

VVT NEN7510:2024 Organisatie: Therapieland B.V. Naam: K. Klijn. Datum: 9 september 2026 versie 1.0 [1]								
5	Organisatorische Beheersmaatregel:		Van toepassing	Geïmplementeerd?	Uitbesteed?	Verantwoordelijkheid toepasseljkheid: IRA	Verantwoording toepasseljkheid: wet/contract en regelgeving	Reden van uitsluiting
5.1	Beleidsregels voor informatiebeveiliging	Beheersmaatregel 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. 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	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.2	Rollen en verantwoordelijkheden bij informatiebeveiliging	Beheersmaatregel Rollen en 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	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.3	Functiescheiding	Beheersmaatregel: Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.4	Managementverantwoordelijkheden	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.5	Contact met overheidsinstanties	Beheersmaatregel: De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

5.6	Contact met speciale belangengroepen	Beheersmaatregel: De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.7	Informatie en analyses over dreigingen	Beheersmaatregel: Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.8	Informatiebeveiliging in projectmanagement	Beheersmaatregel: Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.9	Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen	Beheersmaatregel: Er moet een inventarislijst van informatie en andere gerelateerde bedrijfsmiddelen, met inbegrip van de eigenaren, worden opgesteld en onderhouden. Zorgspecifieke beheersmaatregel: Alle informatiestromen (zowel binnen als tussen organisaties) en de interfaces daarvan (waaronder integratieplatforms) moeten worden opgenomen in de inventarisatie.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.10	Aanvaardbaar gebruik van informatie en andere gerelateerde bedrijfsmiddelen	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.11	Retourneren van bedrijfsmiddelen	Beheersmaatregel: 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. Zorgspecifieke beheersmaatregel: Er moet beleid 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.

5.12	Classificeren van informatie	<p>Beheersmaatregel: Informatie moet worden geclassificeerd volgens de informatiebeveiligingsbehoeften van de organisatie, op basis van de eisen voor vertrouwelijkheid, integriteit, beschikbaarheid en relevante eisen van belanghebbenden.</p> <p>Zorgspecifieke beheersmaatregel: Persoonlijke gezondheidsinformatie behoort uniform als vertrouwelijk te worden geclassificeerd.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.13	Labelen van informatie	<p>Beheersmaatregel: Om informatie te labelen moet een passende reeks procedures worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.14	Overdragen van informatie	<p>Beheersmaatregel: 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.</p> <p>Zorgspecifieke beheersmaatregel: Vóórdat enige overdracht plaatsvindt, moeten er regels, procedures en overeenkomsten zijn ingesteld.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.15	Toegangsbeveiliging	<p>Beheersmaatregel: 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.</p> <p>Zorgspecifieke beheersmaatregel: Er moet beleid voor op rollen gebaseerde toegangsbeveiliging gelden voor de toegang tot persoonlijke gezondheidsinformatie.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.16	Identiteitsbeheer	<p>Beheersmaatregel: De volledige levenscyclus van identiteiten moet worden beheerd.</p> <p>Zorgspecifieke beheersmaatregel: Gebruikers die toegang willen hebben tot persoonlijke gezondheidsinformatie en andere vertrouwelijke informatie, moeten formeel zijn geregistreerd.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

5.17	Authenticatie-informatie	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.18	Toegangsrechten	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.19	Informatiebeveiliging in leveranciersrelaties	Beheersmaatregel: 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. Zorgspecifieke beheersmaatregel: De risico's in verband met toegang door externe partijen tot systemen of de gegevens die zij bevatten moeten worden beoordeeld en beheersmaatregelen passend bij het geïdentificeerde risico moeten worden geïmplementeerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.20	Adresseren van informatiebeveiliging in leveranciersovereenkomsten	Beheersmaatregel: Relevante informatiebeveiligingseisen moeten worden vastgesteld en met elke leverancier op basis van het type leveranciersrelatie worden overeengekomen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.21	Beheren van informatiebeveiliging in de ICT-toeleveringsketen	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.22	Monitoren, beoordelen en het beheren van wijzigingen van leveranciersdiensten	Beheersmaatregel: De organisatie moet de informatiebeveiligingspraktijken en de dienstverlening van leveranciers regelmatig monitoren, beoordelen, evalueren en veranderingen daaraan beheren.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

