Verklaring van Toepasselijkheid **OSSO B.V.**

Norm: **NEN7510-1:2017+A1:2020 NL**

Versie: **7.0**

Datum: 6 September 2021

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
5.1.1	Beleidsregels voor informatiebeveiliging	Ten behoeve van informatiebeveiliging moet een reeks beleidsregels worden gedefinieerd, goedgekeurd door de directie, gepubliceerd en gecommuniceerd aan medewerkers en relevante externe partijen.	☐	☑	☐	☑	☑	
5.1.1 NEN7510	Beleidsregels voor informatiebeveiliging	Organisaties moeten beschikken over een schriftelijk informatiebeveiligingsbeleid dat door het management wordt goedgekeurd, wordt gepubliceerd en vervolgens wordt gecommuniceerd aan alle werknemers en relevante externe partijen.	☐	☑	☐	☑	☑	
5.1.2	Beoordelen van het informatiebeveiligingsgebied	Het beleid voor informatiebeveiliging moet met geplande tussenpozen of als zich significante veranderingen voordoen, worden beoordeeld om te waarborgen dat het voortdurend passend, adequaat en doeltreffend is.	☐	☑	☐	☑	☑	
5.1.2 NEN7510	Beoordelen van het informatiebeveiligingsgebied	Het informatiebeveiligingsbeleid moet aan voortdurende, gefaseerde beoordelingen worden onderworpen zodat het volledige beleid ten minste eenmaal per jaar wordt beoordeeld. Het beleid moet worden beoordeeld als er zich een ernstig beveiligingsincident heeft voorgedaan.	☐	☑	☐	☑	☑	
6.1.1	Rollen en verantwoordelijkheden	Alle verantwoordelijkheden bij informatiebeveiliging behoren te worden gedefinieerd en toegewezen.	☐	☑	☐	☑	☑	
6.1.1 NEN7510-deel-1a	Rollen en verantwoordelijkheden	Organisaties moeten duidelijk verantwoordelijkheden op het gebied van informatiebeveiliging definiëren en toewijzen. Er moet minimaal één individu verantwoordelijk zijn voor beveiliging van gezondheids-informatie binnen de organisatie.	☐	☑	☐	☑	☑	
6.1.1 NEN7510-deel-1b	Rollen en verantwoordelijkheden	over een informatiebeveiligings-managementforum (IBMF) beschikken om te garanderen dat er duidelijke aansturing en zichtbare ondersteuning vanuit het management is voor beveiligingsinitiatieven die betrekking hebben op de beveiliging van gezondheidsinformatie, zoals beschreven in B3 en B4 van bijlage B (6.1.1) in NEN 7510-2.	☐	☑	☐	☑	☑	
6.1.1 NEN7510-deel-2	Rollen en verantwoordelijkheden	Het gezondheids-informatie-beveiligingsforum moet regelmatig, maandelijks of bijna maandelijks, vergaderen. (Het is meestal het effectiefst als het forum vergadert op een tijdstip halverwege tussen twee vergaderingen van het bestuursorgaan waaraan het forum rapporteert. Zo kunnen urgente zaken binnen een korte periode in een geschikte vergadering worden besproken.)	☐	☑	☐	☑	☑	
6.1.1 NEN7510-deel-3	Rollen en verantwoordelijkheden	Er moet een formele verklaring van het toepassingsgebied worden geproduceerd waarin de grens wordt gedefinieerd van nalevingsactiviteiten wat betreft mensen, processen, plekken, platformen en toepassingen.	☐	☑	☐	☑	☑	
6.1.2	Scheiding van taken	Conflicterende taken en verantwoordelijkheden behoren te worden gescheiden om de kans op onbevoegd of onbedoeld wijzigen van de bedrijfsmiddelen van de organisatie te verminderen.	☐	☑	☐	☑	☑	
6.1.2 NEN7510	Scheiding van taken	Organisaties moeten, indien dit haalbaar is, plichten en verantwoordelijkheidsgebieden scheiden teneinde de kansen te verkleinen van onbevoegde wijziging of misbruik van persoonlijke gezondheidsinformatie.	☐	☑	☐	☑	☑	
6.1.3	Contact met overheidsinstanties	Er behoren passende contacten met relevante overheidsinstanties te worden onderhouden.	☐	☑	☐	☑	☑	
6.1.4	Contact met speciale belangengroepen	Er behoren contacten met speciale belangengroepen of andere gespecialiseerde beveiligingsfora en professionele organisaties te worden onderhouden.	☐	☑	☐	☑	☑	
6.1.5	Informatiebeveiliging in projectbeheer	Informatiebeveiliging behoort aan de orde te komen in projectbeheer, ongeacht het soort project.	☐	☑	☐	☑	☑	
6.1.5 NEN7510	Informatiebeveiliging in projectbeheer	Bij het management van projecten moet de patiëntveiligheid als projectrisico in aanmerking worden genomen voor elk project dat gepaard gaat met het verwerken van persoonlijke gezondheidsinformatie.	☐	☑	☐	☑	☑	
6.2.1	Beleid voor mobiele apparatuur	Beleid en ondersteunende beveiligingsmaatregelen behoren te worden vastgesteld om de risico's die het gebruik van mobiele apparatuur met zich meebrengt te beheren.	☐	☑	☐	☑	☑	
6.2.2	Telewerken	Beleid en ondersteunende beveiligingsmaatregelen behoren te worden geïmplementeerd ter beveiliging van informatie die vanaf telewerklocaties wordt benaderd, verwerkt of opgeslagen.	☐	☑	☐	☑	☑	
7.1.1	Screening	Verificatie van de achtergrond van alle kandidaten voor een dienstverband behoort te worden uitgevoerd in overeenstemming met relevante wet- en regelgeving en ethische overwegingen en behoort in verhouding te staan tot de bedrijfseisen, de classificatie van de informatie waartoe toegang wordt verleend en de vastgestelde risico's te zijn.	☐	☑	☐	☑	☑	
7.1.1 NEN7510-deel-1	Screening	Organisaties moeten minimaal de identiteit, het huidige adres en de vorige werkkring van personeel en contractanten en vrijwilligers op het moment van de sollicitatie verifiëren.	☐	☑	☐	☑	☑	

