# AANSLUIT- en IMPLEMENTATIEVOORWAARDEN

Versie: 1.20
Status: Concept
Datum: 30-05-2022

## Inhoud



# 1. *Over dit document*

| | |
|---|---|
| Document nr. | D06 |
| Titel | Aansluit- en implementatievoorwaarden |
| Classificatie | Intern en extern gebruik |
| Bijlagen | n.v.t. |

## 1.1 *Versiehistorie*

| Versie | Auteur | Datum | Wijzigingen en aanvullingen |
|---|---|---|---|
| 1.20. | W. Heemskerk | 30-05-2022 | Volledige herziening n.a.v. versie 1.10.1 |
| | | | |

## 1.2 *Status*

| | | | | |
|---|---|---|---|---|
| Auteur | Informatie Architect | W. Heemskerk | Versie | 1.20. |
| Eigenaar | Manager IV | L. van Wijk | Vastgesteld | --- |

## 2. *Inleiding*

Dit document beschrijft eisen m.b.t. IT, Informatiebeveiliging en Architectuur waaraan informatiesystemen, die door Ipse de Bruggen in gebruik en/of beheer worden genomen dienen te voldoen. Een informatiesysteem kan een softwaretoepassing, al of niet i.c.m. (specifieke) hardware zijn. In dit document worden met 'informatiesysteem' alle componenten bedoeld die door de leverancier als product worden geleverd.

In dit document wordt met 'leverancier' altijd de onderneming of rechtspersoon bedoeld waarmee Ipse de Bruggen een overeenkomst aangaat m.b.t. het informatiesysteem.

*Deze aansluitvoorwaarden en de bijbehorende antwoorden en eventuele uitzonderingen vormen een onlosmakelijk onderdeel van de uiteindelijke overeenkomst tussen de leverancier en Ipse de Bruggen.*

## 3. *Waarom aansluit- en implementatievoorwaarden?*

Het doel van deze voorwaarden is om, nu en in de toekomst, naast de gewenste functionaliteit en beoogde dienstverlening, te toetsen of een informatiesysteem past binnen de architectuur van Ipse de Bruggen. De beschreven voorwaarden worden getoetst tijdens de selectiefase, maar ook tijdens de gehele periode dat een informatiesysteem wordt ingezet/gebruikt. Daarbij is het mogelijk dat de voorwaarden over tijd worden geactualiseerd naar de op dat moment geldende standaarden, normen of bij grote veranderingen binnen en/of buiten Ipse de Bruggen.

De voorwaarden voorzien in een aantal behoeften:

1. Dit document beschrijft eisen waaraan informatiesystemen dienen te voldoen, zodat deze op een eenduidige en solide wijze ontsloten kunnen worden. De voorwaarden in dit document vormen een belangrijk onderdeel van de acceptatiecriteria en dienen daarmee als input voor een programma van eisen.
2. Dit document dient als basis voor de gehele operationele fase, waarbij allerlei vormen van beheer en service management terug kunnen vallen op de voorwaarden wanneer daar aanleiding voor is.

### **3.1** *Scope*

De scope van dit document omvat alle informatiesystemen die, op wat voor wijze dan ook, worden ingezet en/of aangesloten op de IT-Infrastructuur van Ipse de Bruggen. Hieronder vallen ook informatiesystemen die (deels) als SaaS-dienst worden aangeboden. Naast de hier beschreven voorwaarden dient te allen tijden te worden voldaan aan wet- en regelgeving in het algemeen en ten aanzien van (persoons)gegevens- en informatiebeveiliging in het bijzonder. Hieronder vallen ook, waar van toepassing, de vereisten conform de wet aanvullende bepalingen verwerking persoonsgegevens in de zorg m.b.t. digitaal inzagerecht.

### **3.2** *Conformeren of toelichten*

De Aansluitvoorwaarden staan o.a. onder invloed van ontwikkelingen in de markt, binnen de zorgsector en/of binnen Ipse de Bruggen. Hierdoor kunnen de aansluit- en implementatievoorwaarden aangepast worden. Hiervan wordt de leverancier altijd op de hoogte gesteld. Wanneer op enig moment niet (meer) conform deze voorwaarden kan worden geleverd, dient dit te worden aangegeven en toegelicht. Een alternatieve invulling van de voorwaarden is mogelijk, waarbij Ipse de Bruggen beoordeelt of acceptatie mogelijk is (zie ook 3.3).

