Verklaring van toepasselijkheid

Parantion Groep B.V.

NEN7510:2011 - NL

Inhoud

1. Inleiding

Dit document omvat de Verklaring van Toepasselijkheid (VVT) ten behoeve van de certificering voor de NEN 7510:2011 standaard. De doelstelling van dit document is het identificeren van de toepasselijke beheersmaatregelen welke geïmplementeerd dienen te zijn om de bedreigingen tegen Parantion en haar bedrijfsprocessen te controleren en te managen.

De beheersmaatregelen zijn geïdentificeerd op basis van de NEN 2710:2011 standaard opgenomen beheersmaatregelen van de norm. Per beheersmaatregel wordt de toepasselijkheid weergegeven. Voor de van toepassing zijnde beheersmaatregel wordt verwezen naar de gedefinieerde NEN 7510:2011 'best practices' richtlijnen. Deze richtlijnen zijn waar mogelijk specifiek gemaakt voor de bedrijfsprocessen van Parantion. Indien een beheersmaatregel niet van toepassing is, wordt hiervoor een verklaring gegeven.

In dit document wordt de scope en reikwijdte van de certificering beschreven, alsmede de organisatiestructuur en missie en visie van Parantion .

2. Directieverklaring

De Directie van Parantion Groep B.V. verklaart hierbij de in deze VVT vermelde maatregelen bekrachtigd in relatie tot de uitgevoerde risicoanalyses en accepteert het restrisico van niet genomen maatregelen.

Deventer, juni 2016

Roel Smabers

3. Scope

Het ontwikkelen, implementeren, adviseren en leveren van ondersteuning en support op de software applicaties Scorion en Easion (SAAS/Private Cloud) vanuit het kantoor in Deventer en het datacenter in Hengelo. Dit is conform de verklaring van toepasselijkheid versie 3.0
dd. 27 juni 2016.

4. Verklaring van Toepasselijkheid - Maatregelen Selectie NEN7510:2011 - NL

De Verklaring van Toepasselijkheid beschrijft welke maatregelen uit alle NEN 7510 domeinen wel en niet van toepassing zijn. In de tabel “Controls van toepassing” wordt de volgende informatie weergegeven:

4.1 Van toepassing zijnde beheersmaatregelen

Maatregel nr.	Maatregel omschrijving	Reden van toepassing	Geïmple-menteerd
4. Aanpak van de informatiebeveiliging			
4.1	Management systeem voor informatiebeveiliging	Baseline	Ja
4.2 Directieverantwoordelijkheid			
4.2.1	Toewijzen verantwoordelijkheden	Baseline	Ja
4.2.2	Actieve betrokkenheid	Baseline	Ja
4.2.3	Stuurgroep	Baseline	Ja
4.3 PLAN: het ISMS vaststellen			
4.3.1	Plan vaststellen van het ISMS	Baseline	Ja
4.4 DO: het ISMS implementeren en uitvoeren			
4.4.1	Implementeren en uitvoeren ISMS	Baseline	Ja
4.4.2	Beschikbaar stellen van middelen	Baseline	Ja
4.4.3	Training, bewustzijn en bekwaamheid voor het ISMS	Risicoanalyse	Ja
4.5 CHECK: het ISMS monitoren en beoordelen			
4.5.1	Het ISMS monitoren en beoordelen	Baseline	Ja
4.5.2	Interne ISMS-audits	Baseline	Ja
4.5.3	Directiebeoordeling van het ISMS	Baseline	Ja
4.6 ACT: het ISMS onderhouden en verbeteren			
4.6.1	Algemeen	Baseline	Ja
4.6.2	Continue verbetering	Baseline	Ja
4.6.3	Corrigerende maatregelen	Baseline	Ja
4.6.4	Preventieve maatregelen	Baseline	Ja
4.7 Documentatie van het ISMS			
4.7.1	Algemeen	Baseline	Ja
4.7.2	Beheersing van documenten	Baseline	Ja
4.7.3	Beheersing van registraties	Baseline	Ja
5. Beveiligingsbeleid			
5.1 Informatiebeveiligingsbeleid			
5.1.1	Beleidsdocument voor informatiebeveiliging	Baseline	Ja
5.1.2	Beoordeling van het informatiebeveiligingsbeleid	Baseline	Ja
6. Organisatie van informatiebeveiliging			
6.1 Interne organisatie			
6.1.1	Betrokkenheid van de directie bij informatiebeveiliging	Baseline	Ja
6.1.2	Coördinatie van informatiebeveiliging	Baseline	Ja
6.1.4	Goedkeuringsproces voor middelen voor de informatievoorziening	Baseline	Ja
6.1.5	Geheimhoudingsovereenkomst	Risicoanalyse	Ja
6.1.6	Contact met overheidsinstanties	Wet- en regelgeving	Ja
6.1.7	Contact met speciale belangengroepen	Risicoanalyse	Ja
6.1.8	Onafhankelijke beoordeling van informatiebeveiliging	Baseline	Ja
6.2 Externe partijen			
6.2.1	Identificatie van risico's die betrekking hebben op externe partijen	Risicoanalyse	Ja
6.2.2	Beveiliging in de omgang met klanten	Risicoanalyse	Ja
6.2.3	Beveiliging in overeenkomsten met een derde partij	Risicoanalyse	Ja