Verklaring van Toepasselijkheid **OSSO B.V.**

Norm: **NEN7510-1:2017+A1:2020 NL**

Versie: **7.0**

Datum: 6 September 2021

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
7.1.1 NEN7510-deel-2	Screening	Verificatiecontroles van de achtergrond van alle kandidaten voor een dienstverband moeten een verificatie omvatten van de toepasselijke kwalificaties voor zorgverleners, indien er sprake is van accreditatie voor de beroepsgroep op basis van die kwalificaties (bijv. artsen, verplegend personeel enz.)	☐	☐	☐	☐	☐	OSSO is geen zorgverlener en heeft geen personeel waarbij er sprake is van toepasselijke kwalitificaties voor zorgverleners en accreditatie op basis van die kwalificaties (artsen, verplegend personeel, etc).
7.1.1 NEN7510-deel-3	Screening	Als een persoon wordt ingehuurd voor een specifieke beveiligingsfunctie, moet de organisatie zich ervan vergewissen dat: a) de kandidaat over de nodige competentie beschikt om de beveiligingsfunctie te vervullen; b) de functie de kandidaat toevertrouwd kan worden, in het bijzonder als de functie cruciaal is voor de organisatie.	☐	☑	☐	☑	☑	
7.1.2	Arbeidsvoorwaarden	De contractuele overeenkomst met medewerkers en contractanten behoort hun verantwoordelijkheden voor informatiebeveiliging en die van de organisatie te vermelden.	☐	☑	☐	☑	☑	
7.1.2 NEN7510-deel-1	Arbeidsvoorwaarden	Alle organisaties waarvan personeelsleden betrokken zijn bij het verwerken van persoonlijke gezondheidsinformatie, moeten die betrokkenheid in relevante functieomschrijvingen vastleggen. Beveiligingsrollen en verantwoordelijkheden, zoals vastgelegd in het informatiebeveiligingsbeleid van de organisatie, moeten ook in relevante functieomschrijvingen worden vastgelegd.	☐	☑	☐	☑	☑	
7.1.2 NEN7510-deel-2	Arbeidsvoorwaarden	Er moet speciale aandacht worden besteed aan de rollen en verantwoordelijkheden van tijdelijk personeel of personeel met een kort dienstverband zoals vervangers, studenten, stagiairs enz.	☐	☑	☐	☑	☑	
7.2.1	Directieverantwoordelijkheden	De directie behoort van alle medewerkers en contractanten te eisen dat ze informatiebeveiliging toepassen in overeenstemming met de vastgestelde beleidsregels en procedures van de organisatie.	☐	☑	☐	☑	☑	
7.2.2	Bewustzijn, opleiding en training t.a.v. informatiebeveiliging	Alle medewerkers van de organisatie en, voor zover relevant, contractanten behoren een passende bewustzijnsopleiding en -training te krijgen en regelmatige bijscholing van beleidsregels en procedures van de organisatie, voor zover relevant voor hun functie.	☐	☑	☐	☑	☑	
7.2.2 NEN7510-deel-1	Bewustzijn, opleiding en training t.a.v. informatiebeveiliging	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat onderwijs en training over informatiebeveiliging worden gegeven bij de introductie van nieuwe medewerkers en dat er regelmatig updates van beveiligingsbeleid en -procedures van de organisatie worden verstrekt aan alle werknemers en, indien relevant, derde-contractanten, onderzoekers, studenten en vrijwilligers die persoonlijke gezondheidsinformatie verwerken.	☐	☑	☐	☑	☑	
7.2.2 NEN7510-deel-2	Bewustzijn, opleiding en training t.a.v. informatiebeveiliging	Werknemers van de organisatie en, waar relevant, derdecontractanten moeten worden gewezen op disciplinaire processen en gevolgen met betrekking tot schendingen van informatiebeveiliging.	☐	☑	☐	☑	☑	
7.2.3	Disciplinaire procedure	Er behoort een formele en gecommuniceerde disciplinaire procedure te zijn om actie te ondernemen tegen medewerkers die een inbreuk hebben gepleegd op de informatiebeveiliging.	☐	☑	☐	☑	☑	
7.3.1	Beëindiging of wijziging van verantwoordelijkheden van het dienstverband	Verantwoordelijkheden en taken met betrekking tot informatiebeveiliging die van kracht blijven na beëindiging of wijziging van het dienstverband behoren te worden gedefinieerd, gecommuniceerd aan de medewerker of contractant, en ten uitvoer gebracht.	☐	☑	☐	☑	☑	
8.1.1	Inventariseren van bedrijfsmiddelen	Informatie, bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren te worden geïdentificeerd, en van deze middelen behoort een inventaris te worden opgesteld en onderhouden.	☐	☑	☐	☑	☑	
8.1.1 NEN7510	Inventariseren van bedrijfsmiddelen	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten:a) verantwoording afleggen over informatiebedrijfsmiddelen (d.w.z. een inventaris bijhouden van dergelijke bedrijfsmiddelen); b) een eigenaar hebben aangewezen voor deze informatiebedrijfsmiddelen (zie 8.1.2); c) regels hebben voor het aanvaardbare gebruik van deze bedrijfsmiddelen die geïdentificeerd, gedocumenteerd en geïmplementeerd worden.	☐	☑	☐	☑	☑	
8.1.2	Eigendom van bedrijfsmiddelen	Bedrijfsmiddelen die in het inventarisoverzicht worden bijgehouden, behoren een eigenaar te hebben. De eigenaar van het bedrijfsmiddel hebben de verantwoordelijkheid voor de levenscyclus van een bedrijfsmiddel.	☐	☑	☐	☑	☑	
8.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Voor het aanvaardbaar gebruik van informatie en van bedrijfsmiddelen die samenhangen met informatie en informatie verwerkende faciliteiten behoren regels te worden geïdentificeerd, gedocumenteerd en geïmplementeerd.	☐	☑	☐	☑	☑	

