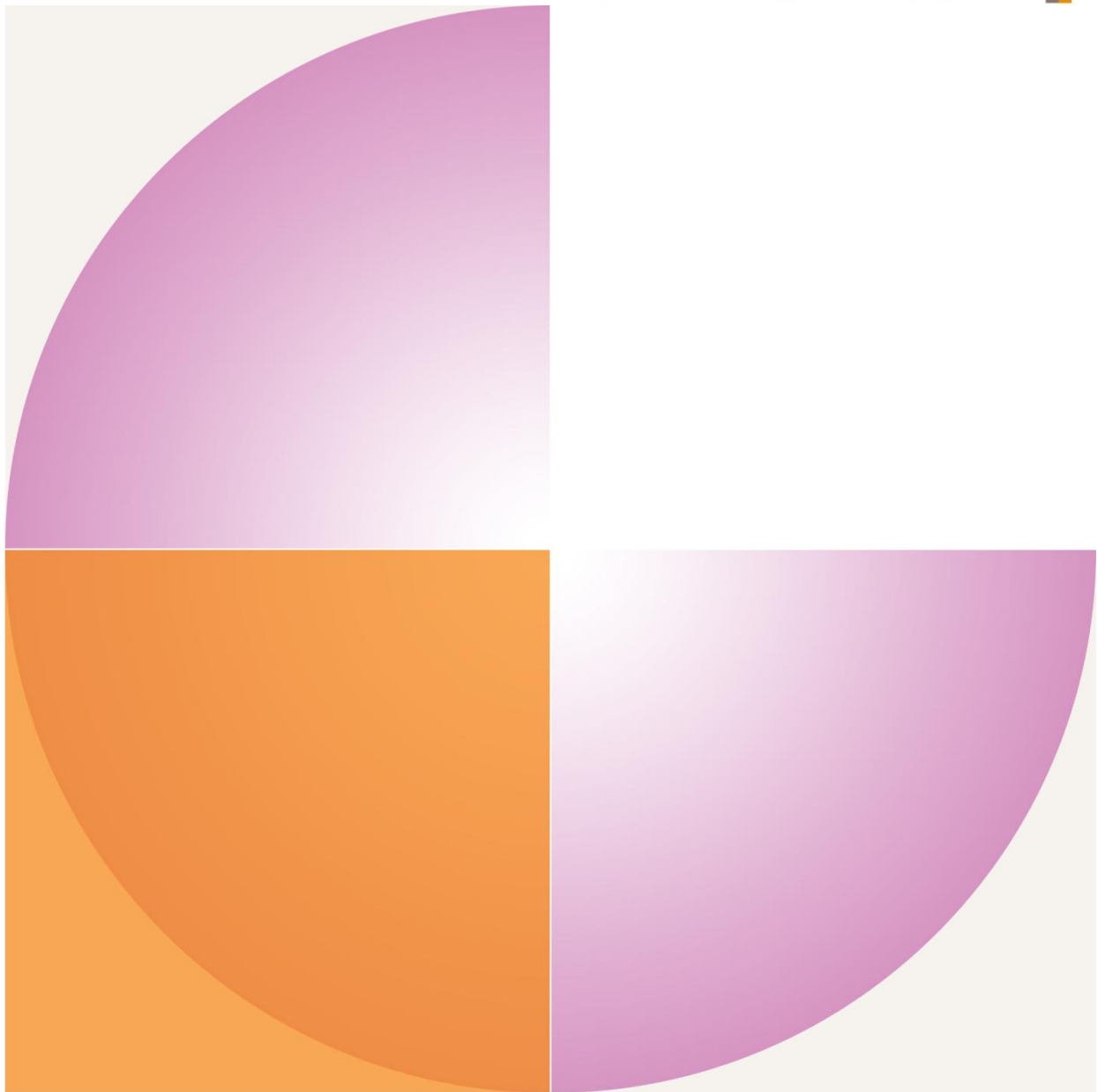


# Programma van eisen zorgserviceprovider (ZSP)

Betere zorg  
door betere informatie



Datum: 25 mei 2013  
Versie: 6.12.0.0  
Referentie: [PvE ZSP]

Nictiz is het landelijke expertisecentrum dat ontwikkeling van ICT in de zorg faciliteert. Met en voor de zorgsector voorziet Nictiz in mogelijkheden en randvoorwaarden voor elektronische informatie-uitwisseling voor en rondom de patiënt. Wij doen dit ter bevordering van de kwaliteit en doelmatigheid in de gezondheidszorg.