7. Beheer van bedrijfsmiddelen			
7.1 Verantwoordelijkheid voor bedrijfsmiddelen			
7.1.1	Inventarisatie van bedrijfsmiddelen	Risicoanalyse	Ja
7.1.2	Verantwoordelijken voor de bedrijfsmiddelen	Risicoanalyse	Ja
7.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Risicoanalyse	Ja
7.2 Classificatie van informatie			
7.2.1	Richtlijnen voor classificatie	Risicoanalyse	Ja
7.2.2	Labeling en verwerking van informatie	Risicoanalyse	Ja
8. Personeel			
8.1 Voorafgaand aan het dienstverband			
8.1.1	Rollen en verantwoordelijkheden	Risicoanalyse	Ja
8.1.2	Screening	Risicoanalyse	Ja
8.2 Tijdens het dienstverband			
8.2.1	Directieverantwoordelijkheid	Risicoanalyse	Ja
8.2.3	Disciplinaire maatregelen	Risicoanalyse	Ja
8.3 Beëindiging of wijziging van dienstverband			
8.3.1	Beëindiging van verantwoordelijkheden	Risicoanalyse	Ja
8.3.2	Retournering van bedrijfsmiddelen	Risicoanalyse	Ja
8.3.3	Intrekken van toegangsrechten	Risicoanalyse	Ja
9. Fysieke beveiliging en beveiliging van de omgeving			
9.1 Beveiligde ruimten			
9.1.2	Fysieke toegangsbeveiliging	Risicoanalyse	Ja
9.1.3	Beveiliging van kantoren, ruimten en faciliteiten	Risicoanalyse	Ja
9.1.4	Bescherming tegen bedreigingen van buitenaf	Risicoanalyse	Ja
9.1.5	Werken in beveiligde ruimten	Risicoanalyse	Ja
9.1.6	Openbare toegang en gebieden voor laden en lossen	Risicoanalyse	Ja
9.2 Beveiliging van apparatuur			
9.2.1	Plaatsing en bescherming van apparatuur	Risicoanalyse	Ja
9.2.2	Nutsvoorzieningen	Risicoanalyse	Ja
9.2.3	Beveiliging van kabels	Risicoanalyse	Ja
9.2.4	Onderhoud van apparatuur	Risicoanalyse	Ja
9.2.6	Veilig verwijderen of hergebruiken van apparatuur	Risicoanalyse	Ja
9.2.7	Verwijdering van bedrijfseigendommen	Risicoanalyse	Ja
10. Beheer van communicatie- en bedieningsprocessen			
10.1 Bedieningsprocedures en verantwoordelijkheden			
10.1.1	Gedocumenteerde bedieningsprocedures	Risicoanalyse	Ja
10.1.2	Wijzigingsbeheer	Risicoanalyse	Ja
10.1.3	Functiescheiding	Risicoanalyse	Ja
10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie	Risicoanalyse	Ja
10.2 Beheer van de dienstverlening door een derde partij			
10.2.1	Dienstverlening	Risicoanalyse	Ja
10.2.2	Controle en beoordeling van dienstverlening door een derde partij	Risicoanalyse	Ja
10.2.3	Beheer van wijzigingen in dienstverlening door een derde partij	Risicoanalyse	Ja
10.3 Systeemplanning en acceptatie			
10.3.1	Capaciteitsbeheer	Risicoanalyse	Ja
10.3.2	Systeemacceptatie	Risicoanalyse	Ja
10.4 Bescherming tegen kwaadaardige programmatuur en 'mobile code'			
10.4.1	Maatregelen tegen kwaadaardige programmatuur	Risicoanalyse	Ja
10.4.2	Maatregelen tegen 'mobile code'	Risicoanalyse	Ja
10.5	Back-up en herstel	Risicoanalyse	Ja