Verklaring van Toepasselijkheid **OSSO B.V.**

Norm: **NEN7510-1:2017+A1:2020 NL**

Versie: **7.0**

Datum: 6 September 2021

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
8.1.4	Teruggeven van bedrijfsmiddelen	Alle medewerkers en externe gebruikers behoren alle bedrijfsmiddelen van de organisatie die ze in hun bezit hebben bij beëindiging van hun dienstverband, contract of overeenkomst terug te geven.	☐	☑	☐	☑	☑	
8.1.4 NEN7510	Teruggeven van bedrijfsmiddelen	Alle werknemers en contractanten moeten, na beëindiging van hun dienstverband, alle persoonlijke gezondheidsinformatie in niet-elektronische vorm die zij in hun bezit hebben, teruggeven en erop toezien dat alle persoonlijke gezondheidsinformatie in elektronische vorm die zij in hun bezit hebben, op relevante systemen wordt bijgewerkt en vervolgens op beveiligde wijze wordt gewist van alle apparaten waarop deze aanwezig was.	☐	☑	☐	☑	☑	
8.2.1	Classificatie van informatie	Informatie behoort te worden geclassificeerd met betrekking tot wettelijke eisen, waarde, belang en gevoeligheid voor onbevoegde bekendmaking of wijziging.	☐	☑	☐	☑	☑	
8.2.1 NEN7510	Classificatie van informatie	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten dergelijke gegevens op uniforme wijze als vertrouwelijk classificeren.	☐	☑	☐	☑	☑	
8.2.2	Informatie labelen	Om informatie te labelen behoort een passende reeks procedures te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door de organisatie.	☐	☑	☐	☑	☑	
8.2.2 NEN7510	Informatie labelen	Alle gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten de gebruikers wijzen op de vertrouwelijkheid van persoonlijke gezondheidsinformatie die toegankelijk is vanaf het systeem (bijv. bij het opstarten of inloggen), en moeten papieren output als vertrouwelijk labelen als die output persoonlijke gezondheidsinformatie bevat.	☐	☑	☐	☑	☑	
8.2.3	Behandelen van bedrijfsmiddelen	Procedures voor het behandelen van bedrijfsmiddelen behoren te worden ontwikkeld en geïmplementeerd in overeenstemming met het informatieclassificatieschema dat is vastgesteld door <organisatie>.	☐	☑	☐	☑	☑	
8.3.1	Beheer van verwijderbare media	Voor het beheren van verwijderbare media behoren procedures te worden geïmplementeerd in overeenstemming met het classificatieschema dat door de organisatie is vastgesteld.	☐	☑	☐	☑	☑	
8.3.1 NEN7510	Beheer van verwijderbare media	Media die persoonlijke gezondheidsinformatie bevatten moeten fysiek worden beschermd of de gegevens ervan moeten versleuteld worden. De status en locatie van media die niet-versleutelde persoonlijke gezondheidsinformatie bevatten, moeten gemonitord worden.	☐	☑	☐	☑	☑	
8.3.2	Verwijderen van media	Media behoren op een veilige en beveiligde manier te worden verwijderd als ze niet langer nodig zijn, overeenkomstig formele procedures.	☐	☑	☐	☑	☑	
8.3.2 NEN7510	Verwijderen van media	Alle persoonlijke gezondheids-informatie moet veilig worden gewist of anders moeten de media worden vernietigd als ze niet meer gebruikt hoeven te worden.	☐	☑	☐	☑	☑	
8.3.3	Media fysiek overdragen	Media die informatie bevatten, behoren te worden beschermd tegen onbevoegde toegang, misbruik of corruptie tijdens transport.	☐	☑	☐	☑	☑	
9.1.1	Beleid voor toegangsbeveiliging	Een beleid voor toegangsbeveiliging behoort te worden vastgesteld, gedocumenteerd en beoordeeld op basis van bedrijfs- en informatiebeveiligingseisen.	☐	☑	☐	☑	☑	
9.1.1 NEN7510-deel-1a	Beleid voor toegangsbeveiliging	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheids-informatiesystemen hun toegang tot persoonlijke gezondheids-informatie beperken tot situaties waarin er een zorgrelatie bestaat tussen de gebruiker en de persoon waarop de gegevens betrekking hebben (de cliënt tot wiens persoonlijke gezondheidsinformatie er toegang wordt gemaakt).	☐	☐	☐	☐	☐	OSSO is beheerder van onderliggende infrastructuur en heeft geen gebruikerstoegang tot persoonlijke gezondheidsinformatie.
9.1.1 NEN7510-deel-1b	Beleid voor toegangsbeveiliging	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheids-informatiesystemen hun toegang tot persoonlijke gezondheids-informatie beperken tot situaties waarin de gebruiker een activiteit uitvoert namens de persoon waarop de gegevens betrekking hebben.	☐	☐	☐	☐	☐	OSSO is beheerder van onderliggende infrastructuur en heeft geen gebruikerstoegang tot persoonlijke gezondheidsinformatie.
9.1.1 NEN7510-deel-1c	Beleid voor toegangsbeveiliging	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de toegang tot dergelijke informatie controleren. In het algemeen moeten de gebruikers van gezondheids-informatiesystemen hun toegang tot persoonlijke gezondheids-informatie beperken tot situaties waarin er specifieke gegevens nodig zijn om deze activiteit te ondersteunen.	☐	☐	☐	☐	☐	OSSO is beheerder van onderliggende infrastructuur en heeft geen gebruikerstoegang tot persoonlijke gezondheidsinformatie.

