ISO/IEC 27001:2023 + A1:2024 + NEN 7510:2024
Name of the organization: Roseman Labs B.V.
Date: 23-02-2026. **Version number**: 1.0

Beheersmaatregel	Omschrijving beheersmaatregel (ISO/IEC 27001) - NL	Omschrijving zorgspecifieke beheersmaatregel (NEN 7510) - NL	Van toepassing	Geïmple-menteerd	Reden	Uitbesteed
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 en als zich significante wijzigingen voordoen, worden beoordeeld.	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	Wet- en regelgeving, contract, risicoanalyse	Nee
A.5.2 Rollen en verantwoordelijkheden bij informatiebeveiliging	Rollen en verantwoordelijkheden bij informatiebeveiliging moeten worden gedefinieerd en toegewezen overeenkomstig de behoeften van de organisatie.	Er moet ten minste één persoon verantwoordelijk zijn voor informatiebeveiliging.	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee
A.5.3 Functiescheiding	Conflicterende taken en conflicterende verantwoordelijkheden moeten worden gescheiden.		Ja	Ja	Risicoanalyse, contract	Nee
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	Ja	Risicoanalyse, contract	Nee
A.5.5 Contact met overheidsinstanties	De organisatie moet contact met de relevante instanties leggen en onderhouden.		Ja	Ja	Risicoanalyse	Nee
A.5.6 Contact met speciale belangengroepen	De organisatie moet contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en beroepsverenigingen leggen en onderhouden.		Ja	Ja	Risicoanalyse	Nee
A.5.7 Informatie en analyses over dreigingen	Informatie met betrekking tot informatiebeveiligingsdreigingen moet worden verzameld en geanalyseerd om informatie over dreigingen te produceren.		Ja	Ja	Risicoanalyse	Nee
A5.8 Informatiebeveiliging in projectmanagement	Informatiebeveiliging moet worden geïntegreerd in projectmanagement.		Ja	Ja	Risicoanalyse	Nee
A.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.	Alle informatiestromen (zowel binnen als tussen organisaties) en de interfaces daarvan (waaronder integratieplatforms) moeten worden opgenomen in de inventarisatie.	Ja	Ja	Risicoanalyse	Nee
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 geïdentificeerd, gedocumenteerd en geïmplementeerd.		Ja	Ja	Risicoanalyse	Nee
A.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	Ja	Risicoanalyse	Nee
A.5.11 Retourneren van bedrijfsmiddelen		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.	Nee	Nee	Roseman Labs verwerkt geen zorginformatie in leesbare vorm. Gegevens die klanten uploaden, worden onmiddellijk cryptografisch beschermd met MPC en zijn op geen moment toegankelijk voor medewerkers. De zorgspecifieke verplichting om de veilige teruggave/verwijdering van zorginformatie door personen te laten bevestigen is daarom niet van toepassing.	
A.5.12 Classificatie 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	Persoonlijke gezondheidsinformatie behoort uniform als vertrouwelijk te worden geclassificeerd.	Ja	Ja	Risicoanalyse	Nee
A.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	Ja	Risicoanalyse	Nee
A.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.	Vóórdat enige overdracht plaatsvindt, moeten er regels, procedures en overeenkomsten zijn ingesteld.	Ja	Ja	Wet- en regelgeving, risicoanalyse, contract	Nee
A.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.	Er moet beleid voor op rollen gebaseerde toegangsbeveiliging gelden voor de toegang tot persoonlijke gezondheidsinformatie.	Ja	Ja	Risicoanalyse, contract	Nee
A.5.16 Identiteitsbeheer	De volledige levenscyclus van identiteiten moet worden beheerd.	Gebruikers die toegang willen hebben tot persoonlijke gezondheidsinformatie en andere vertrouwelijke informatie, moeten formeel zijn geregistreerd.	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee
A.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	Ja	Risicoanalyse, contract	Nee
A.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	Ja	Risicoanalyse, contract	Nee
A.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.	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	Wet- en regelgeving, contract, risicoanalyse	Nee
