

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Verklaring van Toepasselijkheid - Deltacom												
2	Versie: 3.0			Versiedatum: 01-04-2026									
3	NEN 7510-1:2024 NL					Van toepassing?	Reden van aanwezigheid				Volledig geïmplementeerd?	Uitbested	Reden van uitsluiting
4							WR	CO	BR	RA			
5	Hoofdstukken	ISO 27001:2023 opzichts	NEN 7510:2024	Titel beheersmaatregel	Beheersmaatregel								
6	5.1	A.5.1	Beleidsregels voor informatiebeveiliging		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 of zodra zich belangrijke veranderingen voordoen, worden beoordeeld. Zorgspecifieke beheersmaatregel (aanvullend) Het informatiebeveiligingsbeleid moet de aanpak voor het beheer van informatiebeveiliging 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			x	x	Ja	Nee	
7	5.2	A.5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging		Alle verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie. Zorgspecifieke beheersmaatregel (aanvullend) Er moet ten minste één persoon verantwoordelijk zijn voor informatiebeveiliging	Ja			x	x	Ja	Nee	
8	5.3	A.5.3	Functiescheiding		Conflicterende taken en verantwoordelijkheden moeten worden gescheiden.	Ja			x	x	Ja	Nee	
9	5.4	A.5.4	Managementverantwoordelijkheden		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			x	x	Ja	Nee	
10	5.5	A.5.5	Contact met overheidsinstanties		De organisatie moet contact met de relevante instanties leggen en te onderhouden.	Ja			x	x	Ja	Nee	
11	5.6	A.5.6	Contact met speciale belangengroepen		De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en te onderhouden.	Ja			x	x	Ja	Nee	
12	5.7	A.5.7	Informatie en analyses over dreigingen		Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie en analyses over dreigingen te produceren.	Ja			x	x	Ja	Nee	
13	5.8	A.5.8	Informatiebeveiliging in projectmanagement		Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja			x	x	Ja	Nee	
14	5.9	A.5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen		Er moet een inventaristijl van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden. Zorgspecifieke beheersmaatregel (aanvullend) Alle informatiestromen (zowel binnen als tussen organisaties) en de interfaces daarvan (waaronder integratieplatforms) moeten worden opgenomen in de inventarisatie	Ja			x	x	Ja	Nee	
15	5.10	A.5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen		Regels voor het aanvaardbaar gebruik van en procedures voor het omgaan met informatie en andere gerelateerde bedrijfsmiddelen moeten worden vastgesteld, gedocumenteerd en geïmplementeerd.	Ja			x	x	Ja	Nee	
16	5.11	A.5.11	Retourneren van bedrijfsmiddelen		Personeel en andere belanghebbenden, al naargelang de situatie, behoren alle bedrijfsmiddelen van de organisatie die zij in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst te retourneren. Zorgspecifieke beheersmaatregel (aanvullend) Er moet beleid zijn dat vereist dat personen schriftelijk bevestigen dat alle bedrijfsmiddelen in hun bezit in alle formaten op veilige wijze zijn getrouweerd of verwijst indien van toepassing	Ja			x	x	Ja	Nee	
17	5.12	A.5.12	Classificeren van informatie		Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante belanghebbenden. Zorgspecifieke beheersmaatregel (aanvullend) Persoonlijke gezondheidsinformatie behoort uniform als vertrouwelijk te worden geclassificeerd.	Ja			x	x	Ja	Nee	
18	5.13	A.5.13	Labelen van informatie		Om informatie te labelen moet een passende reeks procedures worden vastgesteld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	Ja			x	x	Ja	Nee	
19	5.14	A.5.14	Overdragen van informatie		Er moeten regels, procedures of overeenkomsten voor informatieoverdracht zijn vastgesteld voor alle soorten van overdracht binnen de organisatie en tussen de organisatie en andere partijen. Zorgspecifieke beheersmaatregel (aanvullend) Vóórdat enige overdracht plaatsvindt, moeten er regels, procedures en overeenkomsten zijn ingesteld.	Ja			x	x	Ja	Nee	
20	5.15	A.5.15	Toegangsbeveiliging		Er moeten regels op basis van bedrijfs- en informatiebeveiligingsrisico's worden vastgesteld en geïmplementeerd om de fysieke en logische toegang tot informatie en andere gerelateerde bedrijfsmiddelen te beheersen. Zorgspecifieke beheersmaatregel (aanvullend) Er moet beleid voor op rollen gebaseerde toegangsbeveiliging gelden voor de toegang tot persoonlijke gezondheidsinformatie.	Ja			x	x	Ja	Nee	
21	5.16	A.5.16	Identiteitsbeheer		De volledige levenscyclus van identiteiten moet worden beheerd. Zorgspecifieke beheersmaatregel (aanvullend) Gebruikers die toegang willen hebben tot persoonlijke gezondheidsinformatie en andere vertrouwelijke informatie, moeten formeel zijn geregistreerd.	Ja			x	x	Ja	Nee	
22	5.17	A.5.17	Beheeren van authenticatie informatie		De toewijzing en het beheer van authenticatie informatie moet worden beheerd door middel van een beheerproces waarvan het informeren van het personeel over de juiste manier van omgaan met authenticatie informatie deel uitmaakt.	Ja			x	x	Ja	Nee	