Verklaring van Toepasselijkheid **OSSO B.V.**

Norm: **NEN7510-1:2017+A1:2020 NL**

Versie: **7.0**

Datum: 6 September 2021

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
9.1.1 NEN7510-deel-2a	Beleid voor toegangsbeveiliging	Organisaties die persoonlijke gezondheids-informatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld. Het beleid van de organisatie met betrekking tot toegangscontrole moet worden vastgesteld op basis van vooraf gedefinieerde rollen met bijbehorende bevoegdheden die passen bij, maar beperkt zijn tot, de behoeften van die rol.	☐	☑	☐	☑	☑	
9.1.1 NEN7510-deel-2b	Beleid voor toegangsbeveiliging	Organisaties die persoonlijke gezondheids-informatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld. Organisaties die persoonlijke gezondheids-informatie verwerken, moeten een toegangscontrolebeleid hebben waarmee de toegang tot deze gegevens wordt geregeld. Het toegangscontrolebeleid, als bestanddeel van het in 5.1.1 beschreven beleidskader voor informatiebeveiliging, moet professionele, ethische, juridische en cliëntgerelateerde eisen weerspiegelen en moet de taken die worden uitgevoerd door zorgverleners, en de workflow van de taak in aanmerking nemen.	☐	☐	☐	☐	☐	Als subverwerker is OSSO niet verantwoordelijk voor: professionele, ethische, juridische en cliëntgerelateerde eisen weerspiegelen en moeten de taken die worden uitgevoerd door zorgverleners, en de workflow van de taak in aanmerking nemen.
9.1.1 NEN7510-deel-3	Beleid voor toegangsbeveiliging	De organisatie moet alle partijen identificeren en documenteren waarmee cliëntgegevens worden uitgewisseld, en met deze partijen moeten contractuele afspraken over toegang en rechten worden gemaakt, alvorens cliëntgegevens uit te wisselen.	☐	☑	☐	☑	☑	
9.1.2	Toegang tot netwerken en netwerkdiensten	Gebruikers behoren alleen toegang te krijgen tot het netwerk en de netwerkdiensten waarvoor zij specifiek bevoegd zijn.	☐	☑	☐	☑	☑	
9.2.1	Registratie en afmelden van gebruikers	Een formele registratie- en afmeldingsprocedure behoort te worden geïmplementeerd om toewijzing van toegangsrechten mogelijk te maken.	☐	☑	☐	☑	☑	
9.2.1 NEN7510	Registratie en afmelden van gebruikers	De toegang tot gezondheids-informatiesystemen die persoonlijke gezondheidsinformatie verwerken, moet onderhevig zijn aan een formeel gebruikersregistratieproces. Procedures voor het registreren van gebruikers moeten garanderen dat het vereiste niveau van authenticatie van de geclaimde identiteit van gebruikers overeenkomt met het (de) toegangsniveau(s) waarover de gebruiker zal gaan beschikken. De gebruikersregistratie-gegevens moeten regelmatig worden beoordeeld om te garanderen dat ze volledig en juist zijn en dat toegang nog altijd vereist is.	☐	☑	☐	☑	☑	
9.2.2	Gebruikers toegang verlenen	Een formele gebruikerstoegangsverleningsprocedure behoort te worden geïmplementeerd om toegangsrechten voor alle typen gebruikers en voor alle systemen en diensten toe te wijzen of in te trekken.	☐	☑	☐	☑	☑	
9.2.3	Beheren van speciale toegangsrechten	Het toewijzen en gebruik van speciale toegangsrechten behoren te worden beperkt en beheerst.	☐	☑	☐	☑	☑	
9.2.4	Beheer van geheime authenticatie-informatie van gebruikers	Het toewijzen van geheime authenticatie-informatie behoort te worden beheerst via een formeel beheersproces.	☐	☑	☐	☑	☑	
9.2.5	Beoordeling van toegangsrechten van gebruikers	Eigenaren van bedrijfsmiddelen behoren toegangsrechten van gebruikers regelmatig te beoordelen.	☐	☑	☐	☑	☑	
9.2.6	Toegangsrechten intrekken of aanpassen	De toegangsrechten van alle medewerkers en externe gebruikers voor informatie en informatieverwerkende faciliteiten behoren bij beëindiging van hun dienstverband, contract of overeenkomst te worden verwijderd, en bij wijzigingen behoren ze te worden aangepast.	☐	☑	☐	☑	☑	
9.2.6 NEN7510	Toegangsrechten intrekken of aanpassen	Alle organisaties die persoonlijke gezondheidsinformatie verwerken moeten voor elke vertrekkende afdelings- of tijdelijke medewerker, derde-contractant of vrijwilliger zo snel mogelijk na beëindiging van het dienstverband of de werkzaamheden als contractant of vrijwilliger de toegangsrechten als gebruikers tot dergelijke informatie beëindigen.	☐	☑	☐	☑	☑	
9.3.1	Geheime authenticatie-informatie gebruiken	Van gebruikers behoort te worden verlangd dat zij zich bij het gebruiken van geheime authenticatie-informatie houden aan de praktijk van de organisatie.	☐	☑	☐	☑	☑	
9.4.1	Beperking toegang tot informatie	Toegang tot informatie en systeemfuncties van toepassingen behoort te worden beperkt in overeenstemming met het beleid voor toegangsbeveiliging.	☐	☑	☐	☑	☑	
9.4.1 NEN7510-deel-1	Beperking toegang tot informatie	Alle gezondheidsinformatiesystemen die persoonlijke gezondheids-informatie verwerken, moeten de identiteit van gebruikers vaststellen en dit moet worden gedaan door middel van authenticatie waarbij ten minste twee factoren betrokken worden.	☐	☑	☐	☑	☑	

Verklaring van Toepasselijkheid **OSSO B.V.**

Norm: **NEN7510-1:2017+A1:2020 NL**

Versie: **7.0**

Datum: 6 September 2021

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
9.4.1 NEN7510-deel-2	Beperking toegang tot informatie	De toegang tot functies van informatie- en toepassingssystemen in verband met het verwerken van persoonlijke gezondheidsinformatie moet geïsoleerd (en gescheiden) worden van de toegang tot informatieverwerkings-infrastructuur die geen verband houdt met het verwerken van persoonlijke gezondheidsinformatie.	☐	☑	☐	☑	☑	
9.4.2	Beveiligde inlogprocedures	Indien het beleid voor toegangsbeveiliging dit vereist, behoort toegang tot systemen en toepassingen te worden beheerst door een beveiligde inlogprocedure.	☐	☑	☐	☑	☑	
9.4.3	Systeem voor wachtwoordbeheer	Systemen voor wachtwoordbeheer behoren interactief te zijn en sterke wachtwoorden te waarborgen.	☐	☑	☐	☑	☑	
9.4.4	Speciale systeemhulpmiddelen gebruiken	Het gebruik van systeemhulpmiddelen die in staat zijn om beheersmaatregelen voor systemen en toepassingen te omzeilen behoort te worden beperkt en nauwkeurig te worden gecontroleerd.	☐	☑	☐	☑	☑	
9.4.5	Toegangsbeveiliging op programmabroncode	Toegang tot de programmabroncode behoort te worden beperkt.	☐	☑	☐	☑	☑	
10.1.1	Beleid inzake het gebruik van cryptografische beheersmaatregelen	Ter bescherming van informatie behoort een beleid voor het gebruik van cryptografische beheersmaatregelen te worden ontwikkeld en geïmplementeerd.	☐	☑	☐	☑	☑	
10.1.2	Sleutelbeheer	Met betrekking tot het gebruik, de bescherming en de levensduur van cryptografische sleutels behoort tijdens hun gehele levenscyclus een beleid te worden ontwikkeld en geïmplementeerd.	☐	☑	☐	☑	☑	
11.1.1	Fysieke beveiligingszone	Beveiligingszones behoren te worden gedefinieerd en gebruikt om gebieden te beschermen die gevoelige of essentiële informatie en informatie verwerkende faciliteiten bevatten.	☐	☑	☑	☑	☑	
11.1.1 NEN7510	Fysieke beveiligingszone	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gebruikmaken van beveiligde zones om gebieden te beschermen die informatieverwerkingsfaciliteiten bevatten die dergelijke gezondheidstoepassingen ondersteunen. Deze beveiligde gebieden moeten worden beschermd door passende beheersmaatregelen voor de fysieke toegang om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	☐	☑	☑	☑	☑	
11.1.2	Fysieke toegangsbeveiliging	Beveiligde gebieden behoren te worden beschermd door passende toegangsbeveiliging om ervoor te zorgen dat alleen bevoegd personeel toegang krijgt.	☐	☑	☑	☑	☑	
11.1.3	Kantoren, ruimten en faciliteiten beveiligen	Voor kantoren, ruimten en faciliteiten behoort fysieke beveiliging te worden ontworpen en toegepast.	☐	☑	☑	☑	☑	
11.1.4	Bescherming door bedreigingen van buitenaf	Tegen natuurrampen, kwaadwillige aanvallen of ongelukken behoort fysieke bescherming te worden ontworpen en toegepast.	☐	☑	☑	☑	☑	
11.1.5	Werken in beveiligde gebieden	Voor het werken in beveiligde gebieden behoren procedures te worden ontwikkeld en toegepast.	☐	☑	☐	☑	☑	
11.1.6	Laad- en loslocatie	Toegangspunten zoals laad- en loslocaties en andere punten waar onbevoegde personen het terrein kunnen betreden behoren te worden beheerst, en zo mogelijk te worden afgeschermd van informatie verwerkende faciliteiten om onbevoegde toegang te vermijden.	☐	☑	☑	☑	☑	
11.2.1	Plaatsing en bescherming van apparatuur	Apparatuur behoort zo te worden geplaatst en beschermd dat de risico's van bedreigingen en gevaren van buitenaf, alsook de kans op onbevoegde toegang worden verkleind.	☐	☑	☑	☑	☑	
11.2.2	Nutsvoorzieningen	Apparatuur behoort zo te worden beschermd tegen stroomuitval en andere verstoringen die worden veroorzaakt door ontregelingen in nutsvoorzieningen.	☐	☑	☑	☑	☑	
11.2.3	Beveiliging van bekabeling	Voedings- en telecommunicatiekabels voor het versturen van gegevens of die informatiediensten ondersteunen, behoren te worden beschermd tegen interceptie, verstoring of schade.	☐	☑	☑	☑	☑	
11.2.4	Onderhoud van apparatuur	Apparatuur behoort correct te worden onderhouden om de continue beschikbaarheid en integriteit ervan te waarborgen.	☐	☑	☐	☑	☑	
11.2.5	Verwijdering van bedrijfsmiddelen	Apparatuur, informatie en software behoren niet van de locatie te worden meegenomen zonder voorafgaande goedkeuring.	☐	☑	☐	☑	☑	
11.2.5 NEN7510	Verwijdering van bedrijfsmiddelen	Organisaties die uitrusting, gegevens of software voor het ondersteunen van een zorgtoepassing met persoonlijke gezondheidsinformatie leveren of gebruiken, mogen niet toestaan dat die uitrusting, gegevens of software van de locatie wordt of worden verwijderd of er binnen wordt of worden verplaatst zonder dat de organisatie hiervoor haar goedkeuring heeft gegeven.	☐	☑	☐	☑	☑	
11.2.6	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Bedrijfsmiddelen die zich buiten het terrein bevinden behoren te worden beveiligd, waarbij rekening behoort te worden gehouden met de verschillende risico's van werken buiten het terrein van de organisatie.	☐	☑	☐	☑	☑	

