiliging	Beheersmaatregel ISO 27001	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Beheersmaatregel ISO 27001	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
7.4	Monitoren van de fysieke beveiliging	Beheersmaatregel ISO 27001	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
7.5	Bescherming tegen fysieke en omgevingsbedreigingen	Beheersmaatregel ISO 27001	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
7.6	Werken in beveiligde zones	Beheersmaatregel ISO 27001	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
7.7	'Clear desk' en 'clear screen'	Beheersmaatregel ISO 27001	Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
7.8	Plaatsen en beschermen van apparatuur	Beheersmaatregel ISO 27001	Apparatuur moet veilig worden geplaatst en beschermd.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024		N.v.t.	N.v.t					
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Beheersmaatregel ISO 27001	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
7.10	Opslagmedia	Beheersmaatregel ISO 27001	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Alle persoonlijke gezondheidsinformatie die op verwijderbare media wordt opgeslagen, behoort te worden versleuteld.	Nee	Nee					We maken geen gebruik van verwijderbare media.
7.11	Nuts-voorzieningen	Beheersmaatregel ISO 27001	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
7.12	Beveiligen van bekabeling	Beheersmaatregel ISO 27001	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Ja			X		

		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
7.13	Onderhoud van de apparatuur	Beheersmaatregel ISO 27001	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
7.14	Veilig verwijderen of hergebruiken van apparatuur	Beheersmaatregel ISO 27001	Onderdelen van de apparatuur die opslagmedia bevatten, moeten worden gecontroleerd om te waarborgen dat gevoelige gegevens en gelicentieerde software zijn verwijderd of veilig zijn overschreven voordat ze worden verwijderd of hergebruikt.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn, overig	N.v.t.	N.v.t					
8	Technische maatregelen	Beheersmaatregel ISO 27001								
8.1	'User endpoint devices'	Beheersmaatregel ISO 27001	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, overig	N.v.t.	N.v.t					
8.2	Speciale toegangsrechten	Beheersmaatregel ISO 27001	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.3	Beperking toegang tot informatie	Beheersmaatregel ISO 27001	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.4	Toegangsbeveiliging op broncode	Beheersmaatregel ISO 27001	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Nee	Nee					We hebben geen beschikking over broncode/ontwikkeling.
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.5	Beveiligde authenticatie	Beheersmaatregel ISO 27001	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Er behoort ten minste tweefactorauthenticatie te worden gebruikt voor systemen die persoonlijke gezondheidsinformatie verwerken	Ja	Ja			X		
8.6	Capaciteitsbeheer	Beheersmaatregel ISO 27001	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.7	Bescherming tegen malware	Beheersmaatregel ISO 27001	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.8	Beheer van technische kwetsbaarheden	Beheersmaatregel ISO 27001	Er moet informatie worden verkregen over technische kwetsbaarheden van in gebruik zijnde informatiesystemen, de blootstelling van de organisatie aan dergelijke kwetsbaarheden moet worden geëvalueerd en er moeten passende maatregelen worden getroffen.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.9	Configuratiebeheer	Beheersmaatregel ISO 27001	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.10	Wissen van informatie	Beheersmaatregel ISO 27001	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.11	Maskeren van gegevens	Beheersmaatregel ISO 27001	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, overig	N.v.t.	N.v.t					
8.12	Voorkomen van gegevenslekken (Data leakage prevention)	Beheersmaatregel ISO 27001	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt verwerkt, opgeslagen of getransporteerd.	Ja	Ja	X		X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.13	Back-up van informatie	Beheersmaatregel ISO 27001	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Back-ups van persoonlijke gezondheidsinformatie behoren te worden versleuteld.	Ja	Ja					
8.14	Redundantie van informatieverwerkende faciliteiten	Beheersmaatregel ISO 27001	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.15	Logging	Beheersmaatregel ISO 27001	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.16	Monitoren van activiteiten	Beheersmaatregel ISO 27001	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.17	Kloksynchronisatie	Beheersmaatregel ISO 27001	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.18	Gebruik van speciale systeemhulpmiddelen	Beheersmaatregel ISO 27001	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om en voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.19	Installeren van software op operationele systemen	Beheersmaatregel ISO 27001	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.20	Beveiliging netwerkcomponenten	Beheersmaatregel ISO 27001	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.21	Beveiliging van netwerkdiensten	Beheersmaatregel ISO 27001	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.22	Netwerksegmentatie	Beheersmaatregel ISO 27001	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, overig	N.v.t.	N.v.t					
8.23	Toepassen van webfilters	Beheersmaatregel ISO 27001	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, overig	N.v.t.	N.v.t					
8.24	Gebruik van cryptografie	Beheersmaatregel ISO 27001	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja	Ja			X	Ja	
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, overig	N.v.t.	N.v.t					
8.25	Beveiligen tijdens de ontwikkelcyclus	Beheersmaatregel ISO 27001	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Nee	Nee					We ontwikkelen geen software en systemen.
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.26	Toepassingsbeveiligingseisen	Beheersmaatregel ISO 27001	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn, overig	N.v.t.	N.v.t					
8.27	Veilige systeem-architectuur en technische uitgangspunten	Beheersmaatregel ISO 27001	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Nee	Nee					We ontwikkelen geen software en systemen.
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.28	Veilig coderen	Beheersmaatregel ISO 27001	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Nee	Nee					We ontwikkelen geen software en systemen.
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Beheersmaatregel ISO 27001	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Nee	Nee					We hebben geen toegang tot ontwikkeling- en acceptatieomgevingen.
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.30	Uitbestede systeemontwikkeling	Beheersmaatregel ISO 27001	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Nee					We maken geen gebruik van uitbestede systeemontwikkeling. We kopen standaard applicaties in.
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Beheersmaatregel ISO 27001	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Nee	Nee					We hebben geen toegang tot diverse ontwikkelomgevingen.
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.32	Wijzigingsbeheer	Beheersmaatregel ISO 27001	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.33	Testgegevens	Beheersmaatregel ISO 27001	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Nee	Nee					We hebben geen toegang tot testgegevens.
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen, richtlijn	N.v.t.	N.v.t					
8.34	Bescherming van informatiesystemen tijdens audits	Beheersmaatregel ISO 27001	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Ja			X		
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	geen	N.v.t.	N.v.t					
8.35	HLT – Zero trust-beginselen	Beheersmaatregel ISO 27001	geen	N.v.t.	N.v.t					
		Zorgspecifieke Beheersmaatregel NEN 7510-2:2024	Aan een netwerksegment toegewezen groepen informatiediensten, gebruikers en informatiesystemen behoren zo klein mogelijk te worden gehouden en behoren slechts toegang tot een ander netwerksegment te hebben nadat beide betrokken segmenten elkaar hebben geauthentiseerd.	Ja	Ja			X		