

Verklaring van Toepasselijkheid

September 2026



Actieve Verklaring van Toepasselijkheid

Voor u ligt de definitieve Verklaring van Toepasselijkheid (VVT) van Kersten Hulpmiddelen Specialist B.V., waarin de borging is beschreven van het informatiebeveiligingsbeleid conform ISO 27001:2022 en NEN 7510:2024. De VVT beschrijft het normenkader waar de organisatie zich aan committeert en beschrijft eventuele redenen van uitsluiting.

Scope

De VVT strekt zich uit over de onderneming Kersten Hulpmiddelen Specialist B.V. en richt zich op het beveiligen van informatie binnen de volledige Kersten Hulpmiddelen groep, te weten: Kersten Hulpmiddelspecialist B.V., HM Medical B.V., RTD Arnhem B.V. en BSO B.V.

Het betreft de totale dienstverlening: inkopen, indiceren, adviseren, verstrekken (verhuur en verkoop), installeren, beheer, onderhoud en service, inclusief repareren en reinigen of desinfecteren van revalidatiehulpmiddelen.

Deze VVT is bestemd voor alle medewerkers van Kersten Hulpmiddelen Specialist B.V., RTD Arnhem B.V. en BSO B.V. en al haar stakeholders. Het gehanteerde Information Security Management System (ISMS) is van toepassing op alle bedrijfsprocessen vallend binnen de scope.

Verantwoordelijkheden

De reikwijdte van de VVT is vastgesteld in samenspraak met het directieteam. Met de ondertekening neemt de directie de verantwoordelijkheid om de maatregelen te treffen die nodig zijn om het ISMS doeltreffend en efficiënt te houden. De organisatie treft jaarlijks de nodige maatregelen en acties met de benodigde resources.

Ondertekening namens de directie van Kersten Hulpmiddelen Specialist B.V.

Naam	Bas Alberts	
Functie	CEO	
Plaats	Houten	
Datum	16-09-2026	

Met de ondertekening activeert, borgt en verklaart Kersten Hulpmiddelen Specialist B.V. het normenkader als volgt:

Beheersmaatregel niet van toepassing

#	Beheersmaatregel	Toelichting
8.4	Toegangsbeveiliging op broncode	Binnen de organisatie wordt er geen software ontwikkeld. Deze beheersmaatregel is dan ook niet toegepast.
8.25	Beveiligen tijdens de ontwikkelcyclus	Binnen de organisatie wordt er geen software ontwikkeld. Deze beheersmaatregel is dan ook niet toegepast.
8.28	Veilig coderen	Binnen de organisatie wordt er geen software ontwikkeld. Er wordt dan ook geen gebruikgemaakt van programmeercode.
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Binnen de organisatie wordt er geen software ontwikkeld en is beveiliging tijdens ontwikkeling en acceptatie uitgesloten.

Beheersmaatregel van toepassing

Op basis van een risico-inventarisatie en -analyse is vastgesteld dat de normen in de onderstaande tabel van toepassing zijn voor Kersten Hulpmiddelen Specialist B.V. De tabel beschrijft naast de beheersmaatregelen ook de context die op de eis van toepassing is binnen Kersten Hulpmiddelen Specialist B.V. als het gaat om:

- Risicoanalyse
- Beleid
- Wet- en regelgeving
- Uitbestede diensten of activiteiten
- Contractueel

ISO/IEC 27001:2022 en NEN 7510:2024 Verklaring van Toepasselijkheid

Onderstaande tabel bevat alle 93 beheersmaatregelen uit bijlage A van ISO/IEC 27001:2022. Hiervan zijn er 89 van toepassing en geïmplementeerd; 4 beheersmaatregelen zijn niet van toepassing. Een X in de kolommen Wet- en regelgeving, Contractueel, Beleid, Risicoanalyse en Uitbesteed geeft aan op welke grond de beheersmaatregel van toepassing is.

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
A5 Organisatorische beheersmaatregelen (37 beheersmaatregelen)										
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 en als zich significante wijzigingen voordoen, worden beoordeeld.	Ja	Geïmplementeerd			X	X		
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja	Geïmplementeerd			X	X		
5.3	Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja	Geïmplementeerd			X	X		
5.4	Managementverantwoordelijkheden	Het management moet van al het personeel eisen dat ze informatiebeveiliging toepassen overeenkomstig het vastgestelde informatiebeveiligingsbeleid, de onderwerp specifieke beleidsregels en procedures van de organisatie	Ja	Geïmplementeerd		X	X	X		
5.5	Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden	Ja	Geïmplementeerd		X		X		
5.6	Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen onderhouden.	Ja	Geïmplementeerd			X	X		
5.7	Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	Ja	Geïmplementeerd			X	X	X	