Verklaring van Toepasselijkheid **OSSO B.V.**

Norm: **NEN7510-1:2017+A1:2020 NL**

Versie: **7.0**

Datum: 6 September 2021

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
11.2.6 NEN7510	Beveiliging van apparatuur en bedrijfsmiddelen buiten het terrein	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten garanderen dat het eventuele gebruik buiten hun gebouw van medische apparaten die worden gebruikt om gegevens te registreren of te rapporteren, geautoriseerd is. Dit moet apparatuur omvatten die door werknemers op afstand wordt gebruikt, zelfs indien dit gebruik permanent is (d.w.z. waar het een kernaspect is van de rol van de werknemer, zoals het geval is bij ambulancepersoneel, therapeuten enz.)	☐	☐	☐	☐	☐	OSSO beschikt zelf niet over medische apparatuur.
11.2.7	Veilig verwijderen of hergebruiken van apparatuur	Alle onderdelen van de apparatuur die opslagmedia bevatten, behoren te worden geverifieerd om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.	☐	☑	☐	☑	☑	
11.2.7 NEN7510	Veilig verwijderen of hergebruiken van apparatuur	Organisaties die gezondheidsinformatie verwerken, moeten alle media met toepassingssoftware voor gezondheidsinformatie of persoonlijke gezondheidsinformatie erop veilig wissen of vernietigen als ze niet meer gebruikt hoeven te worden.	☐	☑	☐	☑	☑	
11.2.8	Onbeheerde gebruikersapparatuur	Gebruikers moeten ervoor zorgen dat onbeheerde apparatuur voldoende beschermd is.	☐	☑	☐	☑	☑	
11.2.9	`Clear-desk` en `clear-screen` beleid	Er behoort een `clear-desk`-beleid voor papieren documenten en verwijderbare opslagmedia en een `clear screen`-beleid voor informatie verwerkende faciliteiten te worden ingesteld.	☐	☑	☐	☑	☑	
12.1.1	Bedieningsprocedures en verantwoordelijkheden	Bedieningsprocedures behoren te worden gedocumenteerd en beschikbaar te worden gesteld aan alle gebruikers die ze nodig hebben.	☐	☑	☐	☑	☑	
12.1.2	Wijzigingsbeheer	Veranderingen in de organisatie, bedrijfsprocessen, informatie verwerkende faciliteiten en systemen die van invloed zijn op de informatiebeveiliging behoren te worden beheerst.	☐	☑	☐	☑	☑	
12.1.2 NEN7510	Wijzigingsbeheer	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de veranderingen aan informatieverwerkingsfaciliteiten en systemen die persoonlijke gezondheidsinformatie verwerken, door middel van een formeel en gestructureerd wijzigings-beheersproces beheersen om de gepaste beheersing van host-toepassingen en -systemen en de continuïteit van de cliëntenzorg te garanderen.	☐	☑	☐	☑	☑	
12.1.3	Capaciteitsbeheer	Het gebruik van middelen behoort te worden gemonitord en afgestemd en er behoren verwachtingen te worden opgesteld voor toekomstige capaciteitseisen om de vereiste systeemprestatie te waarborgen.	☐	☑	☐	☑	☑	
12.1.4	Scheiding van ontwikkel-, test en productieomgevingen	Ontwikkel-, test- en productieomgevingen behoren te worden gescheiden om het risico van onbevoegde toegang tot of veranderingen aan de productieomgeving te verlagen.	☐	☑	☐	☑	☑	
12.1.4 NEN7510	Scheiding van ontwikkel-, test en productieomgevingen	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten ontwikkel- en testomgevingen voor gezondheidsinformatiesystemen die dergelijke informatie verwerken (fysiek of virtueel) scheiden van operationele omgevingen waar die gezondheidsinformatiesystemen gehost worden. Er moeten regels voor het migreren van software van de ontwikkel- naar een operationele status worden gedefinieerd en gedocumenteerd door de organisatie die de betroffen toepassing(en) host.	☐	☑	☐	☑	☑	
12.2.1	Beheersmaatregelen tegen malware	Ter bescherming tegen malware behoren beheersmaatregelen voor detectie, preventie en herstel te worden geïmplementeerd in combinatie met passend bewustzijn van gebruikers.	☐	☑	☐	☑	☑	
12.2.1 NEN7510	Beheersmaatregelen tegen malware	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten gepaste preventie-, detectie- en respons-beheersmaatregelen implementeren om bescherming te bieden tegen kwaadaardige software, en passende bewustzijnstraining voor gebruikers implementeren.	☐	☑	☐	☑	☑	
12.3.1	Back-up van informatie	Regelmatig behoren back-upkopieën van informatie, software en systeemafbeeldingen te worden gemaakt en getest in overeenstemming meet een overeengekomen back-upbeleid.	☐	☑	☐	☑	☑	
12.3.1 NEN7510-deel-1	Back-up van informatie	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten back-ups maken van alle persoonlijke gezondheidsinformatie en deze in een fysiek beveiligde omgeving opslaan om te garanderen dat de informatie in de toekomst beschikbaar is.	☐	☑	☐	☑	☑	
12.3.1 NEN7510-deel-2	Back-up van informatie	Om de vertrouwelijkheid ervan te beschermen moeten er versleutelde back-ups worden gemaakt van persoonlijke gezondheidsinformatie.	☐	☑	☐	☑	☑	
12.4.1	Gebeurtenissen registreren	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.	☐	☑	☐	☑	☑	