### 3.3 *Aanvullend onderzoek*

Wanneer een informatiesysteem afwijkt van de vereisten en/of standaarden waardoor b.v. het beveiligingsniveau onzeker is, kan een risicoanalyse, penetratietest of ander aanvullend onderzoek vereist zijn om de kwaliteit van het informatiesysteem te borgen. Resultaat van een dergelijk onderzoek kan leiden tot een aangepaste set aan vereisten of aanvullende maatregelen.

De afweging en mogelijke uitvoering van een onderzoek zijn de verantwoordelijkheid van Ipse de Bruggen. Indien de resultaten van het onderzoek aantonen dat er sprake is van ontwerp- en/of ontwikkelfouten of er is sprake van nalatigheid binnen gebieden als b.v. security by design/default, zullen de kosten van het onderzoek worden verhaald op de leverancier.

## 4. *Aansluiteisen*

| ID | Naam voorwaarde | Omschrijving voorwaarde |
|---|---|---|
| 1. | KvK nummer | De leverancier dient een vestiging in Nederland te hebben en heeft zich ingeschreven in het Nederlandse handelsregister van de Kamer van Koophandel. |
| 2. | Voldoen aan NEN7510-1 (*of gelijkwaardig)* | Een van de leverancier onafhankelijke IT auditor heeft vastgesteld dat wordt voldaan aan de door de Stichting Nederlands Normalisatie-Instituut uitgegeven norm 7510-1:2017 (of gelijkwaardig). |
| 3. | Aansprakelijkheidsverzekering | De leverancier heeft zich adequaat verzekerd en zal zich gedurende de looptijd van de Overeenkomst verzekerd houden voor wettelijke aansprakelijkheid en beroepsaansprakelijkheid. |
| 4. | Gegevensuitwisseling niet buiten Europa | Persoonsgegevens die aan een verwerking worden onderworpen of die bestemd zijn om na hun doorgifte te worden verwerkt, worden alleen naar een persoon of systeem binnen een land in de Europese Unie doorgegeven. Zie ook de meest actuele verwerkersovereenkomst van Ipse de Bruggen. |
| 5. | Melding datalek | De leverancier zal een gebeurtenis waarvan redelijkerwijs kan worden aangenomen dat deze geleid heeft, leidt of kan leiden tot een aanmerkelijke kans op verlies of onrechtmatige verwerking van persoonsgegevens (datalek) per omgaande melden bij de verantwoordelijk functionaris die bij de leverancier hiervoor is aangesteld.<br><br>Indien de leverancier een datalek constateert waarbij persoonsgegevens van Ipse de Bruggen betrokken zijn, informeert de leverancier Ipse de Bruggen onmiddellijk na constatering, conform de meest actuele verwerkersovereenkomst. |

| | | |
|---|---|---|
| 6. | Controle van logboeken | Aanmeldingen (of aanmeldpogingen) bij het aangeboden systeem (of de backend daarvan) dienen te worden gelogd in een ‘open-standaard’ indeling. De resulterende logboeken dienen regelmatig te worden gecontroleerd door de leverancier op onbevoegde raadplegingen. Verdachte situaties en/of incidenten dienen te worden gemeld bij Ipse de Bruggen. Ipse de Bruggen kan inzage in de logboeken opvragen. |
| 7. | Protocollen en/of cryptografie | Bij het inzetten van protocollen en/of cryptografie (waaronder SSL en TLS) wordt gebruik gemaakt van versies die gangbaar zijn en actueel ondersteund worden.<br><br>Hier hanteert Ipse de Bruggen o.a. de richtlijnen en eisen zoals die te vinden zijn op **www.ncsc.nl**.<br><br>Verlopen (end of life) versies worden als onveilig beschouwd, niet geaccepteerd en dienen door de leverancier te worden vervangen door veilige en actuele alternatieven.<br><br>Dit geldt ook tijdens de contractperiode. Wanneer een protocol de status ‘end of life’ krijgt dient hier passend en binnen een termijn van drie maanden op geacteerd te worden. Niet voldoen wordt gezien als een afwijking van de dienstverlening. |
| 8. | Authenticatie en autorisatie | Voor authenticatie en autorisatie van (natuurlijke en niet natuurlijke) gebruikers, wordt gebruik gemaakt van Microsoft Active Directory (AD) en/of Microsoft Azure Active Directory (AAD). Ipse de Bruggen is hiermee in principe identity provider.<br><br>Bij toepassing van server applicaties worden standaard Microsoft modules/software componenten gebruikt, waarbij authenticatie op beveiligde wijze plaatsvindt. Autorisaties worden waar mogelijk middels accounts en groepen in AD/AAD toegekend.<br><br>Voor o.a. SaaS heeft authenticatie via AAD de voorkeur. Andere methodieken zoals ADFS zijn onder voorwaarden mogelijk.<br><br>Wanneer een toepassing (mede) wordt geleverd als APP voor een Smart Phone of tablet dient deze toepassing iOS en de daaronder geldende authenticatie methodieken te ondersteunen. Zie ook punt 20. |