A.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	Ja	Contract, risicoanalyse	Nee
A.5.21 Beheren van informatiebeveiliging in de ICT-toeleveringsketen	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	Contract, risicoanalyse	Nee
A.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	Ja	Risicoanalyse	Nee
A5.23 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	Risicoanalyse	Nee
A.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	Risicoanalyse	Nee
A.5.25 Beoordelen van en besluiten over informatiebeveiligingsgebeurtenissen	De organisatie moet informatiebeveiligingsgebeurtenissen beoordelen en beslissen of ze moeten worden gecategoriseerd als informatiebeveiligingsincidenten.		Ja	Ja	Risicoanalyse	Nee
A.5.26 Reageren op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten moet worden gereageerd in overeenstemming met de gedocumenteerde procedures.		Ja	Ja	Risicoanalyse	Nee
A.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	Risicoanalyse	Nee
A.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	Wet- en regelgeving, contract, risicoanalyse	Nee
A.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	Ja	Risicoanalyse	Nee
A.5.30. ICT-gereedheid voor bedrijfscontinuïteit	De ICT-gereedheid moet worden gepland, geïmplementeerd, onderhouden en getest op basis van bedrijfscontinuïteitsdoelstellingen en ICT-continuïteitseisen.		Ja	Ja	Risicoanalyse	Nee
A.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	Wet- en regelgeving	Nee
A.5.32 Intellectuele-eigendomsrechten	De organisatie moet passende procedures implementeren om intellectuele-eigendomsrechten te beschermen.		Ja	Ja	Risicoanalyse	Nee
A.5.33 Beschermen van registraties	Registraties moeten worden beschermd tegen verlies, vernietiging, vervalsing, toegang door onbevoegden en ongeoorloofde vrijgave.		Ja	Ja	Risicoanalyse	Nee
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 eraan voldoen.		Ja	Ja	Wet- en regelgeving	Nee
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 geplande tussenpozen of zodra zich belangrijke veranderingen voordoen, worden beoordeeld.		Ja	Ja	Risicoanalyse, contract	Nee
A.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	Ja	Risicoanalyse, contract	Nee
A.5.37 Gedocumenteerde bedieningsprocedures	Bedieningsprocedures voor informatieverwerkende faciliteiten moeten worden gedocumenteerd en beschikbaar worden gesteld aan het personeel dat ze nodig heeft.		Ja	Ja	Risicoanalyse, contract	Nee
A.5.38 HLT – Analyse en specificatie van informatiebeveiligingseisen		De informatiebeveiligingsgerelateerde eisen moeten worden opgenomen in de eisen voor nieuwe informatiesystemen of verbeteringen aan bestaande informatiesystemen.	Ja	Ja	Risicoanalyse, contract	Nee
A.5.39 HLT – Zorgontvangers op unieke wijze identificeren		Beleid en processen moeten waarborgen dat elke zorgontvanger op unieke wijze binnen het systeem kan worden geïdentificeerd en dubbele registraties kunnen worden samengevoegd.	Nee	Nee	Roseman Labs faciliteert geen gezondheids-informatie systemen in het primaire zorgproces.	nvt

A.5.40 HLT – Validatie van getoonde/geprinte gegevens		Gegevens die worden getoond/geprint moeten informatie bevatten waarmee de zorgontvanger wordt geïdentificeerd.	Nee	Nee	Roseman Labs verwerkt zelf geen gezondheidsinformatie. De klanten waarbij gezondheidsinformatie wordt geanalyseerd met behulp van het product van Roseman Labs kan deze informatie uitsluitend analyseren onder MPC. Alle zichtbare uitkomsten na analyse worden vooraf inhoudelijk getoetst door een analist en formeel goedgekeurd door een bevoegde approver, conform de voorwaarden van de verantwoordelijke organisatie. De eis tot validatie van getoonde/geprinte patiëntidentificerende gegevens is is verantwoordelijkheid van de klant en daarom niet van toepassing voor Roseman Labs.	nvt
A.5.41 HLT – Openbaar beschikbare gezondheidsinformatie		Openbaar beschikbare gezondheidsinformatie moet worden beschermd, bewaard en beheerd gedurende de volledige levenscyclus.	Nee	Nee	Roseman Labs publiceert zelf geen gezondheidsinformatie.	
