Titel	Maatregel	Van toepassing	Waarom niet van toepassing	Wetgeving	Contractueel	Interface	Uitbesteed	Volledig geimplementeerd
Annex 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		Ja	Ja	Nee	Nee	Ja
Annex 5.1 Beleidsregels voor informatiebeveiliging (zorgspecifiek)	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	Ja	Nee	Nee	Ja
Annex 5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging (zorgspecifiek)	Er moet ten minste één persoon verantwoordelijk zijn voor informatiebeveiliging.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 5.3 Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.5 Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 5.6 Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 5.7 Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 5.8 Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.9 Inventarisatie van informatie en andere gerelateerde bedrijfsmiddelen (zorgspecifiek)	Alle informatiestromen (zowel binnen als tussen organisaties) en de interfaces daarvan (waaronder integratieplatforms) moeten worden opgenomen in de inventarisatie.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.11 Retourneren van bedrijfsmiddelen	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		Nee	Ja	Nee	Nee	Ja
Annex 5.11 Retourneren van bedrijfsmiddelen (zorgspecifiek)	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		Nee	Ja	Nee	Nee	Ja
Annex 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 eisen van belanghebbenden.	Ja		Ja	Ja	Ja	Nee	Ja
Annex 5.12 Classificeren van informatie (zorgspecifiek)	Persoonlijke gezondheidsinformatie behoort uniform als vertrouwelijk te worden geclassificeerd.	Ja		Ja	Ja	Ja	Nee	Ja
Annex 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		Nee	Ja	Ja	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.14 Overdragen van informatie (zorgspecifiek)	Vóórdat enige overdracht plaatsvindt, moeten er regels, procedures en overeenkomsten zijn ingesteld.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Ja	Nee	Ja
Annex 5.15 Toegangsbeveiliging (zorgspecifiek)	Er moet beleid voor op rollen gebaseerde toegangsbeveiliging gelden voor de toegang tot persoonlijke gezondheidsinformatie.	Ja		Nee	Ja	Ja	Nee	Ja
Annex 5.16 Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Ja		Ja	Ja	Ja	Nee	Ja

Annex 5.16 Identiteitsbeheer (zorgspecifiek)	Gebruikers die toegang willen hebben tot persoonlijke gezondheidsinformatie en andere vertrouwelijke informatie, moeten formeel zijn geregistreerd.	Ja		Ja	Ja	Ja	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.18 Toegangsrechten	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		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.19 Informatiebeveiliging in leveranciersrelaties (zorgspecifiek)	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		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.21 Beheren van informatiebeveiliging in de ICT-keten	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		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 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		Ja	Ja	Nee	Nee	Ja
Annex 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 informatiebeveiligingsincidenten te definiëren, vast te stellen en te communiceren.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 5.26 Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 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		Ja	Ja	Nee	Nee	Ja
Annex 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		Ja	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.30 ICT-gereedheid voor bedrijfscontinuiteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Ja	Ja	Nee	Nee	Ja
Annex 5.32 Intellectuele-eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 5.33 Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Ja	Ja	Nee	Nee	Ja

Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 5.36 Naleving van beleid, regels en normen voor informatiebeveiliging	De naleving van het informatiebeveiligingsbeleid, het onderwerpspecifieke beleid, regels en de normen van de organisatie moet regelmatig worden beoordeeld.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 5.37 Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 5.38 HLT – Analyse en specificatie van informatiebeveiligingseisen (zorgspecifiek)	De informatiebeveiligingsgerelateerde eisen moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen aan bestaande informatiesystemen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 5.39 HLT – Zorgontvangers op unieke wijze identificeren (zorgspecifiek)	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	Zorgontvangers zijn geen gebruikers van onze applicaties.	Ja	Ja	Ja	Nee	Ja
Annex 5.40 HLT – Validatie van getoonde/geprinte gegevens (zorgspecifiek)	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	Ja	Ja	Ja	Ja
Annex 5.41 HLT – Openbaar beschikbare gezondheidsinformatie (zorgspecifiek)	Openbaar beschikbare gezondheidsinformatie moet worden beschermd, bewaard en beheerd gedurende de volledige levenscyclus.	Nee	Netbasics kan als beheerder hier geen verantwoordelijkheid voor dragen					
Annex 5.42 HLT – Communicatie in noodsituaties (zorgspecifiek)	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.	Nee	Netbasics is geen zorgorganisatie.					
Annex 5.43 HLT – Incidenten extern melden (zorgspecifiek)	Informatiebeveiligingsincidenten moeten volgens juridische of contractuele verplichtingen of verplichtingen uit hoofde van wet- en regelgeving worden gemeld.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 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 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.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 6.2 Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 6.2 Arbeidsovereenkomst (zorgspecifiek)	In functiebeschrijvingen moeten de beveiligingsrollen en verantwoordelijkheden worden vermeld die van toepassing zijn op het verwerken van persoonlijke gezondheidsinformatie.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 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, onderwerpspecifieke beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie, krijgen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 6.6 Vertrouwelijkheids- of geheimhoudingsovereenkomsten (zorgspecifiek)	Alle personeel dat bevoegd is tot toegang tot persoonlijke gezondheidsinformatie moet er formeel toe worden verplicht die informatie vertrouwelijk te behandelen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja

Annex 6.9 HLT – Managementtraining (zorgspecifiek)	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		Nee	Ja	Nee	Nee	Ja
Annex 7.1 Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 7.2 Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 7.3 Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 7.4 Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 7.6 Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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 worden afgedwongen.	Ja		Nee	Ja	Nee		Ja
Annex 7.8 Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 7.9 Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Ja	Nee	Ja
Annex 7.10 Opslagmedia (zorgspecifiek)	Alle persoonlijke gezondheidsinformatie die op verwijderbare media wordt opgeslagen moet worden versleuteld.	Ja		Nee	Ja	Ja	Nee	Ja
Annex 7.11 Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 7.13 Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en vertrouwelijkheid van informatie te garanderen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 8.1 ‘User endpoint devices’	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.2 Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.3 Beperking toegang tot informatie	De toegang tot informatie en andere gerelateerde bedrijfsmiddelen moet worden beperkt overeenkomstig het vastgestelde onderwerpspecifieke beleid inzake toegangsbeveiliging.	Ja		Nee	Ja	Ja	Nee	Ja
Annex 8.4 Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.5 Beveiligde authenticatie	Er moeten beveiligde authenticatietechnologieën en -procedures worden geïmplementeerd op basis van beperkingen van de toegang tot informatie en het onderwerpspecifieke beleid inzake toegangsbeveiliging	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.5 Beveiligde authenticatie (zorgspecifiek)	Er moet ten minste tweefactorauthenticatie worden gebruikt voor systemen die persoonlijke gezondheidsinformatie verwerken.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.6 Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.7 Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.	Ja		Nee	Ja	Nee	Nee	Ja

Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 8.9 Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.10 Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 8.11 Maskeren van gegevens	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		Nee	Ja	Nee	Nee	Ja
Annex 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 verwerkt, opgeslagen of getransporteerd.	Ja		Ja	Ja	Nee	Nee	Ja
Annex 8.13 Back-up van informatie	Back-ups van informatie, software en systemen moeten worden bewaard en regelmatig worden getest overeenkomstig het overeengekomen onderwerpspecifieke beleid inzake back-ups.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.13 Back-up van informatie (zorgspecifiek)	Back-ups van persoonlijke gezondheidsinformatie moeten worden versleuteld.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.14 Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.15 Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 8.17 Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 8.20 Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.21 Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.22 Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.23 Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 8.25 Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.26 Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 8.28 Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling.	Ja		Nee	Ja	Nee	Nee	Ja

Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 8.30 Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.	Nee	Systeemontwikkeling is in eigen beheer (hosting is wel uitbesteed)	Nee	Ja	Nee	Nee	Nee
Annex 8.31 Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.32 Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 8.33 Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.	Ja		Nee	Ja	Nee	Nee	Ja
Annex 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		Nee	Ja	Nee	Nee	Ja
Annex 8.35 HLT – Zero trust-beginselen (zorgspecifiek)	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		Nee	Ja	Nee	Nee	Ja

s

Jan Broos - Directeur
5-1-2026