**Nictiz**

Postbus 19121  
2500 CC Den Haag  
Oude Middenweg 55  
2491 AC Den Haag

T 070 - 317 34 50  
[info@nictiz.nl](mailto:info@nictiz.nl)  
[www.nictiz.nl](http://www.nictiz.nl)

## Inhoudsopgave

<b>1</b>	<b>Inleiding</b>	<b>3</b>
1.1	Doel en scope	3
1.2	Doelgroep voor dit document	3
1.3	Documenthistorie	3
1.4	Uitleg presentatie van eisen	4
<b>2</b>	<b>Eisen aan de organisatie</b>	<b>5</b>
2.1	Ondersteuning van gebruikers	5
2.2	Beveiligingsmaatregelen	8
2.3	Systeembeheer	11
2.4	Toezicht en verantwoording	13
<b>3</b>	<b>Kwaliteitseisen aan de aangesloten systemen</b>	<b>15</b>
3.1	Connectiviteit	15
3.2	Beschikbaarheid	16

### 1 Inleiding

#### 1.1 Doel en scope

Dit document specificeert de eisen waaraan een netwerkdienstverlener moet voldoen om een betrouwbare partij te zijn voor gegevensuitwisseling in de zorg. Dit document bevat eisen o.h.g.v. vertrouwelijkheid, integriteit en continuïteit van de dienstverlening van de organisatie. Een netwerkdienstverlener die voldoet aan deze eisen kan zich door Nictiz laten kwalificeren als Zorgserviceprovider.

#### 1.2 Doelgroep voor dit document

De doelgroep van dit document bestaat uit:

- netwerkdienstverleners
- overige partijen die zich bezighouden met de ontwikkeling en implementatie van ICT-toepassingen in de zorg, zoals zorgaanbieders, ontwikkelaars, leveranciers en onderzoekers.

#### 1.3 Documenthistorie

Versie	Datum	Omschrijving
6.12.0.0	17-jan-2013	Verwijderen van LSP-specifieke eisen zodat ook gekwalificeerd kan worden zonder aansluiting op het LSP.
6.12.0.0	25-mei-2013	Verdere aanpassingen voor AORTA-vrije versie

## 1.4 Uitleg presentatie van eisen

De eisen die in dit document zijn opgenomen, worden uniform gepresenteerd. De gebruikte tabel per eis bevat onder andere aparte aanduidingen voor het karakter en de verificatiewijze. Hieronder wordt kort aangegeven wat de termen in deze velden aanduiden.

Karakter:

- **Verplicht:** de eis is verplicht voor de in de scope genoemde systemen
- **Optioneel:** de eis is niet verplicht, maar als de functionaliteit wordt geboden, dan moet die voldoen aan wat in de eis is beschreven.
- **Conditioneel:** de eis is verplicht onder de conditie die is gesteld in het veld "Conditie".
- **Conditie LSP:** In een aantal gevallen staat hier de specifieke invulling van de eisen die gelden voor aansluiting op het LSP vermeld.

Verificatiewijze (geeft een indicatie van de wijze waarop de eis wordt getoetst):

- **Opzet:** is de eis in de procedures afgedekt?
- **Bestaan:** is de procedure geïmplementeerd?
- **Werking:** is er terugkijkend, bewijs dat de procedures gewerkt hebben?

## 2 Eisen aan de organisatie

Een ZSP-kwalificatie is een keurmerk dat op één tijdstip wordt verkregen. De geldigheid van de kwalificatie is in principe drie jaar. De ZSP dient Nictiz op de hoogte te houden van wijzigingen in de organisatie die de kwalificatie of het object van kwalificatie veranderen, zodat Nictiz kan beoordelen of herkwalificatie noodzakelijk is om het ZSP-label te behouden.