| | | |
|---|---|---|
| 9. | Multi Factor Authenticatie | Ipse de Bruggen werkt in volgens een ‘zero trust’ principe waarbij tal van aspecten worden gewogen voordat toegang tot de infrastructuur van Ipse de Bruggen wordt toegestaan.<br><br>Eén aspect is het inzetten van een extra factor naast een gebruikersnaam en een wachtwoord.<br>Voor toepassingen die werken met bijzondere persoons- of medische gegevens kan het noodzakelijk zijn om een gebruiker per sessie te verplichten een vorm van MFA aan te bieden.<br><br>Er dient hoe dan ook gebruik gemaakt te worden van de MFA oplossing zoals die bij Ipse de Bruggen wordt ingezet. Deze is op basis van de Microsoft Enterprise Mobility & Security suite. |
| 10. | Single Sign-On (SSO) | Het informatieysteem ondersteunt de inzet van Single Sign On (SSO) voor authenticatie, gebruikmakend van de in punten 8 en 9 genoemde authenticatie- en autorisatievoorzieningen. |
| 11. | Koppelingen en datastromen | Wanneer er een of meerdere koppelingen noodzakelijk zijn voor het uitwisselen van informatie en/of functionele aspecten, dient dit te geschieden middels een API, geleverd door de leverancier.<br><br>Uitwisseling van gegevens tussen verschillende informatiesystemen dient zo veel als mogelijk rechtstreeks en tussen de diverse informatiesystemen onderling plaats te vinden. Het inzetten van tussenliggende systemen/platformen is in beginsel ongewenst. Overleg en afstemming met andere partijen kan hierbij noodzakelijk zijn.<br><br>Andere oplossingen, zoals b.v. VPNs en/of IPSEC tunnels worden niet toegestaan. Afwijkingen op dit punt worden slechts bij hoge uitzondering en op specifieke gronden geaccepteerd door Ipse de Bruggen.<br><br>Directe koppelingen met de infrastructuur van Ipse de Bruggen zijn in beginsel ongewenst. Hiervoor zal per geval een afweging worden gemaakt of de specifieke oplossing kan worden geaccepteerd. |