A.5.42 HLT – Communicatie in noodsituaties		Noodcommunicatiekanalen moeten gepland, geïmplementeerd, onderhouden en getest worden.	Ja	Ja	Risicoanalyse	Nee
A.5.43 HLT – Incidenten extern melden		Informatiebeveiligingsincidenten moeten volgens juridische of wettelijke verplichtingen extern worden gemeld.	Ja	Ja	Wet- en regelgeving	Nee
A.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	Risicoanalyse, contract	Nee
A.6.2 Arbeidsovereenkomst	In arbeidsovereenkomsten moet worden vermeld wat de verantwoordelijkheden van het personeel en van de organisatie zijn wat betreft informatiebeveiliging.	In functiebeschrijvingen moeten de beveiligingsrollen en verantwoordelijkheden worden vermeld die van toepassing zijn op het verwerken van persoonlijke gezondheidsinformatie.	Ja	Ja	Risicoanalyse	Nee
A.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	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee
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	Ja	Risicoanalyse	Nee
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	Ja	Risicoanalyse	Nee
A.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.	Alle personeel dat bevoegd is tot toegang tot persoonlijke gezondheidsinformatie moet er formeel toe worden verplicht die informatie vertrouwelijk te behandelen.	Ja	Ja	Risicoanalyse	Nee
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 ingezien, verwerkt of opgeslagen.		Ja	Ja	Risicoanalyse	Nee
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	Ja	Risicoanalyse, contract	Nee
A.6.9 HLT – Managementtraining		Het management moet passende training krijgen over informatiebeveiliging en hun verantwoordelijkheden.	Ja	Ja	Risicoanalyse	Nee
A.7.1 Fysieke beveiligingszones	Zones die informatie en andere gerelateerde bedrijfsmiddelen bevatten, moeten worden beschermd door beveiligingszones te definiëren en te gebruiken.		Ja	Ja	Risicoanalyse	Nee
A.7.2 Fysieke toegangsbeveiliging	Beveiligde zones moeten worden beschermd door passende toegangsbeveiligingsmaatregelen en toegangspunten.		Ja	Ja	Risicoanalyse, Uitbesteed proces	Gedeeltelijk
A.7.3 Beveiligen van kantoren, ruimten en faciliteiten	Voor kantoren, ruimten en faciliteiten moet fysieke beveiliging worden ontworpen en geïmplementeerd.		Ja	Ja	Risicoanalyse	Gedeeltelijk
A.7.4 Monitoren van de fysieke beveiliging	Het gebouw en terrein moet voortdurend worden gemonitord op onbevoegde fysieke toegang.		Ja	Ja	Risicoanalyse	Gedeeltelijk
A.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	Ja	Risicoanalyse	Nee
A.7.6 Werken in beveiligde zones	Voor het werken in beveiligde zones moeten beveiligingsmaatregelen worden ontwikkeld en geïmplementeerd.		Ja	Ja	Risicoanalyse	Nee
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 worden afgedwongen.		Ja	Ja	Risicoanalyse	Nee
A.7.8 Plaatsen en beschermen van apparatuur	Apparatuur moet veilig worden geplaatst en beschermd.		Ja	Ja	Risicoanalyse	Gedeeltelijk
A.7.9 Beveiligen van bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen buiten het gebouw en/of terrein moeten worden beschermd.		Ja	Ja	Risicoanalyse	Nee
A.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.	Alle persoonlijke gezondheidsinformatie die op verwijderbare media wordt opgeslagen moet worden versleuteld.	Ja	Ja	Risicoanalyse	Nee
A.7.11 Nutsvoorzieningen	Informatieverwerkende faciliteiten moeten worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door storingen in nutsvoorzieningen.		Ja	Ja	Risicoanalyse	Gedeeltelijk
A.7.12 Beveiliging van bekabeling	Voedingskabels en kabels voor het versturen van gegevens of die informatiediensten ondersteunen, moeten worden beschermd tegen onderschepping, interferentie of beschadiging.		Ja	Ja	Risicoanalyse	Nee
A.7.13 Onderhoud van apparatuur	Apparatuur moet op de juiste wijze worden onderhouden om de beschikbaarheid, integriteit en betrouwbaarheid van informatie te garanderen.		Ja	Ja	Risicoanalyse	Nee
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	Ja	Risicoanalyse	Nee
A.8.1 'User endpoint devices'	Informatie die is opgeslagen op, wordt verwerkt door of toegankelijk is via 'user endpoint devices' moet worden beschermd.		Ja	Ja	Risicoanalyse	Nee
A.8.2 Speciale toegangsrechten	Het toewijzen en het gebruik van speciale toegangsrechten moet worden beperkt en beheerd.		Ja	Ja	Risicoanalyse, contract	Nee
A.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	Ja	Risicoanalyse, contract	Nee
A.8.4 Toegangsbeveiliging op broncode	Lees- en schrijftoegang tot broncode, ontwikkelinstrumenten en softwarebibliotheken moet op passende wijze worden beheerd.		Ja	Ja	Risicoanalyse, contract	Nee
A.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	Er moet ten minste tweefactorauthenticatie worden gebruikt voor systemen die persoonlijke gezondheidsinformatie verwerken.	Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee