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
5.8	Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement	Ja	Geïmplementeerd			X	X		
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden.	Ja	Geïmplementeerd		X	X	X		
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 geïdentificeerd, gedocumenteerd, en geïmplementeerd.	Ja	Geïmplementeerd	X	X	X	X		
5.11	Retourneren van bedrijfsmiddelen	Personeel en andere belanghebbenden, al naar gelang de situatie, moeten alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst retourneren.	Ja	Geïmplementeerd		X	X	X		
5.12	Classificeren van informatie	Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit en beschikbaarheid en relevante eisen van belanghebbenden.	Ja	Geïmplementeerd			X	X		
5.13	Labelen van informatie	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	Geïmplementeerd			X	X		
5.14	Overdragen van informatie	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	Geïmplementeerd		X	X	X		
5.15	Toegangsbeveiliging	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	Geïmplementeerd			X	X		
5.16	Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja	Geïmplementeerd			X	X		

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
5.17	Authenticatie-informatie	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	Geïmplementeerd			X	X		
5.18	Toegangsrechten	Toegangsrechten voor informatie en andere gerelateerde bedrijfsmiddelen moeten worden verstrekt, beoordeeld, aangepast en verwijder overeenkomstig het onderwerp specifieke beleid en de regels inzake toegangsbeveiliging van de organisatie	Ja	Geïmplementeerd			X	X		
5.19	Informatiebeveiliging in leveranciersrelaties	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	Geïmplementeerd		X	X	X		
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen	Ja	Geïmplementeerd		X	X	X		
5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Er moeten processen procedures worden bepaald en geïmplementeerd om de informatiebeveiligingsrisico's in verband met de toeleveringsketen van ICT-producten en- diensten te beheersen	Ja	Geïmplementeerd		X	X	X		
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	Ja	Geïmplementeerd			X	X		
5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja	Geïmplementeerd			X	X		
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	De organisatie moet plannen opstellen voor, en zich voorbereiden op, het beheren van informatiebeveiligingsincidenten door processen, rollen en verantwoordelijkheden voor het beheer van informatie- beveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja	Geïmplementeerd			X	X		

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
5.25	Beeoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Geïmplementeerd	X		X	X		
5.26	Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Geïmplementeerd	X		X	X		
5.27	Leren van informatiebeveiligingsincidenten	Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Geïmplementeerd	X		X	X		
5.28	Verzamelen van bewijsmateriaal	De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen	Ja	Geïmplementeerd	X	X	X	X		
5.29	Informatiebeveiliging tijdens een verstoring	De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Geïmplementeerd		X	X	X		
5.30	ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	Ja	Geïmplementeerd			X	X		
5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	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	Geïmplementeerd	X	X	X	X		
5.32	Intellectuele eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	Ja	Geïmplementeerd	X	X	X	X		
5.33	Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Geïmplementeerd	X	X	X	X		
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 eraan voldoen.	Ja	Geïmplementeerd	X	X	X	X		

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
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 geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.	Ja	Geïmplementeerd			X	X		
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerp specifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	Geïmplementeerd			X	X		
5.37	Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatie verwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja	Geïmplementeerd				X		
A6 Mensgerichte beheersmaatregelen (8 beheersmaatregelen)										
6.1	Screening	De achtergrond van alle kandidaten voor een dienstverband moet worden gecontroleerd voordat ze bij de organisatie in dienst treden en daarna op gezette tijden worden herhaald. Hierbij moet rekening worden gehouden met de toepasselijke wet- en regelgeving en ethische verwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Ja	Geïmplementeerd	X			X		
6.2	Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja	Geïmplementeerd	X	X		X		
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerp specifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.	Ja	Geïmplementeerd			X	X		
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	Geïmplementeerd			X	X		

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
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	Ja	Geïmplementeerd			X	X		
6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Vertrouwelijkheids- of geheimhoudingsovereenkomsten die de behoeften van de organisatie inzake de bescherming van informatie weerspiegelen, moeten worden geïdentificeerd, gedocumenteerd, regelmatig worden beoordeeld en ondertekend door personeel en andere relevante belanghebbenden.	Ja	Geïmplementeerd		X	X	X		
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 ingezien, verwerkt of opgeslagen.	Ja	Geïmplementeerd			X	X		
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	Geïmplementeerd	X	X	X	X	X	
A7 Fysieke beheersmaatregelen (14 beheersmaatregelen)										
7.1	Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja	Geïmplementeerd			X	X		
7.2	Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	Ja	Geïmplementeerd		X	X	X		
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja	Geïmplementeerd			X	X		
7.4	Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja	Geïmplementeerd			X	X		
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Er moet bescherming tegen fysieke en omgevingsdreigingen, zoals natuurrampen en andere opzettelijke of onopzettelijke fysieke dreigingen voor de infrastructuur, worden ontworpen en geïmplementeerd.	Ja	Geïmplementeerd			X	X		