10.6 Beheer van netwerkbeveiliging			
10.6.1	Maatregelen voor netwerken	Risicoanalyse	Ja
10.6.2	Beveiliging van netwerkdiensten	Risicoanalyse	Ja
10.7 Behandeling van media			
10.7.1	Beheer van verwijderbare media	Risicoanalyse	Ja
10.7.2	Verwijdering van media	Risicoanalyse	Ja
10.7.4	Beveiliging van systeemdocumentatie	Risicoanalyse	Ja
10.8 Uitwisseling van informatie			
10.8.1	Beleid en procedures voor informatie-uitwisseling	Risicoanalyse	Ja
10.8.2	Uitwisselingsovereenkomsten	Risicoanalyse	Ja
10.8.3	Fysiek transport van media	Risicoanalyse	Ja
10.8.4	Elektronische berichtenuitwisseling	Risicoanalyse	Ja
10.8.5	Systemen voor bedrijfsinformatie	Risicoanalyse	Ja
10.10 Controle			
10.10.1	Aanmaken audit-logbestanden	Risicoanalyse	Ja
10.10.2	Controle van systeemgebruik	Risicoanalyse	Ja
10.10.4	Logbestanden van administrators en operators	Risicoanalyse	Ja
10.10.5	Registratie van storingen	Risicoanalyse	Ja
11. Toegangsbeveiliging			
11.2 Beheer van toegangsrechten van gebruiker			
11.2.2	Beheer van speciale bevoegdheden	Risicoanalyse	Ja
11.2.3	Beheer van gebruikerswachtwoorden	Risicoanalyse	Ja
11.2.4	Beoordeling van toegangsrechten van gebruikers	Risicoanalyse	Ja
11.3 Verantwoordelijkheden van gebruikers			
11.3.1	Gebruik van wachtwoorden	Risicoanalyse	Ja
11.3.2	Onbeheerde gebruikersapparatuur	Risicoanalyse	Ja
11.3.3	'Clear desk'- en 'clear screen'-beleid	Risicoanalyse	Ja
11.4 Toegangsbeheersing voor netwerken			
11.4.1	Beleid ten aanzien van het gebruik van netwerkdiensten	Risicoanalyse	Ja
11.4.2	Authenticatie van gebruikers bij externe verbindingen	Risicoanalyse	Ja
11.4.3	Identificatie van netwerkapparatuur	Risicoanalyse	Ja
11.4.4	Bescherming op afstand van poorten voor diagnose en configuratie	Risicoanalyse	Ja
11.4.5	Scheiding van netwerken	Risicoanalyse	Ja
11.4.6	Beheersmaatregelen voor netwerkverbindingen	Risicoanalyse	Ja
11.4.7	Beheersmaatregelen voor netwerkrouting	Risicoanalyse	Ja
11.5 Toegangsbeveiliging voor besturingssystemen			
11.5.1	Beveiligde inlogprocedures	Risicoanalyse	Ja
11.5.2	Gebruikersidentificatie en authenticatie	Risicoanalyse	Ja
11.5.3	Systemen voor wachtwoordbeheer	Risicoanalyse	Ja
11.5.4	Gebruik van systeemhulpmiddelen	Risicoanalyse	Ja
11.5.5	Time-out van sessies	Risicoanalyse	Ja
11.5.6	Beperking van verbindingstijd	Risicoanalyse	Ja
11.6 Toegangsbeheersing voor toepassingen en informatie			
11.6.1	Beheersen van toegang tot informatie	Risicoanalyse	Ja
11.6.2	Isoleren van gevoelige systemen	Risicoanalyse	Ja
11.7 Draagbare computers en telewerken			
11.7.1	Draagbare computers en communicatievoorzieningen	Risicoanalyse	Ja
11.7.2	Telewerken	Risicoanalyse	Ja
12. Verwerving, ontwikkeling en onderhoud van informatiesystemen			
12.1 Beveiligingseisen voor informatiesystemen			
12.1.1	Analyse en specificatie van beveiligingseisen	Risicoanalyse	Ja