Daarnaast is de ZSP verplicht jaarlijks een self-assesment uit te voeren en de resultaten met een eigen verklaring van compliance aan Nictiz te verstrekken. Nictiz zal hiervoor het initiatief nemen.

### 2.1 Ondersteuning van gebruikers

Een ZSP dient te voldoen aan de volgende eisen met betrekking tot de ondersteuning van gebruikers:

<b>ZSP.FBH.e4010</b>	
<b>De ZSP dient te beschikken over een servicedesk ten behoeve van ondersteuning van de dienstverlening aan zorgaanbieders. Deze servicedesk dient:</b>	
<b>a) een inschatting te geven van de verwachte oplostermijn;</b>	
<b>b) regelmatig te rapporteren over de voortgang van de oplossing;</b>	
<b>c) op in de SLA met de afnemers vastgestelde tijden bereikbaar te zijn;</b>	
<b>d) vastgestelde procedures voor het registreren, afhandelen, afsluiten en rapporteren van incidenten te hebben;</b>	
<b>e) voortgangsbewaking uit te oefenen op de afhandeling van incidenten.</b>	
<b>Doelstelling</b>	De dienstverlening van een ZSP aan zorgaanbieder, andere ZSP's en andere afnemers moet gewaarborgd worden door het bieden van een aanspreekpunt waarbij incidenten en problemen kunnen worden gemeld en opgevolgd.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	Een ZSP zal, afhankelijk van de aard van het incident en de geleverde diensten aan de zorgaanbieder, namens de zorgaanbieder het contact voeren met alle betrokken partijen, zodat de zorgaanbieder één loket voor ondersteuning heeft. Een ZSP zal verder doorgaans medewerkers van de servicedesk met service-, incident- of call-management instrumenten willen ondersteunen.
<b>Verificatiewijze</b>	Opzet, bestaan en werking.
<b>Voorheen</b>	

**ZSP.FBH.e4020**

**De ZSP heeft procedures in werking voor de adequate afhandeling van verschillende klassen van beschikbaarheidsincidenten. Een ZSP dient gebruikersondersteuning aan te bieden met een serviceniveau dat is afgestemd op de prioriteit van het incident. De prioriteit is gebaseerd op onderstaande classificatie van aangemelde incidenten:**

- a) klasse 1: de dienstverlening is voor één of meer afnemers onbeschikbaar.**
- b) klasse 2: de dienstverlening is voor nagenoeg alle afnemers beperkt onbeschikbaar.**
- c) klasse 3: de dienstverlening is voor enkele afnemers beperkt onbeschikbaar.**

**De hersteltijd is voor klasse 1, binnen 1 uur; voor klasse 2 binnen 4 uur; en voor klasse 3 binnen 24 uur.**

<b>Doelstelling</b>	Het streven naar hoge beschikbaarheid en garanties voor de duur van evt. verminderde- of on-beschikbaarheid en inzicht te hebben in de impact van incidenten op de betrouwbare werking van het netwerk. Afhankelijkheden van toeleveranciers moeten daarbij ook duidelijk worden gemaakt. Een ZSP dient zorgaanbieders hulp te bieden bij het in gebruik nemen, buiten gebruik stellen, of wijzigen van de aansluiting op een netwerk en dient problemen te classificeren op basis van mate van (on-)beschikbaarheid.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	Onder beperkt onbeschikbaar verstaan wij uitval van services die, mits ze een beperkte duur hebben, geen onmiddellijke belemmering van het businessproces van de klant impliceren en/of die door een work-around tijdelijk kunnen worden gecompenseerd. Anders is er sprake van volledige onbeschikbaarheid en gelden de daarbij behorende hersteltermijnen.
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	Ook ZSP.fbh.e4080 opgenomen in deze eis.