23	5.18	A.5.18	Toegangsrechten		Toegangsrechten met betrekking tot 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			x	x	Ja	Nee	
24	5.19	A.5.19	Informatiebeveiliging in leveranciersrelaties		Er moeten processen en procedures te worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met het gebruik van producten of diensten van de leverancier te beheersen. Zorgspecifieke beheersmaatregel (aanvullend) De risico's in verband met toegang door externe partijen tot systemen of de gegevens die zij bezitten moeten worden beoordeeld en beheersmaatregelen passend bij het geïdentificeerde risico moeten worden geïmplementeerd	Ja			x	x	Ja	Nee	
25	5.20	A.5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten		Relevante informatiebeveiligingsrisico's moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie te worden overeengekomen.	Ja			x	x	Ja	Nee	
26	5.21	A.5.21	Beheeren van informatiebeveiliging in de ICT keten		Er moeten processen en procedures worden vastgesteld en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toevoerketens van ICT producten en diensten te beheersen.	Ja			x	x	Ja	Nee	
27	5.22	A.5.22	Monitoren, beoordelen en het beheeren van wijzigingen van leveranciersdiensten		De organisatie moet de informatiebeveiligingspraktijken en de leveranciersdiensten regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan te beheersen.	Ja			x	x	Ja	Nee	
28	5.23	A.5.23	Informatiebeveiliging voor het gebruik van clouddiensten		Processen voor het aanschaffen, gebruiken, beheeren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingsrisico's van de organisatie worden opgesteld.	Ja			x	x	Ja	Nee	
29	5.24	A.5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten		De organisatie moet plannen opstellen voor, en zich voor te bereiden op, het beheeren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja			x	x	Ja	Nee	
30	5.25	A.5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen		De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en te besluiten of ze moeten worden geclassificeerd als informatiebeveiligingsincidenten.	Ja			x	x	Ja	Deels - gebruik van tooling	
31	5.26	A.5.26	Reageren op informatiebeveiligingsincidenten		Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja			x	x	Ja	Nee	
32	5.27	A.5.27	Leren van informatiebeveiligingsincidenten		Kennis die is opgebouwd met informatiebeveiligingsincidenten moeten worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja			x	x	Ja	Nee	
33	5.28	A.5.28	Verzamelen van bewijsmateriaal		De organisatie moet procedures opstellen en implementeren voor het identificeren, verzamelen, veiligstellen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	Ja			x	x	Ja	Nee	
34	5.29	A.5.29	Informatiebeveiliging tijdens een verstoring		De organisatie moet plannen maken voor het op het passend niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja			x	x	Ja	Nee	
35	5.30	A.5.30	ICT gereedheid voor bedrijfscontinuïteit		De ICT gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsbeoordelingen en ICT continuïteitsplannen.	Ja			x	x	Ja	Nee	

Organisatorische beheersmaatregelen

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Verklaring van Toepasselijkheid - Deltacom												
2	Versie: 3.0		Versiedatum: 01-04-2026										
3	NEN 7510-1:2024 NL					Van toepassing?	Reden van aanwezigheid			Volledig geïmplementeerd?	Uitbested	Reden van uitsluiting	
4	Hoofdstukken	ISO 27001:2023 controls	NEN 7510:2024	Titel beheersmaatregel	Beheersmaatregel		WR	CO	BR	RA			
5		5.31	A.5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Eisen van 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 vastgesteld, gedocumenteerd en actueel gehouden.	Ja	x		x	x	Ja	Nee	
36		5.32	A.5.32	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele eigendomsrechten te beschermen.	Ja	x		x	x	Ja	Nee	
37		5.33	A.5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	x			x	Ja	Nee	
38		5.34	A.5.34	Privacy en bescherming van persoonsgegevens	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 ervan te voldoen.	Ja	x			x	Ja	Nee	
39		5.35	A.5.35	Onafhankelijke beoordeling van informatiebeveiliging	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 gepaste tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja	x			x	Ja	Nee	
40		5.36	A.5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderzwaarspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	x			x	Ja	Nee	
41		5.37	A.5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja		x	x	x	Ja	Nee	
42		A.5.38	HLT - Analyse en specificatie van informatiebeveiligingsrisico's	Zorgspecifieke beheersmaatregelen De informatiebeveiligingsgerelateerde eisen moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen aan bestaande informatiesystemen.	Nee						Nee	Nee	Deltacom heeft zelf geen informatiesystemen waarin zorgspecifieke informatie wordt opgeslagen.