| | | |
|---|---|---|
| 12. | Het loggen van systeem en applicatie gebeurtenissen | Het informatiesysteem maakt gebruik van de standaard eventlog faciliteiten (syslog) van het besturingssysteem, waarbij ten minste op basis van applicatie ID, proces/thread ID en een timestamp de applicatie specifieke events zijn te onderscheiden.<br><br>Het informatiesysteem biedt de mogelijkheid om het niveau van logging te specificeren (*trace, debug, information, warning, error, fatal, security*).<br><br>Het logsysteem ondersteund een SIEM-systeem. Ipse de Bruggen maakt gebruik van een SOC waarbij een SIEM is inbegrepen. De logging dient toegankelijk te zijn/worden gemaakt voor het SIEM dat wordt ingezet door de SOC leverancier van Ipse de Bruggen. |
| 13. | Mail integratie | Indien integratie met een e-mailsysteem noodzakelijk is voor de juiste werking van het informatiesysteem, dan wordt dit gerealiseerd d.m.v. de Microsoft Exchange omgeving van Ipse de Bruggen (geen eigen e-mail provider of server).<br><br>Indien er vanuit het informatiesysteem e-mails verstuurd dienen te worden namens (een van) de domein(en) van Ipse de Bruggen, dan dient dit via een smart host methodiek afgeleverd te worden op de e-mail omgeving van Ipse de Bruggen. Communicatie geschiedt op basis van SMTP en TLS. |
| 14. | Licenties en compliance | Het informatiesysteem maakt geen gebruik van hardware (o.a. *dongles en/of usb-keys*) voor licentiebeheer of andere vormen van compliance controle. |
| 15. | Vaste verwijzingen | Het informatiesysteem moet separaat en flexibel (eventueel per gebruiker) configureerbaar zijn en geen vaste verwijzingen bevatten naar:<br><br>• Databasenamen,<br>• Driveletters,<br>• Werkfolders,<br>• UNC paden,<br>• Tijdelijke folders,<br>• IP adressen,<br>• Directory systemen (LDAP),<br>• Domeinnamen,<br>• Licentie-gegevens, c.q. bestand(en),<br>• (Service) accounts,<br>• Omgeving specifieke (OTAP) variabelen,<br>• Configureerbare applicatie instellingen. |

| | | |
|---|---|---|
| 16. | Gebruikersinterface / front end | De gebruikersinterface van het informatiesysteem wordt als webapplicatie aangeboden.<br><br>Traditionele en/of virtuele desktopapplicaties zijn in beginsel ongewenst. Hiervoor zal per geval een afweging worden gemaakt of de geboden methode wordt geaccepteerd en op welke wijze deze zal worden aangeboden aan de gebruikers hiervan.<br><br>Web-toepassingen dienen compatibel te zijn met en ondersteund te worden op de actuele, standaard Microsoft Browser voor Windows.<br><br>Indien het informatiesysteem gericht is op gebruik vanaf een smartphone of tablet (en niet als native app wordt aangeboden) dienen in ieder geval Apple iOS, de standaard browser op dat platform en in sommige gevallen Microsoft Edge op dat platform ondersteund te worden. |
| 17. | Apps voor smartphone en tablet | Apps, die worden ingezet ter ondersteuning en/of gebruik van het informatiesysteem, zijn geschikt voor iPhone en iPad en ondersteunen de meest recente versie van iOS (N) en twee versies daaronder (N-2).<br><br>Gegevens worden niet lokaal opgeslagen. Wanneer dit vereist is dient een passende encryptie toegepast te worden (zie ook punt 7). Indien de App ingezet wordt voor het aanbieden/verwerken van (zeer) gevoelige gegevens is MFA vereist (zie ook punt 9).<br><br>De App of apps moet(en) worden aangeboden en, waar nodig, gemanaged kunnen worden middels Microsoft Intune. |
| 18. | Documentatie | • Van het informatiesysteem is het volgende bekend en beschikbaar voor Ipse de Bruggen:<br>• Change log met wijzigingen t.o.v. de voorgaande versie.<br>• Aanbevolen hardware configuratie voor werkplek- en/of mobiele apparatuur.<br>• Verwerkingswijze van transacties en/of handelingen: batch of (near) real-time.<br>• Afhankelijkheden met andere informatiesystemen en/of applicaties in de vorm van specificaties van software die door het informatiesysteem gebruikt wordt zoals database, databaseversie, benodigde licenties, etc.<br>• Vereiste randapparatuur en de ondersteuning hierop.<br>• Op welke wijze de authenticatie beveiligd is, bijvoorbeeld. b.v. met gebruikersnaam en wachtwoord en/of Multi Factor Authenticatie<br>• Welke autorisaties vereist zijn. |