<b>ZSP.FBH.e4030</b>	
<b>De ZSP dient meldingen van de afnemers te beheren en af te handelen.</b>	
<b>Doelstelling</b>	De kwaliteit van de dienstverlening verhogen door gebruik te maken van de vragen en opmerkingen van afnemers.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	De ZSP zal zo procedures ontwikkelen en in stand houden die bij het afhandelen en beheren van meldingen worden gevolgd. Onder meldingen verstaan wij vragen, opmerkingen en incidenten anders dan beschikbaarheidsincidenten. Zie daarvoor <b>ZSP.FBH.e4020</b> . In voorkomende gevallen zal een ZSP hier een beheerinstrument voor inzetten.
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	

## 2.2 Beveiligingsmaatregelen

Een ZSP dient te voldoen aan de volgende beveiligingseisen:

<b>ZSP.BVL.e4010</b>	
<b>De ZSP heeft een informatiebeveiligingsbeleid met beleidsmaatregelen, uitgangspunten en gedragsregels ten aanzien van informatiebeveiliging opgesteld en geïmplementeerd waarin aandacht wordt besteed aan het beveiligingsniveau van alle netwerkkoppelingen van:</b> <ul style="list-style-type: none"><li><b>a) de eigen beheersystemen;</b></li><li><b>b) netwerkcommunicatie;</b></li><li><b>c) Aangesloten instellingen en registers;</b></li></ul> <b>Dit beleid wordt regelmatig getoetst en bijgesteld o.a. aan de hand van risico-analyses.</b>	
<b>Doelstelling</b>	Deze eis is bedoeld als middel om voldoende bescherming te verkrijgen tegen de bedreigingen van de integriteit, vertrouwelijkheid en authenticiteit van de gegevensuitwisseling tussen de zorgaanbieders. Verder dient het om voldoende waarborgen te realiseren zodat het doel en het belang van informatiebeveiliging voldoende in de ZSP-organisatie wordt verankerd. Tevens vormt het een communicatiemiddel naar ZSP-medewerkers, zodat deze zich aan de geldende voorschriften, gedragsregels en maatregelen kunnen houden.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	

<b>ZSP.BVL.e4020</b>	
<b>De ZSP heeft beveiligingseisen geformuleerd ten aanzien van personeel. Onderdeel daarvan zijn:</b> <ul style="list-style-type: none"><li><b>a) Een geheimhoudingsverklaring;</b></li><li><b>b) Een verklaring omtrent gedrag (VOG);</b></li><li><b>c) Een disciplinair proces bij overtredingen;</b></li><li><b>d) Procedure beëindiging dienstverband.</b></li></ul>	
<b>Doelstelling</b>	Borging van de betrouwbaarheid van het personeel.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	Omdat in sommige gevallen ZSP personeel tot op een persoon herleidbare gegevens onder ogen kan krijgen zijn deze maatregelen nodig.
<b>Verificatiewijze</b>	Opzet, bestaan en werking.
<b>Voorheen</b>	



<b>ZSP.BVL.e4030</b>	
<b>De ZSP heeft beveiligingsmaatregelen geïmplementeerd ten aanzien van de fysieke beveiliging.</b>	
<b>Doelstelling</b>	Het aantal incidenten en hun gevolgen te verkleinen.
<b>Karakter</b>	Verplicht
<b>Toelichting</b>	<p>Kritische of gevoelige apparatuur voor informatieverwerking, zoals ICT hardware en bekabeling, moet opgesteld zijn in een ruimte die:</p> <ul style="list-style-type: none"> <li>a) Beveiligd is</li> <li>b) omgeven is door een goed gedefinieerde beveiligingsgrens</li> <li>c) passende toegangsbelemmeringen en ingangcontroles heeft</li> <li>d) fysieke beveiliging tegen ongeoorloofde toegang bevat</li> <li>e) het toebrengen van schade minimaliseert</li> <li>f) andere niet toegestane inmenging uitsluit</li> <li>g) een functionerende noodstroomvoorziening ter beschikking heeft</li> </ul> <p>Er zijn voorzieningen getroffen die de continuïteit van de informatieverwerking garanderen, bijvoorbeeld in de volgende situaties:</p> <ul style="list-style-type: none"> <li>a) schade door brand</li> <li>b) wateroverlast</li> <li>c) explosies</li> <li>d) ordeverstoringen</li> <li>e) andere natuurlijke, of door mensen veroorzaakte calamiteiten.</li> </ul>
<b>Conditie</b>	
<b>Verificatiewijze</b>	Opzet en bestaan
<b>Voorheen</b>	