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
12.4.2	Beschermen van informatie in logbestanden	Logfaciliteiten en informatie in logbestanden behoren te worden beschermd tegen vervalsing e onbevoegde toegang.	☑	☑	☐	☑	☑	
12.4.2 NEN7510	Beschermen van informatie in logbestanden	Auditverslagen moeten beveiligd zijn en niet gemanipuleerd kunnen worden. De toegang tot hulpmiddelen voor audits van systemen en audittrajecten moet worden beveiligd om misbruik of compromittering te voorkomen.	☑	☑	☐	☑	☑	
12.4.3	Logbestanden van beheerders en operators	Activiteiten van systeembeheerders en operators behoren te worden vastgelegd en de logbestanden te worden beschermd en regelmatig te worden beoordeeld.	☐	☑	☐	☑	☑	
12.4.4	Kloksynchronisatie	De klokken van alle relevante informatie verwerkende systemen binnen een organisatie behoren te worden gesynchroniseerd met één referentiebrontijd.	☐	☑	☐	☑	☑	
12.4.4 NEN7510	Kloksynchronisatie	Gezondheidsinformatiesystemen die tijdkritische activiteiten voor gedeelde zorg ondersteunen, moeten in tijdssynchronisatie-diensten voorzien om het traceren en reconstrueren van de tijdlijnen voor activiteiten waar vereist te ondersteunen.	☐	☑	☐	☑	☑	
12.5.1	Software installeren op operationele systemen	Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	☐	☑	☐	☑	☑	
12.6.1	Beheer van technische kwetsbaarheden	Om het op operationele systemen installeren van software te beheersen behoren procedures te worden geïmplementeerd.	☐	☑	☐	☑	☑	
12.6.2	Beperkingen voor het installeren van software	Voor het door gebruikers installeren van software behoren regels te worden vastgesteld en te worden geïmplementeerd.	☐	☑	☐	☑	☑	
12.7.1	Beheersmaatregelen betreffende audit van informatiesystemen	Auditeisen en -activiteiten die verificatie van uitvoeringssystemen met zich meebrengen, behoren zorgvuldig te worden gepland en afgestemd om bedrijfsprocessen zo min mogelijk te verstoren.	☐	☑	☐	☑	☑	
13.1.1	Beheersmaatregelen voor netwerken	Netwerken behoren te worden beheerd en beheerst om informatie in systemen en toepassingen te beschermen.	☐	☑	☐	☑	☑	
13.1.2	Beveiliging van netwerkdiensten	Beveiligingsdiensten, dienstverleningsniveaus en beheereisen voor alle netwerkdiensten (aansluitingen, particuliere netwerkdiensten) behoren te worden geïdentificeerd en opgenomen in overeenkomsten betreffende netwerkdiensten. Dit geldt zowel voor diensten die intern worden geleverd als voor uitbestede diensten.	☐	☑	☐	☑	☑	
13.1.3	Scheiding in netwerkdiensten	Groepen van netwerkdiensten, -gebruikers en -systemen behoren te worden gescheiden.	☐	☑	☐	☑	☑	
13.2.1	Beleid en procedure voor informatietransport	Ter bescherming van het informatietransport, dat via alle soorten communicatiefaciliteiten verloopt, behoren formele beleidsregels, procedures en beheersmaatregelen voor transport van kracht te zijn.	☐	☑	☐	☑	☑	
13.2.2	Overeenkomsten over informatietransport (transport intern/extern)	Overeenkomsten behoren betrekking te hebben op het beveiligd transporteren van bedrijfsinformatie tussen de organisatie en externe partijen.	☐	☑	☐	☑	☑	
13.2.3	Elektronische berichten	Informatie die is opgenomen in elektronische berichten behoort passend te worden beveiligd.	☑	☑	☐	☑	☑	
13.2.4	Overeenkomsten over informatietransport	Eisen voor vertrouwelijkheids-geheimhoudingsovereenkomsten, die de behoeften van de organisatie betreffende het beschermen van informatie weerspiegelen, behoren te worden vastgesteld, regelmatig te worden beoordeeld en gedocumenteerd.	☑	☑	☐	☑	☑	
13.2.4 NEN7510	Overeenkomsten over informatietransport	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten beschikken over een vertrouwelijkheidsovereenkomst waarin de vertrouwelijke aard van deze informatie staat omschreven. De overeenkomst moet van toepassing zijn op al het personeel dat toegang heeft tot gezondheidsinformatie.	☐	☑	☐	☑	☑	
14.1.1	Analyse en specificatie van informatiebeveiligingseisen	De eisen die verband houden met informatiebeveiliging behoren te worden opgenomen in de eisen voor nieuwe informatiesystemen of voor uitbreidingen van bestaande informatiesystemen.	☐	☑	☐	☑	☑	
14.1.1.1 NEN7510	Analyse en specificatie van informatiebeveiligingseisen	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten: a) zekerstellen dat elke cliënt op unieke wijze kan worden geïdentificeerd binnen het systeem; b) in staat zijn dubbele of meerdere registraties samen te voegen indien wordt vastgesteld dat er onbedoeld meer registraties voor dezelfde cliënt zijn aangemaakt, of tijdens een medisch noodgeval.	☐	☐	☐	☐	☐	Als subverwerker ligt dit buiten de verantwoordelijkheden van OSSO.
14.1.1.2 NEN7510	Analyse en specificatie van informatiebeveiligingseisen	Gezondheidsinformatiesystemen die persoonlijke gezondheidsinformatie verwerken, moeten voorzien in persoonsidentificatie-informatie die zorgverleners helpt bevestigen dat de opgevraagde elektronische gezondheidsregistratie overeenkomt met de cliënt die wordt behandeld.	☐	☐	☐	☐	☐	Als subverwerker ligt dit buiten de verantwoordelijkheden van OSSO.
14.1.2	Toepassingen op openbare netwerken beveiligen	Informatie die deel uitmaakt van uitvoeringsdiensten en die via openbare netwerken wordt uitgewisseld, behoort te worden beschermd tegen frauduleuze activiteiten.	☐	☑	☐	☑	☑	