5.23	Informatiebeveiliging voor het gebruik van clouddiensten	Beheersmaatregel: Processen voor het aanschaffen, gebruiken, beheren en beëindigen van clouddiensten moeten overeenkomstig de informatiebeveiligingseisen van de organisatie worden opgesteld.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.24	Plannen en voorbereiden van het beheer van informatiebeveiligingsincidenten	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.25	Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	Beheersmaatregel: De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.26	Reageren op informatiebeveiligingsincidenten	Beheersmaatregel: Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.27	Leren van informatiebeveiligingsincidenten	Beheersmaatregel: Kennis die is opgedaan met informatiebeveiligingsincidenten moet worden gebruikt om de beheersmaatregelen voor informatiebeveiliging te versterken en te verbeteren.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.28	Verzamelen van bewijsmateriaal	Beheersmaatregel: De organisatie moet procedures vaststellen en implementeren voor het identificeren, verzamelen, verkrijgen en bewaren van bewijs met betrekking tot informatiebeveiligingsgebeurtenissen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.29	Informatiebeveiliging tijdens een verstoring	Beheersmaatregel: De organisatie moet plannen maken voor het op het passende niveau waarborgen van de informatiebeveiliging tijdens een verstoring.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.30	ICT-gereedheid voor bedrijfscontinuïteit	Beheersmaatregel: De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

5.31	Wettelijke, statutaire, regelgevende en contractuele eisen	Beheersmaatregel: 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	Ja	Integrale risico analyse	N.V.T.	N.V.T.
5.32	Intellectuele-eigendomsrechten	Beheersmaatregel: De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.33	Beschermen van registraties	Beheersmaatregel: Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.34	Privacy en bescherming van persoonsgegevens	Beheersmaatregel: De organisatie behoort de eisen met betrekking tot het behoud van privacy en de bescherming van persoonsgegevens volgens de toepasselijke wet- en regelgeving en contractuele eisen te identificeren en eraan te voldoen.	Ja	Ja	Nee	Integrale risico analyse	Wet en regelgeving	N.V.T.
5.35	Onafhankelijke beoordeling van informatiebeveiliging	Beheersmaatregel: 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	Ja	Integrale risico analyse	N.V.T.	N.V.T.
5.36	Naleving van beleid, regels en normen voor informatiebeveiliging	Beheersmaatregel: De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.37	Gedocumenteerde bedieningsprocedures	Beheersmaatregel: Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.38	HLT – Analyse en specificatie van informatiebeveiligingseisen	Zorgspecifieke beheersmaatregel: De informatiebeveiligingsgerelateerde eisen moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen aan bestaande informatiesystemen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

5.39	HLT – Zorgontvangers op unieke wijze identificeren	Zorgspecifieke beheersmaatregel: Beleid en processen moeten waarborgen dat elke zorgontvanger op unieke wijze binnen het systeem kan worden geïdentificeerd en moeten in staat te zijn dubbele of meervoudige registraties samen te voegen als er dubbele of meervoudige registraties zijn voor een en dezelfde zorgontvanger.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.40	HLT – Validatie van getoonde/geprinte gegevens	Zorgspecifieke beheersmaatregel: Als er gegevens worden getoond en/of geprint door gezondheidsinformatiesystemen moeten deze gegevens ook informatie omvatten waarmee de zorgontvanger waarop de gegevens betrekking heeft wordt geïdentificeerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.41	HLT – Openbaar beschikbare gezondheidsinformatie	Zorgspecifieke beheersmaatregel: Openbaar beschikbare gezondheidsinformatie moet worden beschermd, bewaard en beheerd gedurende de volledige levenscyclus.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.42	HLT – Communicatie in noodsituaties	Zorgspecifieke beheersmaatregel: Noodcommunicatiekanalen binnen een zorgorganisatie die in werking treden wanneer er een storing is in de continuïteit van de ICT van de organisatie moet worden gepland, geïmplementeerd, onderhouden en beproefd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
5.43	HLT – Incidenten extern melden	Zorgspecifieke beheersmaatregel: Informatiebeveiligingsincidenten moeten volgens juridische of contractuele verplichtingen of verplichtingen uit hoofde van wet- en regelgeving worden gemeld.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
6	Mensgerichte Beheersmaatregel:		Van toepassing	Geïmplementeerd?	Uitbesteed?	Verantwoordelijkheid toepasselijheid: IRA	Verantwoording toepasselijheid: wet/contract en regelgeving	Reden van uitsluiting
6.1	Screening	Beheersmaatregel: 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 overwegingen, en deze controle moet in verhouding staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's.	Gedeeltelijk	Gedeeltelijk	Nee	Integrale risico analyse	Wet en regelgeving	Therapieland erkent geen risico's voor het niet herhalen van de screening. Daarom wordt het volgende deel van de beheersmaatregel als niet van toepassing bepaald: "en daarna op gezette tijden te worden herhaald."