<b>ZSP.BVL.e4040</b>	
<b>De ZSP heeft een beleid voor logische toegang waardoor iedere beheerder een uniek user-id heeft. Elke wijziging wordt op het niveau van user-id geregistreerd zodat iedere beheerder van de infrastructuur uniek identificeerbaar en traceerbaar is.</b>	
<b>Doelstelling</b>	Om ongeautoriseerde toegang te voorkomen zijn er procedures en regels nodig. Zonder het vastleggen van de procedures en regels zijn de verantwoordelijkheden niet duidelijk, wat leidt tot slecht gecontroleerde beveiliging.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	

<b>Toelichting</b>	<p>Er moet een registratie zijn van gebruikers die toegang hebben tot informatiesystemen (en -diensten). Het betreft hier alleen de informatiesystemen die worden gebruikt ten behoeve van de zorg en dus niet de financiële administratie van de ZSP, mail, etc.</p> <p>De ZSP heeft procedures , die aantoonbaar worden nageleefd, voor het melden en afmelden van gebruikers. Daarnaast zijn procedures noodzakelijk voor het toewijzen van unieke gebruikersidentificaties.</p>
<b>Verificatiewijze</b>	Opzet, bestaan en werking
<b>Voorheen</b>	

<b>ZSP.BVL.e4050</b>	
<b>De ZSP dient zijn afnemers te beschermen tegen bedreigingen van andere systemen die toegang hebben tot het netwerk van de ZSP. De ZSP dient aan te geven welke maatregelen er zijn getroffen ter bescherming tegen bedreigingen van buitenaf</b>	
<b>Doelstelling</b>	Om te voorkomen dat de dienstverlening in gevaar komt zijn maatregelen (zoals virusscanners, anti-spam apparatuur, inbraak detectie systemen) noodzakelijk. Verder zijn ook maatregelen nodig om de invoer van kwaadaardige of foutieve programmatuur in de beschermde omgeving te voorkomen.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	<p>Het beschermen tegen bedreigingen van andere systemen die toegang hebben tot het netwerk van de ZSP kan door bijvoorbeeld gebruik te maken van:</p> <ul style="list-style-type: none"> <li>a) virusscanners</li> <li>b) anti-spam apparatuur</li> <li>c) inbraak detectie systemen (Intrusion Detection Systems)</li> <li>d) inbraak preventie systemen (Intrusion Prevention Systems)</li> <li>e) gescheiden ontwikkel-, test-, acceptatie-, en productievoorzieningen</li> <li>f) proxy servers</li> <li>g) firewalls</li> </ul>
<b>Verificatiewijze</b>	Opzet en bestaan
<b>Voorheen</b>	

<b>ZSP.BVL.e4060</b>	
<b>De ZSP heeft een actueel continuïteitsplan. Periodiek wordt het continuïteitsplan getest.</b>	
<b>Doelstelling</b>	Het doel van deze eis is om de continuïteit van de dienstverlening door de ZSP in overeenstemming met de gemaakte afspraken te waarborgen.