Verklaring van Toepasselijkheid **OSSO B.V.**

Norm: **NEN7510-1:2017+A1:2020 NL**

Versie: **7.0**

Datum: 6 September 2021

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
14.1.3	Transacties van toepassingen beschermen	Informatie die deel uitmaakt van transacties van toepassingen behoort te worden beschermd ter voorkoming van onvolledige overdracht, foutieve routering, onbevoegd wijzigen of onbevoegd openbaar maken van berichten.	☐	☑	☐	☑	☑	
14.1.3.1 NEN7510	Transacties van toepassingen beschermen	Openbaar beschikbare gezondheidsinformatie (niet zijnde persoonlijke gezondheidsinformatie) moet worden gearchiveerd. De integriteit van openbaar beschikbare gezondheidsinformatie moet worden beschermd om onbevoegde wijzigingen te voorkomen. De bron (auteurschap) van openbaar beschikbare gezondheidsinformatie moet worden vermeld en de integriteit ervan moet worden beschermd.	☐	☐	☐	☐	☐	Als subverwerker ligt dit buiten de verantwoordelijkheden van OSSO.
14.2.1	Beleid voor beveiligd ontwikkelen	Voor het ontwikkelen van software en systemen behoren regels te worden vastgesteld en op ontwikkelactiviteiten binnen de organisatie te worden toegepast.	☐	☑	☐	☑	☑	
14.2.2	Procedure voor wijzigingsbeheer met betrekking tot systemen	Wijzigingen aan systemen binnen de levenscyclus van de ontwikkeling behoren te worden beheerst door het gebruik van formele procedures voor wijzigingsbeheer.	☐	☑	☐	☑	☑	
14.2.3	Technische beoordeling van toepassingen na wijzigingen besturingsplatform	Als besturingsplatforms zijn veranderd behoren bedrijf kritische toepassingen te worden beoordeeld en getest om te waarborgen dat er geen nadelige impact is op de activiteiten of beveiliging van de organisatie.	☐	☑	☐	☑	☑	
14.2.4	Beperkingen op wijzigingen aan softwarepakketten	Wijzigingen aan softwarepakketten behoren te worden ontraden, beperkt tot noodzakelijke veranderingen en daar waar van toepassingen strikt te worden gedocumenteerd en gecontroleerd/getoetst.	☐	☑	☐	☑	☑	
14.2.5	Principes voor engineering van beveiligde systemen	Principes behoren te worden vastgelegd, gedocumenteerd, onderhouden en toegepast voor alle verrichtingen betreffende het implementeren van informatiesystemen.	☐	☑	☐	☑	☑	
14.2.6	Beveiligde ontwikkelomgeving	Organisatie behoren beveiligde ontwikkelomgevingen vast te stellen en passend te beveiligen voor verrichtingen op het gebied van systeemontwikkeling en integratie die betrekking heeft op de gehele levenscyclus van de systeemontwikkeling.	☐	☑	☐	☑	☑	
14.2.7	Uitbestede systeemontwikkeling	Uitbestede systeemontwikkeling behoort onder supervisie te staan van en te worden gemonitord door de organisatie.	☐	☑	☐	☑	☑	
14.2.8	Testen van systeembeveiliging	Tijdens ontwikkelactiviteiten behoort de beveiligingsfunctionaliteit te worden getest.	☐	☑	☐	☑	☑	
14.2.9	Systeemacceptatietests	Voor nieuwe informatiesystemen, upgrades en nieuwe versies behoren programma's voor het uitvoeren van acceptatietests en gerelateerde criteria te worden vastgesteld.	☐	☑	☐	☑	☑	
14.2.9 NEN7510	Systeemacceptatietests	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten acceptatiecriteria vaststellen voor geplande nieuwe informatiesystemen, upgrades en nieuwe versies. Voorafgaand aan acceptatie moeten ze geschikte testen van het systeem uitvoeren. [A1> Klinische gebruikers moeten worden betrokken bij het testen van klinisch relevante systeemelementen.<A1]	☐	☑	☐	☑	☑	
14.3.1	Bescherming van testgegevens	Testgegevens behoren zorgvuldig te worden gekozen, beschermd en gecontroleerd.	☐	☑	☐	☑	☑	
15.1.1	Informatiebeveiligingsbeleid voor leveranciers	Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie te worden overeengekomen en gedocumenteerd.	☐	☑	☐	☑	☑	
15.1.1 NEN7510	Informatiebeveiligingsbeleid voor leveranciers	Organisaties die gezondheidsinformatie verwerken moeten de risico's in verband met toegang door externe partijen tot deze systemen of gegevens die zij bevatten, beoordelen en vervolgens beveiligings-beheersmaatregelen implementeren die bij het geïdentificeerde risiconiveau en de toegepaste technologieën passen.	☐	☑	☐	☑	☑	
15.1.2	Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	Alle relevante informatiebeveiligingseisen behoren te worden vastgesteld en overeengekomen met elke leverancier die toegang heeft tot IT-infrastructuurelementen ten behoeve van de informatie van de organisatie, of deze verwerkt, opslaat, communiceert of biedt.	☐	☑	☐	☑	☑	
15.1.3	Toeleverancierskeketen van informatie- en communicatietechnologie	Overeenkomsten met leveranciers behoren eisen te bevatten die betrekking hebben op de informatiebeveiligingsrisico's in verband met de toeleverancierskeketen van de diensten en producten op het gebied van informatie- en communicatietechnologie.	☐	☑	☐	☑	☑	
15.2.1	Monitoring en beoordeling van dienstverlening van leveranciers	Met de leverancier behoren de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie te worden overeengekomen en gedocumenteerd.	☐	☑	☐	☑	☑	
15.2.2	Beheer van veranderingen in dienstverlening van leveranciers	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	☐	☑	☐	☑	☑	