6.2	Arbeidsovereenkomst	<p>Beheersmaatregel: In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.</p> <p>Zorgspecifieke beheersmaatregel: In functiebeschrijvingen moeten de beveiligingsrollen en verantwoordelijkheden worden vermeld die van toepassing zijn op het verwerken van persoonlijke gezondheidsinformatie.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
6.3	Bewustwording van, opleiding en training in informatiebeveiliging	<p>Beheersmaatregel: Personeel van de organisatie en relevante belanghebbenden moeten een passende bewustwording van, opleiding en training in informatiebeveiliging en regelmatige updates over het informatiebeveiligingsbeleid, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
6.4	Disciplinaire procedure	<p>Beheersmaatregel: 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.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
6.5	Verantwoordelijkheden na beëindiging of wijziging van het dienstverband	<p>Beheersmaatregel: 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.</p>	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

6.6	Vertrouwelijkheids- of geheimhoudingsovereenkomsten	Beheersmaatregel: 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. Zorgspecifieke beheersmaatregelen: Alle personeel dat bevoegd is tot toegang tot persoonlijke gezondheidsinformatie moet er formeel toe worden verplicht die informatie vertrouwelijk te behandelen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
6.7	Werken op afstand	Beheersmaatregel: 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	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
6.8	Melden van informatiebeveiligingsgebeurtenissen	Beheersmaatregel: De organisatie moet voorzien in een mechanisme waarmee personeel waargenomen of vermoede informatiebeveiligingsgebeurtenissen tijdig via passende kanalen kan melden.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
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	Ja	Nee	Integrale risico analyse	NIS2/Cbw	N.V.T.
7	Fysieke beheersmaatregelen		Van toepassing	Geïmplementeerd?	Uitbesteed?	Verantwoordelijkheid toepasseljkheid: IRA	Verantwoording toepasseljkheid: wet/contract en regelgeving	Reden van uitsluiting
7.1	Fysieke beveiligingszones	Beheersmaatregel: Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
7.2	Fysieke toegangsbeveiliging	Beheersmaatregel: Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
7.3	Beveiligen van kantoren, ruimten en faciliteiten	Beheersmaatregel: Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

7.4	Monitoren van de fysieke beveiliging	Beheersmaatregel: Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Nee	Nee	Nee	N.V.T.	N.V.T.	De kantoorruimte van Therapieland bevat geen bedrijfs- of cliëntgegevens en geen opslagmedia. Alle gegevens en systemen zijn onderbracht in het datacenter, dat via een uitbestede dienst door de leverancier wordt beheerd. Op basis hiervan wordt deze beheersmaatregel uitgesloten.
7.5	Beschermen tegen fysieke en omgevingsdreigingen	Beheersmaatregel: 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	Ja	Integrale risico analyse	N.V.T.	N.V.T.
7.6	Werken in beveiligde zones	Beheersmaatregel: Voor het werken in beveiligde zones behoren beveiligingsmaatregelen te worden ontwikkeld en geïmplementeerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
7.7	'Clear desk' en 'clear screen'	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
7.8	Plaatsen en beschermen van apparatuur	Beheersmaatregel: Apparatuur moet veilig worden geplaatst en beschermd.	Ja	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
7.9	Beveiligen van bedrijfsmiddelen buiten het terrein	Beheersmaatregel: Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
7.10	Opslagmedia	Beheersmaatregel: Opslagmedia moeten worden beheerd gedurende hun volledige levenscyclus van aanschaf, gebruik, transport en verwijdering overeenkomstig het classificatieschema en de hanteringseisen van de organisatie. Zorgspecifieke beheersmaatregel: Alle persoonlijke gezondheidsinformatie die op verwijderbare media wordt opgeslagen moet worden versleuteld.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
7.11	Nutsvoorziening en	Beheersmaatregel: Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.

7.12	Beveiligen van bekabeling	Beheersmaatregel: Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.	Ja	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
7.13	Onderhoud van apparatuur	Beheersmaatregel: Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen.	Ja	Ja	Ja	Integrale risico analyse	N.V.T.	N.V.T.
7.14	Veilig verwijderen of hergebruiken van apparatuur	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8	Technologische beheersmaatregelen		Van toepassing	Geïmplementeerd?	Uitbesteed?	Verantwoordelijkheid toepasselijkheid: IRA	Verantwoording toepasselijkheid: wet/contract en regelgeving	Reden van uitsluiting
8.1	'User endpoint devices'	Beheersmaatregel: Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.2	Speciale toegangsrechten	Beheersmaatregel: Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.3	Beperking toegang tot informatie	Beheersmaatregel: De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.4	Toegangsbeveiliging op broncode	Beheersmaatregel: Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