<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	<p>Omdat potentieel iedere zorgverlener op elk moment van de dag behoefte kan hebben aan informatie, die via de ZSP wordt opgehaald en afgeleverd bij een zorgaanbieder, is de continuïteit van de dienstverlening zeer belangrijk.</p> <p>Als gevolg hiervan moet de ZSP continuïteitsbeheer implementeren waarbij de volgende items zijn geadresseerd:</p> <ul style="list-style-type: none"> <li>a) het vaststellen en verminderen van risico's;</li> <li>b) het beperken van de gevolgen van incidenten die schade toebrengen</li> <li>c) het binnen de vastgestelde termijnen hervatten van de connectiviteit.</li> </ul>
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	

### 2.3 Systeembeheer

Een ZSP dient te voldoen aan de volgende eisen inzake beheer:

<b>ZSP.SBH.e4010</b>	
<b>Er dient altijd (7x24 uur) ten minste een beheerder telefonisch bereikbaar te zijn voor de afnemers die in staat is de nodige beheertaken uit te voeren.</b>	
<b>Functie</b>	De functie van deze eis is om te waarborgen dat de ZSP altijd kan worden beheerd.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	Een ZSP zal zijn beheermedewerkers waarschijnlijk van mobiele telecommunicatiemiddelen en middelen voor beheer op afstand willen voorzien om beheertaken uit te voeren.
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	

<b>ZSP.SBH.e4020</b>	
<b>Beschikbaarheid van ICT-diensten en ICT-middelen wordt continu (geautomatiseerd) gemeten en geregistreerd. Passende signaleringen en opvolging daarvan zijn ingericht.</b>	
<b>Doelstelling</b>	De functie van deze eis is om problemen zo snel mogelijk op te lossen.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	

<b>Toelichting</b>	Een ZSP zal in voorkomende gevallen een monitorinstrument willen inrichten waarmee een bericht kan worden gerelateerd aan het IP-adres van bij het probleem betrokken communicatiepartijen.
<b>Verificatiewijze</b>	Opzet, bestaan en werking.
<b>Voorheen</b>	

<b>ZSP.SBH.e4030</b>	
<b>De ZSP dient de connecties door te kunnen meten en daarover te rapporteren. Rapportage van de meting bevat informatie over de geleverde en gebruikte bandbreedte per verbinding per zorgaanbieder binnen het netwerk.</b>	
<b>Doelstelling</b>	De functie van deze eis is het voorkomen, lokaliseren of oplossen van capaciteit- en communicatieproblemen.
<b>Karakter</b>	Verplicht
<b>Conditie LSP</b>	<b>20 connecties tegelijkertijd moeten kunnen worden doorgemeten.</b>
<b>Toelichting</b>	Bij voorkeur worden metingen proactief uitgevoerd en gelogd met behulp van monitoring-instrumenten.
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	

<b>ZSP.SBH.e4040</b>	
<b>De ZSP dient maandelijkse rapportages te maken over de gerealiseerde beschikbaarheid en over frequentie, tijdsduur en hersteltijden van ZSP-storingen en die op verzoek van afnemers kunnen overleggen.</b>	
<b>Doelstelling</b>	Inzicht hebben in de prestaties en potentiële verbetering van het ZSP-netwerk.
<b>Karakter</b>	Verplicht
<b>Conditie LSP</b>	Conditioneel voor aansluiting op LSP is een maandelijkse rapportage aan AORTA-regie.
<b>Toelichting</b>	
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	

<b>ZSP.SBH.e4050</b>	
<b>Een ZSP dient gepland onderhoud, waarbij onderbreking van de dienstverlening plaatsvindt, minimaal 5 werkdagen van tevoren aan te kondigen aan alle afnemers.</b>	
<b>Doelstelling</b>	Om alle afnemers in staat te stellen te anticiperen op

	verminderde beschikbaarheid van de functies van het netwerk is een melding van de ZSP nodig.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	Een ZSP zal procedures ontwikkelen en in stand houden die bij aankondiging van onderhoud worden gevolgd.
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	

<b>ZSP.SBH.e4060</b>	
<b>De ZSP dient het verhuizen van netwerkverbindingen van een afnemer naar een andere ZSP binnen 3 weken mogelijk te maken zonder verlies van continuïteit, gerekend vanaf het moment van een werkende verbinding.</b>	
<b>Doelstelling</b>	De functie van deze eis is om vrije marktwerking te bevorderen. Dit wordt bevorderd door belemmeringen voor zorgaanbieders om van ZSP te wisselen te verminderen.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	Voor zover nodig zal de ZSP de huidige routing binnen haar netwerk voor de betreffende afnemer teniet doen. Een procedure verhuizen/afsluiten afnemer zou hiervoor gebruikt kunnen worden.  ZSP's zijn afhankelijk van de aanleg van fysieke communicatielijnen. Daarom wordt gerekend vanaf het moment van een werkende verbinding tussen het zorgaanbieder en de "andere" ZSP.
<b>Verificatiewijze</b>	Opzet.
<b>Voorheen</b>	