A.8.6 Capaciteitsbeheer	Het gebruik van middelen moet worden gemonitord en aangepast overeenkomstig de huidige en verwachte capaciteitseisen.		Ja	Ja	Risicoanalyse	Nee
A.8.7 Bescherming tegen malware	Bescherming tegen malware moet worden geïmplementeerd en ondersteund door een passend gebuikersbewustzijn.		Ja	Ja	Risicoanalyse	Nee
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 moeten passende maatregelen worden getroffen.		Ja	Ja	Risicoanalyse, contract	Nee
A8.9 Configuratiebeheer	Configuraties, met inbegrip van beveiligingsconfiguraties, van hardware, software, diensten en netwerken moeten worden vastgesteld, gedocumenteerd, geïmplementeerd, gemonitord en beoordeeld.		Ja	Ja	Risicoanalyse	Nee

A8.10 Wissen van informatie	In informatiesystemen, apparaten of andere opslagmedia opgeslagen informatie moet worden gewist als deze niet langer vereist is		Ja	Ja	Risicoanalyse	Nee
A8.11 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	Ja	Risicoanalyse	Nee
A8.12 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	Risicoanalyse	Nee
A.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	Back-ups van persoonlijke gezondheidsinformatie moeten worden versleuteld.	Ja	Ja	Risicoanalyse, contract	Nee
A 8.14 Redundantie van informatieverwerkende faciliteiten	Informatieverwerkende faciliteiten moeten met voldoende redundantie worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.		Ja	Ja	Risicoanalyse	Gedeeltelijk
A.8.15 Logging	Er moeten logbestanden waarin activiteiten, uitzonderingen, fouten en andere relevante gebeurtenissen worden geregistreerd, worden geproduceerd, opgeslagen, beschermd en geanalyseerd.		Ja	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee
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	Ja	Risicoanalyse	Gedeeltelijk
A.8.17 Kloksynchronisatie	De klokken van informatieverwerkende systemen die door de organisatie worden gebruikt, moeten worden gesynchroniseerd met goedgekeurde tijdbronnen.		Ja	Ja	Risicoanalyse	Nee
A.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	Ja	Risicoanalyse	Nee
A8.19 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	Ja	Risicoanalyse	Nee
A8.20 Beveiliging netwerkcomponenten	Netwerken en netwerkapparaten moeten worden beveiligd, beheerd en beheerst om informatie in systemen en toepassingen te beschermen.		Ja	Ja	Risicoanalyse	Nee
A.8.21 Beveiliging van netwerkdiensten	Beveiligingsmechanismen, dienstverleningsniveaus en dienstverleningseisen voor alle netwerkdiensten moeten worden geïdentificeerd, geïmplementeerd en gemonitord.		Ja	Ja	Risicoanalyse, contract	Nee
A8.22 Netwerksegmentatie	Groepen informatiediensten, gebruikers en informatiesystemen moeten in de netwerken van de organisatie worden gesegmenteerd.		Ja	Ja	Risicoanalyse, contract	Nee
A8.23 Toepassen van webfilters	De toegang tot externe websites moet worden beheerd om de blootstelling aan kwaadaardige inhoud te beperken.		Ja	Ja	Risicoanalyse	Nee
A.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	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee
A.8.25 Beveiligen tijdens de ontwikkelcyclus	Voor het veilig ontwikkelen van software en systemen moeten regels worden vastgesteld en toegepast.		Ja	Ja	Risicoanalyse	Nee
A8.26 Toepassingsbeveiligingseisen	Er moeten eisen aan de informatiebeveiliging worden geïdentificeerd, gespecificeerd en goedgekeurd bij het ontwikkelen of aanschaffen van toepassingen.		Ja	Ja	Risicoanalyse	Nee
A8.27 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	Ja	Wet- en regelgeving, contract, risicoanalyse	Nee
A8.28 Veilig coderen	Er moeten principes voor veilig coderen worden toegepast op softwareontwikkeling		Ja	Ja	Risicoanalyse	Nee
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	Ja	Risicoanalyse, contract	Nee
A.8.30 Uitbestede systeemontwikkeling	De organisatie moet de activiteiten in verband met uitbestede systeemontwikkeling sturen, bewaken en beoordelen.		Ja	Ja	Risicoanalyse	Nee
A8.31 Scheiding van ontwikkel-, test- en productieomgevingen	Ontwikkel-, test- en productieomgevingen moeten worden gescheiden en beveiligd.		Ja	Ja	Risicoanalyse	Nee
A.8.32 Wijzigingsbeheer	Wijzigingen in informatieverwerkende faciliteiten en informatiesystemen moeten onderworpen zijn aan procedures voor wijzigingsbeheer.		Ja	Ja	Risicoanalyse	Nee
A8.33 Testgegevens	Testgegevens moeten op passende wijze worden geselecteerd, beschermd en beheerd.		Ja	Ja	Risicoanalyse	Nee
A.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	Ja	Risicoanalyse, contract	Nee
A.8.35 HLT – Zero trust-beginselen		Netwerksegmenten moeten zo klein mogelijk zijn en mogen alleen toegang krijgen na wederzijdse authenticatie.	Ja	Ja	Risicoanalyse	Nee