IPS • Verklaring van Toepasselijkheid NEN 7510
v 1.3 | 09-08-2017

Index: WE: Wettelijke Eis, **CE**: Contractuele Eis, **BR**: Business Requirements/Best Practice), **RA**: Risico Analyse

Nr.	Doelstelling en maatregel NEN 7510:2011	Geselecteerd & Geïmplementeerd Ja/Nee	Onderbouwing (indien niet geselecteerd)	Reden van selectie (zie index) WE	CE	BR/BP	RA
5	**Beveiligingsbeleid**						
5.1	**Informatiebeveiligingsbeleid**						
5.1.1	Beleidsdocument voor informatiebeveiliging	Ja				■	
5.1.2	Beoordeling van het informatiebeveiligingsbeleid	Ja				■	
6	**Organisatie van informatiebeveiliging**						
6.1	**Interne organisatie**						
6.1.1	Betrokkenheid van de directie bij informatiebeveiliging	Ja				■	
6.1.2	Coördinatie van informatiebeveiliging	Ja				■	
6.1.3	Toewijzing van verantwoordelijkheden voor informatiebeveiliging	Ja				■	■
6.1.4	Goedkeuringsproces voor middelen voor de informatievoorziening	Ja				■	
6.1.5	Geheimhoudingsovereenkomst	Ja			■		
6.1.6	Contact met overheidsinstanties	Ja		■			
6.1.7	Contact met speciale belangengroepen	Ja				■	
6.1.8	Onafhankelijke beoordeling van informatiebeveiliging	Ja				■	
6.2	**Externe partijen**						
6.2.1	Identificatie van risico's die betrekking hebben op externe partijen	Ja				■	■
6.2.2	Beveiliging in de omgang met klanten	Ja				■	■
6.2.3	Beveiliging in overeenkomsten met een derde partij	Ja			■		■
7	**Beheer van bedrijfsmiddelen**						
7.1	**Verantwoordelijkheid voor bedrijfsmiddelen**						
7.1.1	Inventarisatie van bedrijfsmiddelen	Ja				■	■
7.1.2	Verantwoordelijken voor de bedrijfsmiddelen	Ja				■	
7.1.3	Aanvaardbaar gebruik van bedrijfsmiddelen	Ja				■	
7.2	**Classificatie van informatie**						
7.2.1	Richtlijnen voor classificatie	Ja				■	■
7.2.2	Labeling en verwerking van informatie	Ja				■	■
8	**Personeel**						
8.1	**Voorafgaand aan het dienstverband**						
8.1.1	Rollen en verantwoordelijkheden	Ja				■	■
8.1.2	Screening	Ja					■
8.1.3	Arbeidsvoorwaarden	Ja				■	■
8.2	**Tijdens het dienstverband**						
8.2.1	Directieverantwoordelijkheid	Ja				■	
8.2.2	Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	Ja					■
8.2.3	Disciplinaire maatregelen	Ja					■
8.3	**Beëindiging of wijziging van dienstverband**						
8.3.1	Beëindiging van verantwoordelijkheden	Ja					■
8.3.2	Retournering van bedrijfsmiddelen	Ja				■	■
8.3.3	Intrekken van toegangsrechten	Ja					■
9	**Fysieke beveiliging en beveiliging van de omgeving**						
9.1	**Beveiligde ruimten**						
9.1.1	Fysieke beveiliging van de omgeving	Ja					■
9.1.2	Fysieke toegangsbeveiliging	Ja					■
9.1.3	Beveiliging van kantoren, ruimten en faciliteiten	Ja					■
9.1.4	Beschermen tegen bedreigingen van buitenaf	Ja					■
9.1.5	Werken in beveiligde ruimten	Ja					■
9.1.6	Openbare toegang en gebieden voor laden en lossen	Nee	IPS maakt geen gebruik van een laad- en losruimte.				
9.2	**Beveiliging van apparatuur**						
9.2.1	Plaatsing en bescherming van apparatuur	Ja				■	
9.2.2	Nutsvoorzieningen	Ja					■
9.2.3	Beveiliging van kabels	Ja				■	
9.2.4	Onderhoud van apparatuur	Ja					■
9.2.5	Beveiliging van apparatuur buiten het terrein	Ja				■	■
9.2.6	Veilig verwijderen of hergebruiken van apparatuur	Ja					■
9.2.7	Verwijdering van bedrijfseigendommen	Ja					■
10	**Beheer van communicatie- en bedieningsprocessen**						
10.1	**Bedieningsprocedures en verantwoordelijkheden**						
10.1.1	Gedocumenteerde bedieningsprocedures	Ja				■	
10.1.2	Wijzigingsbeheer	Ja				■	
10.1.3	Functiescheiding	Ja				■	■
10.1.4	Scheiding van faciliteiten voor ontwikkeling, testen en productie	Ja					■
10.2	**Beheer van de dienstverlening door een derde partij**						
10.2.1	Dienstverlening	Ja			■	■	
10.2.2	Controle en beoordeling van dienstverlening door een derde partij	Ja				■	