## 2.4 Toezicht en verantwoording

Een ZSP dient te voldoen aan de volgende eisen t.a.v. zijn organisatie:

<b>ZSP.FBH.e4040</b>	
<b>Een ZSP dient een geldige inschrijving te hebben bij een Kamer van Koophandel.</b>	
<b>Doelstelling</b>	Om een zorgaanbieder de mogelijkheid te geven om de ondernemingsgegevens van een ZSP te verifiëren is een inschrijving bij een Kamer van Koophandel nodig.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	

<b>Toelichting</b>	
<b>Verificatiewijze</b>	Bestaan
<b>Voorheen</b>	

<b>ZSP.FBH.e4050</b>	
<b>Een ZSP dient als hoofdaannemer op te treden wanneer deze gebruik maakt van diensten van derden.</b>	
<b>Doelstelling</b>	Een zorgaanbieder hoeft hierdoor geen anderen dan de ZSP aan te spreken op de diensten die de ZSP levert.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	Op deze manier wordt geprobeerd voldoende waarborgen te verkrijgen met betrekking tot de aansprakelijkheid van de ZSP. De ZSP kan dus onderaannemers hebben maar blijft verantwoordelijk.
<b>Verificatiewijze</b>	Opzet en bestaan
<b>Voorheen</b>	

<b>ZSP.FBH.e4070</b>	
<b>De ZSP dient een <i>service level agreement (SLA)</i> te hebben met iedere aangesloten zorgaanbieder.</b>	
<b>Doelstelling</b>	De functie van deze eis is om een duidelijk en beschreven beeld te hebben van de aan de zorgaanbieder geleverde diensten en voorwaarden.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	De ZSP zal hiervoor doorgaans een service management en delivery proces willen inrichten.
<b>Verificatiewijze</b>	Opzet en bestaan
<b>Voorheen</b>	

### 3 Kwaliteitseisen aan de aangesloten systemen

Dit hoofdstuk licht de eisen toe waaraan een ZSP moet voldoen. Een ZSP moet de volgende functies kunnen uitvoeren, ongeacht of de gebruikers die daadwerkelijk benutten:

- Datacommunicatiefuncties in opdracht van het informatiesysteem van een zorgaanbieder.

De datacommunicatiefuncties omvatten:

- (a) Netwerktransport van data van de zorgaanbieder naar andere zorgaanbieders al dan niet via centraal ingerichte componenten;
- (b) Domain Name Systeem functies.

#### 3.1 Connectiviteit

ZSP.CON.e4010	
<b>Het ZSP dient vast te leggen welke gespecificeerde berichtuitwisseling via het netwerk mogelijk is.</b>	
<b>Doelstelling</b>	De <i>protocolstack</i> moet ongehinderd door het netwerk van de ZSP getransporteerd worden.
<b>Karakter</b>	Verplicht
<b>Conditie LSP</b>	Voor het LSP geldt de stack die beschreven is in de AORTA-architectuur.
<b>Toelichting</b>	
<b>Verificatiewijze</b>	Opzet.
<b>Voorheen</b>	