43		A.5.39	HLT - Zorgontvangers op unieke wijze identificeren	Zorgspecifieke beheersmaatregelen Beleid en processen moeten waarborgen dat elke zorgontvanger op unieke wijze binnen het systeem kan worden geïdentificeerd en moeten in staat zijn dubbele of meervoudige registraties samen te voegen als er dubbele of meervoudige registraties zijn voor een en dezelfde ontvanger.	Nee						Nee	Nee	Deltacom heeft zelf geen informatiesystemen waarin zorgspecifieke informatie wordt opgeslagen.
44		A.5.40	HLT - Validatie van gekende / geprinte gegevens	Zorgspecifieke beheersmaatregelen Als gegevens worden gekend en/of geprint door gezondheidsinformatiesystemen moeten deze gegevens ook informatie omvatten waarmee de zorgontvanger waarop de gegevens betrekking heeft wordt geïdentificeerd.	Nee						Nee	Nee	Deltacom heeft zelf geen informatiesystemen waarin zorgspecifieke informatie wordt opgeslagen.
45		A.5.41	HLT - Openbaar beschikbare gezondheidsinformatie	Zorgspecifieke beheersmaatregelen Openbaar beschikbare zorginformatie moet worden beschermd, bewaard en beheerd gedurende de volledige levenscyclus.	Nee						Nee	Nee	Deltacom heeft zelf geen informatiesystemen waarin zorgspecifieke informatie wordt opgeslagen.
46		A.5.42	HLT - Communicatie in noodsituaties	Zorgspecifieke beheersmaatregelen Noodcommunicatiekanalen binnen een zorgorganisatie die in werking treden wanneer er een storing is in de continuïteit van de ICT van de organisatie moet worden gestand, geïmplementeerd, onderhouden en beproefd.	Nee						Nee	Nee	Deltacom heeft zelf geen informatiesystemen waarin zorgspecifieke informatie wordt opgeslagen.
47		A.5.43	HLT - Incidenten extern melden	Zorgspecifieke beheersmaatregelen Informatiebeveiligingsincidenten moeten volgens juridische of contractuele verplichtingen of verplichtingen uit hoofde van wet- en regelgeving worden gemeld.	Ja	x	x	x	x	x	Ja	Nee	
48	Mensgerichte beheersmaatregelen	6.1	A.6.1	Screening	De achtergrond van alle kandidaten die in aanmerking komen voor posities binnen de organisatie moeten worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op grote tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving, voorschriften en ethische overwegingen, en deze controle moet in verhouding staan tot de bedrijfsrisico's, de classificatie van informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja			x	x	Ja	Nee	
50		6.2	A.6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging. Zorgspecifieke beheersmaatregel (aanvullend) In functiebeschrijvingen moeten de bevestigingspunten en verantwoordelijkheden worden vermeld die van toepassing zijn op het verwerken van persoonlijke gezondheidsinformatie.	Ja	x		x	x	Ja	Nee	
54		6.3	A.6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding, training en bijhouding in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.	Ja			x	x	Ja	Nee	
57		6.4	A.6.4	Disciplinaire procedure	Er moet een formele en gecommuniceerde disciplinaire procedure zijn om actie te ondernemen tegen personeel en andere belanghebbenden die zich schuldig hebben gemaakt aan een schending van het informatiebeveiligingsbeleid.	Ja			x	x	Ja	Nee	
60		6.5	A.6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband moeten worden gedefinieerd, gehandhaafd en gecommuniceerd aan relevant personeel en andere belanghebbenden.	Ja	x		x	x	Ja	Nee	
61		6.6	A.6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	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 onderkend door personeel en andere relevante belanghebbenden. Zorgspecifieke beheersmaatregel (aanvullend) Alle personeel dat toegang is tot toegang tot persoonlijke gezondheidsinformatie moet er formeel toe worden verplicht die informatie vertrouwelijk te behandelen.	Ja		x	x	x	Ja	Nee	