10.2.3	Beheer van wijzigingen in dienstverlening foor een derde partij	Ja				■	
10.3	**Systeemplanning en -acceptatie**						
10.3.1	Capaciteitsbeheer	Ja				■	
10.3.2	Systeemacceptatie	Ja				■	
10.4	**Bescherming tegen kwaadaardige programmatuur en 'mobile code'**						
10.4.1	Maatregelen tegen kwaadaardige programmatuur	Ja					■
10.4.2	Maatregelen tegen 'mobile code'	Ja					■
10.5	**Back-up en herstel**						
10.5.1	Reservekopieën (back-ups)	Ja					■
10.6	**Beheer van netwerkbeveiliging**						
10.6.1	Maatregelen voor netwerken	Ja					■
10.6.2	Beveiliging van netwerkdiensten	Ja					■
10.7	**Behandeling van media**						
10.7.1	Beheer van verwijderbare media	Nee	Patiëntgegevens zijn bij IPS niet aanwezig op verwijderbare media.				
10.7.2	Verwijdering van media	Nee	Patiëntgegevens zijn bij IPS niet aanwezig op verwijderbare media.				
10.7.3	Procedures voor de behandeling van informatie	Nee	Patiëntgegevens zijn bij IPS niet aanwezig op verwijderbare media.				
10.7.4	Beveiliging van systeemdocumentatie	Ja				■	
10.8	**Uitwisseling van informatie**						
10.8.1	Beleid en procedures voor informatieuitwisseling	Ja					■
10.8.2	Uitwisselingsovereenkomsten	Ja			■		■
10.8.3	Fysiek transport van media	Nee	Patiëntgegevens zijn bij IPS niet aanwezig op verwijderbare media.				
10.8.4	Elektronische berichtenuitwisseling	Ja				■	■
10.8.5	Systemen voor bedrijfsinformatie	Ja					■
10.9	**Diensten voor e-commerce**						
10.9.1	E-commerce	Ja				■	
10.9.2	Online transacties	Nee	Er vinden geen transacties plaats in de systemen van IPS.				
10.9.3	Openbaar beschikbare informatie	Nee	IPS verwerkt geen openbaar beschikbare zorginformatie.				

Nr.	Doelstelling en maatregel NEN 7510:2011	Geselecteerd & Geïmplementeerd Ja/Nee	Onderbouwing (indien niet geselecteerd)	WE	CE	BR/BP	RA
10.10	**Controle**						
10.10.1	Aanmaken van audit-logbestanden	Ja				■	
10.10.2	Controle van systeemgebruik	Ja				■	■
10.10.3	Bescherming van informatie in logbestanden	Ja				■	
10.10.4	Logbestanden van administrators en operators	Ja				■	
10.10.5	Registratie van storingen	Ja				■	
10.10.6	Synchronisatie van systeemklokken	Ja				■	
11	**Toegangsbeveiliging**						
11.1	**Bedrijfseisen ten aanzien van toegangsbeheersing**						
11.1.1	Toegangsbeleid	Ja					■
11.2	**Beheer van toegangsrechten van gebruikers**						
11.2.1	Registratie van gebruikers	Ja				■	■
11.2.2	Beheer van speciale bevoegdheden	Ja				■	■
11.2.3	Beheer van gebruikerswachtwoorden	Ja				■	■
11.2.4	Beoordeling van toegangsrechten van gebruikers	Ja				■	■
11.3	**Verantwoordelijkheden van gebruikers**						
11.3.1	Gebruik van wachtwoorden	Ja				■	■
11.3.2	Onbeheerde gebruikersapparatuur	Ja				■	■
11.3.3	'Clear desk'- en 'clear screen'-beleid	Ja				■	■
11.4	**Toegangsbeheersing voor netwerken**						
11.4.1	Beleid ten aanzien van het gebruik van netwerkdiensten	Ja				■	■
11.4.2	Authenticatie van gebruikers bij externe verbindingen	Ja				■	■
11.4.3	Identificatie van netwerkapparatuur	Ja				■	■
11.4.4	Bescherming op afstand van poorten voor diagnose en configuratie	Ja				■	
11.4.5	Scheiding van netwerken	Ja				■	■
11.4.6	Beheersmaatregelen voor netwerkverbindingen	Ja				■	■
11.4.7	Beheersmaatregelen voor netwerkroutering	Ja				■	■
11.5	**Toegangsbeveiliging voor besturingssystemen**						
11.5.1	Beveiligde inlogprocedures	Ja				■	■
11.5.2	Gebruikersidentificatie en -authenticatie	Ja				■	■
11.5.3	Systemen voor wachtwoordbeheer	Ja				■	■
11.5.4	Gebruik van systeemhulpmiddelen	Ja				■	■
11.5.5	Time-out van sessies	Ja				■	■
11.5.6	Beperking van verbindingstijd	Ja				■	■
11.6	**Toegangsbeheersing voor toepassing en informatie**						
11.6.1	Beheersen van toegang tot informatie	Nee	IPS voert niet het beheer uit van toepassingssystemen van zorginstellingen.				