8.5	Beveiligde authenticatie	Beheersmaatregel: Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging. Zorgspecifieke beheersmaatregel: Er moet ten minste tweefactorauthenticatie worden gebruikt voor systemen die persoonlijke gezondheidsinformatie verwerken.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.6	Capaciteitsbeheer	Beheersmaatregel: Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.7	Bescherming tegen malware	Beheersmaatregel: Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebruikersbewustzijn.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.8	Beheer van technische kwetsbaarheden	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.9	Configuratiebeheer	Beheersmaatregel: Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.10	Wissen van informatie	Beheersmaatregel: In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

8.11	Maskeren van gegevens	Beheersmaatregel: Gegevens moeten worden gemaskeerd overeenkomstig het onderwerpspecifieke beleid inzake toegangsbeveiliging en andere gerelateerde onderwerpspecifieke beleidsregels, en bedrijfsfeisen van de organisatie, rekening houdend met de toepasselijke wetgeving.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.12	Voorkomen van gegevenslekken (data leakage prevention)	Beheersmaatregel: 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	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.13	Back-up van informatie	Beheersmaatregel: Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.14	Redundantie van informatieverwerkende faciliteiten	Beheersmaatregel: Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.15	Logging	Beheersmaatregel: Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.16	Monitoren van activiteiten	Beheersmaatregel: Netwerken, systemen en toepassingen moeten worden gemonitord op afwijkend gedrag en er moeten passende maatregelen worden getroffen om potentiële informatiebeveiligingsincidenten te evalueren.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.17	Kloksynchronisatie	Beheersmaatregel: De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

8.18	Gebruik van speciale systeemhulpmiddelen	Beheersmaatregel: 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	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.19	Installeren van software op operationele systemen	Beheersmaatregel: Er moeten procedures en maatregelen worden geïmplementeerd om het installeren van software op operationele systemen op veilige wijze te beheren.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.20	Beveiliging netwerkcomponenten	Beheersmaatregel: Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.21	Beveiliging van netwerkdiensten	Beheersmaatregel: Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.22	Netwerksegmentatie	Beheersmaatregel: Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.23	Toepassen van webfilters	Beheersmaatregel: De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Nee	Nee	Nee	N.V.T.	N.V.T.	Therapieland past geen webfiltering toe. Het risico van het bezoeken van schadelijke websites wordt op andere wijze afgedekt: medewerkers zijn geïnformeerd over de risico's via het personeelsreglement, en endpoint protection is ingericht als technische beheersmaatregel tegen malware en andere bedreigingen die via internetgebruik kunnen ontstaan.
8.24	Gebruik van cryptografie	Beheersmaatregel: Regels voor het doeltreffende gebruik van cryptografie, met inbegrip van het beheer van cryptografische sleutels, moeten worden gedefinieerd en geïmplementeerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.25	Beveiligen tijdens de ontwikkelcyclus	Beheersmaatregel: Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

8.26	Toepassingsbeveiligingseisen	Beheersmaatregel: Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.27	Veilige systeemarchitectuur en technische uitgangspunten	Beheersmaatregel: Uitgangspunten voor het ontwerpen van beveiligde systemen moeten worden vastgesteld, gedocumenteerd, onderhouden en toegepast voor alle activiteiten betreffende het ontwikkelen van informatiesystemen.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.28	Veilig coderen	Beheersmaatregel: Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.29	Testen van de beveiliging tijdens ontwikkeling en acceptatie	Beheersmaatregel: Processen voor het testen van de beveiliging moeten worden gedefinieerd en geïmplementeerd in de ontwikkelcyclus.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.30	Uitbestede systeemontwikkeling	Beheersmaatregel: De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Nee	Nee	N.V.T.	N.V.T.	Therapieland besteedt de ontwikkeling van software niet uit aan derden; softwareontwikkeling vindt intern plaats. Deze control is daarom niet van toepassing.
8.31	Scheiding van ontwikkel-, test- en productieomgevingen	Beheersmaatregel: Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.32	Wijzigingsbeheer	Beheersmaatregel: Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer. aan procedures voor wijzigingsbeheer.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.33	Testgegevens	Beheersmaatregel: Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
8.34	Bescherming van informatiesystemen tijdens audits	Beheersmaatregel: Audittests en andere auditactiviteiten waarbij operationele systemen worden beoordeeld, moeten worden gepland en overeengekomen tussen de tester en het verantwoordelijke management.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.

8.35	HLT – Zero trust-beginselen	Zorgspecifieke beheersmaatregel: Aan een netwerksegment toegewezen 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 geauthentiseerd.	Ja	Ja	Nee	Integrale risico analyse	N.V.T.	N.V.T.
------	-----------------------------	--	----	----	-----	--------------------------	--------	--------

[1] Verklaring van Toepasselijkheid