62		6.7	A.6.7	Werken op afstand	Wanneer personeel op afstand werkt, moeten er beveiligingsmaatregelen worden geïmplementeerd om informatie te beschermen die buiten het gebouw en/of terrein van de organisatie wordt ingezet, verwerkt of opgeslagen.	Ja			x	x	Ja	Nee	
64		6.8	A.6.8	Melden van informatiebeveiligingsgebeurtenissen	De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja		x	x	x	Ja	Nee	
65		A.6.9	HLT - Managementtraining	Zorgspecifieke beheersmaatregel Het management van de organisatie moet passende training krijgen, naarmate relevant is voor hun rollen en verantwoordelijkheden met betrekking tot informatiebeveiliging en hoe het wordt beheerd.	Ja	x			x	x	Ja	Nee	
66	Fysieke beheersmaatregelen	7.1	A.7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja			x	x	Ja	Nee	
69		7.2	A.7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangscodes en toegangsregels.	Ja			x	x	Ja	Ja	
71		7.3	A.7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja			x	x	Ja	Ja	
72		7.4	A.7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja			x	x	Ja	Ja	
73		7.5	A.7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere natuurlijke of onnatuurlijke fysieke dreigingen van de infrastructuur, worden ontworpen en geïmplementeerd.	Ja			x	x	Ja	Nee	
74		7.6	A.7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja			x	x	Ja	Nee	
75		7.7	A.7.7	Clear desk en Clear screen	Er moeten clear desk regels voor papieren documenten en verwijderbare opslagmedia en clear screen regels voor informatieverwerkende faciliteiten worden gedefinieerd en op passende wijze ten uitvoer worden gebracht.	Ja			x	x	Ja	Nee	
76		7.8	A.7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja			x	x	Ja	Nee	
77		7.9	A.7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja			x	x	Ja	Deels - gedeeltelijke uitbesteding aan datacenter	
78		7.10	A.7.10	Opslagmedia	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringsvoorschriften van de organisatie. Zorgspecifieke beheersmaatregel (aanvullend) Alle persoonlijke gezondheidsinformatie die op verwijderbare media wordt opgeslagen moet worden versleuteld.	Ja			x	x	Ja	Nee	
80		7.11	A.7.11	Nutvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutvoorzieningen.	Ja			x	x	Ja	Deels - Gedeelte verantwoordelijkheid met verhuurder	
84													

	A	B	C	D	E	F	G	H	I	J	K	L	M
1	Verklaring van Toepasselijkheid - Deltacom												
2	Versie: 3.0			Versiedatum: 01-04-2026									
3	NEN 7510-1:2024 NL					Van toepassing?	Reden van aanwezigheid				Volledig geïmplementeerd?	Uitbested	Reden van uitsluiting
4	Hoofdstukken	ISO 27001:2023 controls	NEN 7410:2024	Titel beheersmaatregel	Beheersmaatregel		WR	CO	BR	RA			
5		7.12	A.7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of de informatiediensten onderscheiden, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja			x	x	Ja	Nee	
85		7.13	A.7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze te worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja			x	x	Ja	Nee	
86		7.14	A.7.14	Veilig verwijderen of hergebruiken van apparatuur	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			x	x	Ja	Nee	
87													
89		8.1	A.8.1	User endpoint devices	Informatie die is opgeslagen op, wordt vervoerd door of toegankelijk is via user endpoint devices moet worden beschermd.	Ja			x	x	Ja	Nee	
90		8.2	A.8.2	Speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten moeten worden beperkt en beheerd.	Ja			x	x	Ja	Nee	
91		8.3	A.8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moeten worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja			x	x	Ja	Nee	
92		8.4	A.8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Nee					Nee	Nee	Deltacom doet niet aan software en/of systeemontwikkeling, er is geen broncode.