11.6.2	Isoleren van gevoelige systemen	Ja		■		■	■
11.7	**Draagbare computers en telewerken**						
11.7.1	Draagbare computers en communicatievoorzieningen	Ja					■
11.7.2	Telewerken	Ja					■
12	**Verwerving, ontwikkeling en onderhoud van informatiesystemen**						
12.1	**Beveiligingseisen voor informatiesystemen**						
12.1.1	Analyse en specificatie van beveiligingseisen	Ja				■	■
12.2	**Correcte verwerking in toepassingen**						
12.2.1	Validatie van invoergegevens	Nee	IPS voert niet het beheer uit van toepassingssystemen van zorginstellingen.				
12.2.2	Beheersing van interne gegevensverwerking	Nee	IPS voert niet het beheer uit van toepassingssystemen van zorginstellingen.				
12.2.3	Integriteit van berichten	Nee	IPS voert niet het beheer uit van toepassingssystemen van zorginstellingen.				
12.2.4	Validatie van uitvoergegevens	Nee	IPS voert niet het beheer uit van toepassingssystemen van zorginstellingen.				
12.3	**Cryptografische beheersmaatregelen**						
12.3.1	Beleid voor het gebruik van cryptografische beheersmaatregelen	Ja					■
12.3.2	Sleutelbeheer	Ja				■	
12.4	**Beveiliging van systeembestanden**						
12.4.1	Beheersing van operationele programmatuur	Ja				■	■
12.4.2	Bescherming van testdata	Nee	Het is niet mogelijk om patiëntgegevens te gebruiken als testdata.				
12.4.3	Toegangsbeheersing van broncode voor programmatuur	Ja		■		■	
12.5	**Beveiliging bij ontwikkelings- en ondersteuningprocessen**						
12.5.1	Procedures voor wijzigingsbeheer	Ja				■	
12.5.2	Technische beoordeling van toepassingen na wijzigingen in het besturingssysteem	Ja				■	
12.5.3	Restricties op wijzigingen in programmatuurpakketten	Ja				■	
12.5.4	Informatielekken	Ja		■		■	■
12.5.5	Uitbestede ontwikkeling van programmatuur	Ja				■	
12.6	**Beheer van technische kwetsbaarheden**						
12.6.1	Beheersing van technische kwetsbaarheden	Ja				■	
13	**Beheer van informatiebeveiligingsincidenten**						
13.1	**Rapportage van informatiebeveiligingsgebeurtenissen en zwakke plekken**						
13.1.1	Rapportage van informatiebeveiligingsgebeurtenissen	Nee	IPS kan geen informatiebeveiligingsgebeurtenissen rapporteren aan patiënten.				
13.1.2	Rapportage van zwakke plekken in de beveiliging	Ja				■	
13.2	**Beheer van informatiebeveiligingsincidenten en -verbeteringen**						
13.2.1	Verantwoordelijkheden en procedures	Ja				■	
13.2.2	Leren van informatiebeveiligingsincidenten	Ja				■	
13.2.3	Verzamelen van bewijsmateriaal	Ja				■	
14	**Bedrijfscontinuïteitsbeheer**						
14.1	**Informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer**						
14.1.1	Informatiebeveiliging opnemen in het proces van bedrijfscontinuïteitsbeheer	Ja				■	■
14.1.2	Bedrijfscontinuïteit en risicobeoordeling	Ja				■	■
14.1.3	Continuïteitsplannen en informatievoorziening	Ja				■	■
14.1.4	Kader voor bedrijfscontinuïteitsplanning	Ja				■	
14.1.5	Testen, onderhoud en herbeoordelen van bedrijfscontinuïteitsplannen	Ja				■	■
15	**Naleving**						
15.1	**Naleving van wettelijke voorschriften**						
15.1.1	Identificatie van toepasselijke wetgeving	Ja		■			■
15.1.2	Intellectuele eigendomsrechten (Intellectual Property Rights, IPR)	Ja		■			■
15.1.3	Bescherming van bedrijfsdocumenten	Ja		■	■	■	■
15.1.4	Bescherming van gegevens en geheimhouding van persoonsgegevens	Ja		■	■		■
15.1.5	Voorkomen van misbruik van IT-voorzieningen	Ja		■			■
15.1.6	Voorschriften voor het gebruik van cryptografische beheersmaatregelen	Ja		■			■
15.2	**Naleving van beveiligingsbeleid en -normen en technische naleving**						
15.2.1	Naleving van beveiligingsbeleid en -normen	Ja				■	
15.2.2	Controle op technische naleving	Ja				■	
15.3	**Overwegingen bij audits van informatiesystemen**						