12.2 Correcte verwerking in toepassingen			
12.2.2	Beheersing van interne gegevensverwerking	Risicoanalyse	Ja
12.2.3	Integriteit van berichten	Risicoanalyse	Ja
12.3 Cryptografische beheersmaatregelen			
12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	Risicoanalyse	Ja
12.3.2	Sleutelbeheer	Risicoanalyse	Ja
12.4 Beveiliging van systeembestanden			
12.4.1	Beheersing van operationele programmatuur	Risicoanalyse	Ja
12.4.2	Bescherming van testdata	Risicoanalyse	Ja
12.4.3	Toegangsbeheersing voor broncode van programmatuur	Risicoanalyse	Ja
12.5 Beveiliging bij ontwikkelings- en ondersteuningsprocessen			
12.5.1	Procedures voor wijzigingsbeheer	Risicoanalyse	Ja
12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem	Risicoanalyse	Ja
12.5.3	Restricties op wijzigingen in programmatuurpakketten	Risicoanalyse	Ja
12.5.4	Informatielekken	Risicoanalyse	Ja
12.6 Beheer van technische kwetsbaarheden			
12.6.1	Beheersing van technische kwetsbaarheden	Risicoanalyse	Ja
13. Beheer van informatiebeveiligingsincidenten			
13.1 Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken			
13.1.1	Rapportage van informatiebeveiligingsgebeurtenissen	Baseline	Ja
13.1.2	Rapportage van zwakke plekken in de beveiliging	Baseline	Ja
13.2 Beheer van informatiebeveiligingsincidenten en verbeteringen			
13.2.1	Verantwoordelijkheden en procedures	Baseline	Ja
13.2.2	Leren van informatiebeveiligingsincidenten	Baseline	Ja
13.2.3	Verzamelen van bewijsmateriaal	Baseline	Ja
14. Bedrijfscontinuïteitsbeheer			
14.1 Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer			
14.1.1	Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer	Baseline	Ja
14.1.2	Bedrijfscontinuïteit en risicobeoordeling	Baseline	Ja
14.1.3	Continuïteitsplannen en informatievoorziening	Baseline	Ja
14.1.4	Kader voor de bedrijfscontinuïteitsplanning	Baseline	Ja
14.1.5	Testen, onderhoud en herbeoordeling van bedrijfscontinuïteitsplannen	Baseline	Ja
15. Naleving			
15.1 Naleving van wettelijke voorschriften			
15.1.1	Identificatie van toepasselijke wetgeving	Baseline	Ja
15.1.2	Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)	Baseline	Ja
15.1.3	Bescherming van bedrijfsdocumenten	Risicoanalyse	Ja
15.1.5	Voorkomen van misbruik van IT-voorzieningen	Baseline	Ja
15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Risicoanalyse	Ja
15.2 Naleving van beveiligingsbeleid en normen en technische naleving			
15.2.1	Naleving van beveiligingsbeleid en normen	Baseline	Ja
15.2.2	Controle op technische naleving	Baseline	Ja
15.3 Overwegingen bij audits van informatiesystemen			
15.3.1	Beheersmaatregelen voor audits van informatiesystemen	Baseline	Ja
15.3.2	Bescherming van audithulpmiddelen voor audits van informatiesystemen	Baseline	Ja