Verklaring van Toepasselijkheid **OSSO B.V.**

Norm: **NEN7510-1:2017+A1:2020 NL**

Versie: **7.0**

Datum: 6 September 2021

Nummer	Onderwerp	Beheersmaatregel	Wetgeving	Risicoanalyse	Uitbesteed	Van toepassing	Geïmplementeerd	Reden indien niet van toepassing
16.1.1	Verantwoordelijkheden en procedures	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	☐	☑	☐	☑	☑	
16.1.2	Rapportage van informatiebeveiligingsgebeurtenissen	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	☐	☑	☐	☑	☑	
16.1.2 NEN7510	Rapportage van informatiebeveiligingsgebeurtenissen	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten verantwoordelijkheden en procedures met betrekking tot het managen van beveiligingsincidenten vaststellen:	☐	☑	☐	☑	☑	
16.1.3	Rapportage van zwakke plekken in de informatiebeveiliging	Melden van zwakke plekken door medewerkers bij waargenomen of vermeende zwakke plekken.	☐	☑	☐	☑	☑	
16.1.4	Beoordeling van en besluitvorming over informatiebeveiligingsgebeurtenissen	Informatiebeveiligingsgebeurtenissen behoren te worden beoordeeld en er behoort te worden geoordeeld of zij moeten worden geclassificeerd als informatiebeveiligingsincident.	☐	☑	☐	☑	☑	
16.1.5	Respons op informatiebeveiligingsincidenten	Op informatiebeveiligingsincidenten behoort te worden gereageerd in overeenstemming met de gedocumenteerde procedures.	☑	☑	☐	☑	☑	
16.1.6	Lering uit informatiebeveiligingsincidenten	Kennis die is verkregen uit informatiebeveiligingsincidenten behoort te worden gebruikt om de waarschijnlijkheid of impact van toekomstige incidenten te verkleinen.	☐	☑	☐	☑	☑	
16.1.7	Verzamelen van bewijsmateriaal	De organisatie dient procedures te definiëren en toe te passen voor het identificeren, verzamelen, verkrijgen en bewaren van informatie die als bewijs kan dienen.	☑	☑	☐	☑	☑	
17.1.1	Informatiebeveiligingscontinuïteit plannen	De organisatie behoort haar eisen voor informatiebeveiliging en voor de continuïteit van het informatiebeveiligingsbeheer in ongunstige situaties, bijv. een crisis of een ramp, vast te stellen.	☑	☑	☐	☑	☑	
17.1.2	Informatiebeveiligingscontinuïteit implementeren	De organisatie behoort de processen, procedures en beheersmaatregelen vast te stellen, te implementeren, en te handhaven om het vereiste niveau van continuïteit voor informatiebeveiliging tijdens een ongunstige situatie te waarborgen.	☑	☑	☐	☑	☑	
17.1.3	Informatiebeveiligingscontinuïteit verifiëren, beoordelen en evalueren	De organisatie behoort ten behoeve van informatiebeveiligingscontinuïteit vastgestelde en geïmplementeerde beheersmaatregelen regelmatig te verifiëren om te waarborgen dat ze deugdelijk en doeltreffend zijn tijdens ongunstige situaties.	☑	☑	☐	☑	☑	
17.2.1	Beschikbaarheid van informatie verwerkende faciliteiten	Informatieverwerkende faciliteiten behoren met voldoende redundantie te worden geïmplementeerd om aan beschikbaarheidseisen te voldoen.	☐	☑	☐	☑	☑	
18.1.1	Vaststellen van toepasselijke wetgeving en contractuele eisen	Alle relevante wettelijke statutaire, regelgevende, contractuele eisen en de aanpak van de organisatie om aan deze eisen te voldoen behoren voor elk informatiesysteem en de organisatie expliciet te worden vastgesteld, gedocumenteerd en actueel gehouden.	☑	☑	☐	☑	☑	
18.1.2	Intellectueel-eigendomsrecht	Om de naleving van wettelijke, regelgevende en contractuele eisen in verband met intellectuele eigendomsrechten en het gebruik van eigendomssoftwareproducten te waarborgen behoren passende procedures te worden geïmplementeerd.	☑	☑	☐	☑	☑	
18.1.3	Beschermen van registraties	Registraties behoren in overeenstemming met wettelijke, regelgevende, contractuele en bedrijfseisen te worden beschermd tegen verlies, vernietiging, vervalsing, onbevoegde toegang en onbevoegde vrijgave.	☑	☑	☐	☑	☑	
18.1.4	Privacy en bescherming van persoonsgegevens	Privacy en bescherming van persoonsgegevens behoren, voor zover van toepassing, te worden gewaarborgd in overeenstemming met relevante wet- en regelgeving.	☑	☑	☐	☑	☑	
18.1.4 NEN7510-deel-1	Privacy en bescherming van persoonsgegevens	Organisaties die persoonlijke gezondheidsinformatie verwerken, moeten de geïnformeerde toestemming van cliënten beheren.	☐	☐	☐	☐	☐	Als subverwerker ligt dit buiten de verantwoordelijkheden van OSSO.
18.1.4 NEN7510-deel-2	Privacy en bescherming van persoonsgegevens	Waar mogelijk moet geïnformeerde toestemming van cliënten worden verkregen voordat persoonlijke gezondheidsinformatie per e-mail, fax of telefonisch wordt gecommuniceerd of anderszins bekend wordt gemaakt aan partijen buiten de zorginstelling.	☐	☐	☐	☐	☐	Als subverwerker ligt dit buiten de verantwoordelijkheden van OSSO.
18.1.5	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Cryptografische beheersmaatregelen behoren te worden toegepast in overeenstemming met alle relevante overeenkomsten, wet- en regelgeving.	☑	☑	☐	☑	☑	
18.2.1	Onafhankelijke beoordeling van informatiebeveiliging	De aanpak van de organisatie ten aanzien van het beheer van informatiebeveiliging en de implementatie hiervan behoort periodiek onafhankelijk en met geplande tussenpozen te worden beoordeeld.	☐	☑	☑	☑	☑	
18.2.2	Naleving van beveiligingsbeleid en -normen	[A1>Leidinggevenden moeten regelmatig de naleving van de informatieverwerking en -procedures binnen hun <A1] verantwoordelijkheidsgebied te beoordelen aan de hand van desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.	☑	☑	☐	☑	☑	
18.2.3	Beoordeling van technische naleving	Informatiesystemen behoren regelmatig te worden beoordeeld op naleving van de beleidsregels en normen van de organisatie voor informatiebeveiliging.	☐	☑	☐	☑	☑	