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
7.6	Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja	Geïmplementeerd			X	X		
7.7	Clear desk 'en 'Clear screen'	Er moeten 'clear desk'-regels voor papieren documenten en verwijderbare opslagmedia en 'clear screen'-regels voor informatie verwerkende faciliteiten worden gedefinieerd en op passende wijze worden afgedwongen.	Ja	Geïmplementeerd			X	X		
7.8	Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja	Geïmplementeerd			X	X		
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja	Geïmplementeerd			X	X		
7.10	Opslagmedia	Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie.	Ja	Geïmplementeerd			X	X	X	
7.11	Nutsvoorzieningen	Informatie verwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Geïmplementeerd					X	
7.12	Beveiligen van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Geïmplementeerd					X	
7.13	Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.	Ja	Geïmplementeerd				X	X	
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	Geïmplementeerd				X	X	

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
A8 Technologische beheersmaatregelen (34 beheersmaatregelen)										
8.1	User endpoint devices	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja	Geïmplementeerd				X	X	
8.2	Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja	Geïmplementeerd				X	X	
8.3	Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerp specifieke beleid inzake toegangsbeveiliging.	Ja	Geïmplementeerd				X	X	
8.4	Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Nee	Niet van toepassing						Binnen de organisatie wordt er geen software ontwikkeld. Deze beheersmaatregel is dan ook niet toegepast.
8.5	Beveiligde authenticatie	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerp specifieke beleid inzake toegangsbeveiliging.	Ja	Geïmplementeerd				X	X	
8.6	Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Geïmplementeerd				X	X	
8.7	Bescherming tegen Malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Ja	Geïmplementeerd				X	X	
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 moeten passende maatregelen worden getroffen.	Ja	Geïmplementeerd		X	X	X	X	

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
8.9	Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Geïmplementeerd			X		X	
8.10	Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	Ja	Geïmplementeerd	X	X	X	X	X	
8.11	Maskeren van gegevens	Gegevens moeten worden gemaskeerd overeenkomstig het onderwerp specifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerp specifieke beleidsregels, en bedrijfseisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja	Geïmplementeerd	X		X			
8.12	Voorkomen van gegevenslekken	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	Geïmplementeerd	X	X	X	X	X	
8.13	Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerp specifieke beleid inzake back-ups.	Ja	Geïmplementeerd		X	X	X	X	
8.14	Redundantie van informatie verwerkende faciliteiten	Informatie verwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Geïmplementeerd			X	X		
8.15	Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Geïmplementeerd		X	X	X	X	
8.16	Monitoren van activiteiten	Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Geïmplementeerd			X	X		

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
8.17	Kloksynchronisatie	De klokken van informatie verwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	Ja	Geïmplementeerd			X	X		
8.18	Gebruik van speciale systeemhulpmiddelen	Het gebruik van systeemhulpmiddelen die in staat kunnen zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen, moet worden beperkt en nauwkeurig worden gecontroleerd.	Ja	Geïmplementeerd		X		X		
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	Geïmplementeerd			X	X		
8.20	Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Geïmplementeerd			X	X		
8.21	Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Geïmplementeerd			X	X		
8.22	Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja	Geïmplementeerd			X	X		
8.23	Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja	Geïmplementeerd			X	X		
8.24	Gebruik van cryptografie	Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja	Geïmplementeerd		X	X	X		
8.25	Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Nee	Niet van toepassing						Binnen de organisatie wordt er geen software ontwikkeld. Deze beheersmaatregel is dan ook niet toegepast.

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
8.26	Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Geïmplementeerd		X	X	X		
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	Geïmplementeerd			X	X		
8.28	Veilig coderen	Principes voor veilig coderen moeten worden toegepast op softwareontwikkeling.	Nee	Niet van toepassing						Binnen de organisatie wordt er geen software ontwikkeld. Er wordt dan ook geen gebruikgemaakt van programmeercode.
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.	Nee	Niet van toepassing						Binnen de organisatie wordt er geen software ontwikkeld en is beveiliging tijdens ontwikkeling en acceptatie uitgesloten.
8.30	Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Ja	Geïmplementeerd			X	X		
8.31	Scheiding van ontwikkel- test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja	Geïmplementeerd		X	X	X	X	
8.32	Wijzigingsbeheer	Wijzigingen in informatie verwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja	Geïmplementeerd		X	X	X	X	
8.33	Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja	Geïmplementeerd			X	X		

#	Titel beheersmaatregel	Beheersmaatregel	Toepasselijk	Status	Wet- en regelgeving	Contractueel	Beleid	Risicoanalyse	Uitbesteed	Rechtvaardiging voor uitsluiting
8.34	Bescherming van informatiesystemen tijdens audits	Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Geïmplementeerd		X	X	X	X	