| | | |
|---|---|---|
| | | • Databeheer:<br>1. bewaartermijn(en)<br>2. databehoefte (verwachte hoeveelheid opslag)<br>3. belangrijke normwaarden<br>4. beschrijving hoe er wordt gehandeld in geval van een verstoring, aanval, dataverlies.<br><br>• Informatie over netwerkconnectiviteit:<br>1. welke protocollen gebruikt het informatiesysteem in communicatie met andere lagen (*tiers*) of andere systemen en/of applicaties<br>2. welke poorten gebruikt het informatiesysteem in communicatie met andere systemen<br>3. lagen (*tiers*) of andere systemen en/of applicaties<br>4. bandbreedtegebruik voor verschillende vormen van functionaliteit (bijv. *queries* uitvoeren, printen, etc.).<br>5. robuustheid van de netwerkcommunicatie bij lage bandbreedte, zoals hoge *latency*<br>6. wat gebeurt er bij uitval van een verbinding / wat zijn de gevolgen voor de gebruiker. |
| 19. | Doorlegplicht kettingbeding | De leverancier heeft de verplichting om de voorwaarden 1 t/m 18 te verleggen (de ketting) en opnieuw het (ketting)beding overeen te komen met een opvolgende bewerker en/of sub-leverancier indien (delen van) het informatiesysteem worden uitbesteed aan een derde partij. |

## 5. *Criteria m.b.t. Informatiebeveiliging*

In voorgaande versies van de aansluit- en implementatievoorwaarden waren een aantal criteria vervat in een bijlage (‘*D09 Checklist Acceptatiecriteria IDB’*). Deze bijlage is met ingang van deze versie komen te vervallen. Alle actuele criteria zijn nu in dit document opgenomen onder punten 5.1 en 5.2.

### **5.1** *Generieke criteria (voor alle toepassingen):*

In het kader van informatiebeveiliging zijn voor Ipse de Bruggen onderstaande elementen van grote waarde. Geef bij elk element aan wat de situatie is m.b.t. de geleverde dienst/oplossing/toepassing (kruis aan wat van toepassing is):

| | |
|---|---|
| De toepassing voldoet aan gangbare eisen m.b.t. privacy by design/default: | ☐ *ja / nee* ☐. |
| De toepassing voldoet aan gangbare eisen m.b.t. security by design/default: | ☐ *ja / nee* ☐. |
| Er is een rollenmatrix beschikbaar: | ☐ *ja / nee* ☐. |
| Accounts binnen het systeem zijn voldoende beveiligd: | ☐ *ja / nee* ☐. |
| Wijzigingen aan accounts, wachtwoorden en/of rollen worden gelogd: | ☐ *ja / nee* ☐. |
| Mutaties van toepassing- en/of systeemgegevens worden gelogd: | ☐ *ja / nee* ☐. |
| Gegevens worden voldoende versleuteld opgeslagen: | ☐ *ja / nee* ☐. |
| Er zijn voorzieningen voor het maken van back-ups (data en logs): | ☐ *ja / nee* ☐. |
| Back-ups kunnen worden versleuteld: | ☐ *ja / nee* ☐. |
| Er zijn voorzieningen voor het herstellen van data uit back-ups: | ☐ *ja / nee* ☐. |
| Back-up en herstel acties worden gelogd: | ☐ *ja / nee* ☐. |

### **5.2** *Specifieke criteria (bij maatwerktoepassingen):*

Voor alle (delen van) toepassingen die als specifiek maatwerk worden ontwikkeld is een aanvullende set aan elementen van toepassing. Geef bij elk element aan wat de situatie is m.b.t. de geleverde dienst/oplossing/toepassing (kruis aan wat van toepassing is):

| | |
|---|---|
| Technisch ontwerp beschikbaar / opgeleverd: | ☐ *ja / nee* ☐. |
| Functioneel ontwerp beschikbaar / opgeleverd: | ☐ *ja / nee* ☐. |
| Documentatie van (eventueel) benodigde API opgeleverd: | ☐ *ja / nee* ☐. |
| Er is een (digitale) handleiding beschikbaar: | ☐ *ja / nee* ☐. |
| Is de handleiding in het Nederlands: | ☐ *ja / nee* ☐. |
| Er is een (beknopte) Nederlandstalige handleiding voor gebruikers: | ☐ *ja / nee* ☐. |
| Het te leveren systeem is afdoende technisch getest en "geslaagd": | ☐ *ja / nee* ☐. |
| Gebruikersacceptatietest is uitgevoerd en als voldoende beoordeeld: | ☐ *ja / nee* ☐. |
| Het product wordt geleverd met een gangbare installatiemethodiek: | ☐ *ja / nee* ☐. |
| Er wordt een configureerbaar product opgeleverd: | ☐ *ja / nee* ☐. |
| Benodigde tools voor het beheer worden meegeleverd: | ☐ *ja / nee* ☐. |