95		8.5	A.8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatie technologieën en procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke of aanvullende beleid inzake toegangsbeveiliging. Zorgspecifieke beheersmaatregel (aanvullend) Er moet ten minste biometrische authenticatie worden gebruikt voor systemen die persoonlijke gezondheidsinformatie verwerken.	Ja			x	x	Ja	Nee	deels - gebruik van passwordmanager
96		8.6	A.8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en afgestemd overeenkomstig de huidige en verwachte capaciteitseisen.	Ja			x	x	Ja	Deels	
97		8.7	A.8.7	Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Ja			x	x	Ja	Nee	
98		8.8	A.8.8	Beheer van technische kwetsbaarheden	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 behoren passende maatregelen te worden getroffen.	Ja	x		x	x	Ja	Deels - gebruik van tooling	
100		8.9	A.8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja			x	x	Ja	Nee	
101		8.10	A.8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moeten worden gewist als deze niet langer nodig is.	Ja			x	x	Ja	Nee	
102		8.11	A.8.11	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfsleiden van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja			x	x	Ja	Nee	
103		8.12	A.8.12	Voorkomen van gegevenslekken (data leakage prevention)	Maatregelen om gegevenslekken te voorkomen moeten worden toegepast in systemen, netwerken en andere apparaten waarop of waarmee gevoelige informatie wordt vervoerd, opgeslagen of getransporteerd.	Ja			x	x	Ja	Nee	
104		8.13	A.8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig te worden geëvalueerd overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups. Zorgspecifieke beheersmaatregel (aanvullend) Back-ups van persoonlijke gezondheidsinformatie moeten worden versleuteld.	Ja			x	x	Ja	Deels - we behouden de back-uplossing volledig, maar maken gebruik van een cloud oplossing	
105		8.14	A.8.14	Redundantie van informatieverwerkende systemen	Informatieverwerkende faciliteiten moeten met voldoende redundante worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja			x	x	Ja	Deels - datacenter	
107		8.15	A.8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja			x	x	Ja	Deels - gebruik van tooling	
108		8.16	A.8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er behoren passende maatregelen te worden genomen om potentiële informatiebeveiligingsincidenten te enablen.	Ja			x	x	Ja	Deels - gebruik van tooling	
110		8.17	A.8.17	Klok synchronisatie	De klokken van informatieoverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdsbronnen.	Ja			x	x	Ja	Nee	
111		8.18	A.8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te ontzeilen, moeten worden beperkt en nauwkeurig te worden gecontroleerd.	Ja			x	x	Ja	Nee	
113		8.19	A.8.19	Installeren van software op operationele systemen	Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja			x	x	Ja	Nee	
114		8.20	A.8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkkomponenten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja			x	x	Ja	Nee	
115		8.21	A.8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveau's en dienstverleningsprocedures voor alle netwerkdiensten moeten worden gedefinieerd, geïmplementeerd en gemonitord.	Ja			x	x	Ja	Nee	
116		8.22	A.8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers- en informatiesystemen moeten in de netwerken van de organisatie te worden geïmplementeerd.	Ja			x	x	Ja	Nee	
117		8.23	A.8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja			x	x	Ja	Nee	
118		8.24	A.8.24	Gebruik van cryptografie	Regels voor het doelbepaalde gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja			x	x	Ja	Nee	
119		8.25	A.8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja			x	x	Ja	Nee	
120		8.26	A.8.26	Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden gedefinieerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja			x	x	Ja	Nee	
121		8.27	A.8.27	Veilige systeemarchitectuur en technische uitgangspunten	Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja			x	x	Ja	Nee	
123		8.28	A.8.28	Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op software ontwikkeling.	Nee					Nee	Nee	Deltacom doet niet aan software en/of systeemontwikkeling, er is geen broncode.
124		8.29	A.8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja			x	x	Ja	Nee	
125		8.30	A.8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Ja			x	x	Ja	Deels	
127		8.31	A.8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja			x	x	Ja	Nee	
128		8.32	A.8.32	Wijzigingsbeheer	Wijzigingen in informatieverwerkingsfaciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja			x	x	Ja	Nee	
130		8.33	A.8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Nee					Nee	Nee	Deltacom doet niet aan software en/of systeemontwikkeling, er zijn geen testgegevens.
132		8.34	A.8.34	Bescherming van informatiesystemen tijdens audits	Audit en andere borginsactiviteiten waarbij operationele systemen worden beoordeeld moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja			x	x	Ja	Nee	
133			A.8.35	HLT - Zero trust-beginselen	Zorgspecifieke beheersmaatregelen Aan een netwerksegment toegevoegde groepen informatiediensten, gebruikers en informatiesystemen moeten zo klein mogelijk worden gehouden en mogen slechts toegang tot een ander netwerksegment hebben nadat beide betrokken segmenten elkaar hebben geauthenticeerd.	Ja			x	x	Ja	Nee	
134													
135													
136	Legenda (voor geselecteerde maatregelen en redenen voor selectie)												
137	WR: Wet- en regelgeving, CO: contractuele overeenkomst, BR/BP: business requirements / adopted best practices, RRA: resultaat risico assessment												

7. technologische beheersmaatregelen