4.2 Niet van toepassing zijnde maatregelen

Maatregel nr.	Maatregel omschrijving	Reden niet van toepassing	Geïmple-menteerd
6.1.3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging	Parantion verwerkt geen patiëntgegevens, er hoeft binnen de organisatie geen verantwoordelijke voor aangewezen te worden.	Nee
8.1.3	Arbeidsvoorwaarden	Parantion verwerkt geen patiëntgegevens. Geheimhouding is ingeregeld via ISO 27001 standaarden met daarbij rekening houdend met de WBP.	Nee
8.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Parantion verwerkt geen patiëntgegevens. Opleiding bewustwording en training mbt informatiebeveiliging en WBP zijn ingeregeld volgens ISO 27001.	Nee
9.1.1	Fysieke beveiliging van de omgeving	Parantion verwerkt geen patiëntgegevens en slaat deze dus ook niet fysiek op.	Nee
9.2.5	Beveiliging van apparatuur buiten het terrein	Parantion werkt niet met medische apparatuur.	Nee
10.5.1	Reservekopieën (back-ups)	Parantion verwerkt geen patiëntgegevens, Back-up beleid in ingeregeld volgens ISO:27001.	Nee
10.7.3	Procedures voor de behandeling van informatie	Parantion verwerkt geen patiëntgegevens. Media en fysieke informatiedragers zijn geregeld ingeregeld volgens ISO:27001.	Nee
10.9.1	E-commerce	Parantion levert geen applicatie service over een publiek netwerk.	Nee
10.9.2	Onlinetransacties	Parantion heeft geen mogelijkheid om online transacties uit te voeren.	Nee
10.9.3	Openbaar beschikbare informatie	Parantion verwerkt geen openbaar beschikbare zorginformatie.	Nee
10.10.3	Bescherming van informatie in logbestanden	Parantion verwerkt geen patiëntgegevens	Nee
10.10.6	Synchronisatie van systeemklokken	Parantion faciliteert geen tijd kritische zorgactiviteiten.	Nee
11.1.1	Toegangsbeleid	Parantion verwerkt geen patiëntgegevens	Nee
11.2.1	Registratie van gebruikers	Parantion verwerkt geen patiëntgegevens. Gebruikersregistratie is ingeregeld via ISO:27001.	Nee
12.2.1	Validatie van invoergegevens	Parantion verwerkt geen patiëntgegevens en maakt ook geen gebruik van patiënt identificatie.	Nee
12.2.4	Validatie van uitvoergegevens	Parantion verwerkt geen patiëntgegevens en faciliteert geen applicatie EPD.	Nee
12.5.5	Uitbestede ontwikkeling van programmatuur	Parantion besteedt geen ontwikkeling van apparatuur uit	Nee
15.1.4	Bescherming van gegevens en geheimhouding van persoonsgegevens	Parantion verwerkt geen patiëntgegevens en hoeft hiervoor dus ook geen toestemming van de patiënt voor te vragen.	Nee