ZSP.CON.e4050	
<b>De grenzen aan de domeinen dienen helder te zijn zodat duidelijk is welke componenten onder wiens beheer vallen, welke aansprakelijkheden gelden en welke afspraken gelden voor alle netwerkcomponenten.</b>	
<b>Doelstelling</b>	'De functie van deze eis is om het domein van de ZSP te scheiden van het domein van de zorgaanbieder. Zodoende vormen gebeurtenissen in het netwerk van de ZSP in mindere mate een operationeel risico voor het netwerk van de zorgaanbieder en andersom. Daarnaast kan ter plekke van het scheidingsvlak het netwerkverkeer bewaakt worden.
<b>Karakter</b>	Verplicht
<b>Conditie LSP</b>	De ZSP dient op de zorgaanbiederlocatie een door de ZSP te beheren netwerkcomponent te plaatsen.
<b>Toelichting</b>	Een ZSP zal deze installatie, beheer en onderhoudswerkzaamheden op de locatie bij een zorgaanbieder verrichten. Een zorgaanbieder zal hiervoor ruimte en een aansluiting op het elektriciteitsnetwerk ter beschikking stellen en

	de ZSP-medewerker toegang moeten verlenen tot de voorziening.
<b>Verificatiewijze</b>	Opzet en bestaan
<b>Voorheen</b>	

<b>ZSP.CON.e4060</b>	
<b>De ZSP mag voor het verkeer tussen de afnemers geen onderdelen gebruiken die gebaseerd, configureerbaar of benaderbaar zijn via het openbare internet.</b>	
<b>Doelstelling</b>	De componenten geen doelwit te laten zijn van inbraken vanaf openbaar internet.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	Voor een netwerk dat gevoelige informatie uitwisselt is dit ongewenst en risicoverhogend.
<b>Verificatiewijze</b>	Opzet en bestaan
<b>Voorheen</b>	

### 3.2 Beschikbaarheid

<b>ZSP.BES.e4010</b>	
<b>Een ZSP dient 24 uur per dag, 7 dagen per week beschikbaar te zijn.</b>	
<b>Doelstelling</b>	Het doel van deze eis is om een voldoende niveau van continuïteit van ZSP dienstverlening te waarborgen. Hierdoor kunnen zorgaanbieders vrijwel altijd gegevens met elkaar uitwisselen.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	In de bedrijfsvoering van een ZSP mogen niet bij voorbaat perioden gepland worden waarin netwerkverkeer tussen zorgaanbieders niet mogelijk is. De ZSP zal haar infrastructuur zo moeten inrichten dat de faalkans en de hersteltijd van componenten in overeenstemming zijn met de gestelde eisen.
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	



<b>ZSP.BES.e4020</b>	
<b>De overall beschikbaarheid (exclusief gepland onderhoud) van het netwerk dat onder een ZSP ressorteert dient minimaal 99,9% per jaar te zijn.</b>	
<b>Doelstelling</b>	Het doel van deze eis is om een voldoende niveau van continuïteit van de dienstverlening van de ZSP te waarborgen.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	De ZSP zal haar infrastructuur zo moeten inrichten dat de faalkans en de hersteltijd van componenten in overeenstemming zijn met de gestelde eisen.
<b>Verificatiewijze</b>	Opzet, bestaan en werking.
<b>Voorheen</b>	

<b>ZSP.BES.e4040</b>	
<b>De ZSP dient onderhoud gepland te laten plaatsvinden.</b>	
<b>Doelstelling</b>	Het doel van deze eis is dat gepland onderhoud een zo min mogelijk verstorend effect heeft op het normale berichtenverkeer.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	De ZSP heeft onderhoudsprocedures die worden gevolgd. Ook zal de ZSP in voorkomende gevallen bepaalde componenten redundant willen uitvoeren
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	

<b>ZSP.BES.e4050</b>	
<b>De ZSP dient de afnemers op de hoogte te stellen wanneer het netwerk, na onderhoud of storing, weer beschikbaar is.</b>	
<b>Doelstelling</b>	De functie van deze eis is om tijdelijke maatregelen die door een zorgaanbieder of andere afnemer ten behoeve van het ZSP onderhoud zijn genomen te niet te doen.
<b>Karakter</b>	Verplicht
<b>Conditie</b>	
<b>Toelichting</b>	
<b>Verificatiewijze</b>	Opzet en bestaan.
<b>Voorheen</b>	



## **Bijlage A: Referenties**

<b>Referentie</b>	<b>Document</b>	<b>Versie</b>