**{project} project**

**Beheer afspraken CareFacts**

**hosting en applicatiebeheer**

Rotterdam, {datum}

# Deelnemende partijen:

**{klant}**

{adres}

KvK nr {nr}, hierna te noemen de **Opdrachtgever**.

Vertegenwoordigd door **{vertegenwoordiger}**

**{hosting provider}**

{adres}

KvK nr {nr}, hierna te noemen de **Hosting provider**.

Vertegenwoordigd door **{vertegenwoordiger}**

**MagnaFacta IT Solutions** (handelsnaam van Thranx Investment B.V.)

Oostzeedijk 314, 3063 CC Rotterdam

KvK nr 24292882, hierna te noemen: **MagnaFacta**.

Vertegenwoordigd door **Matijs de Jong**

**Engon**

Deelshouten 16, 5581 SG Waalre

KvK nr 50842250, hierna te noemen: **Engon**.

Vertegenwoordigd door **Jasper van Gestel**

Engon is een onderaannemer van MagnaFacta die met goedkeuring van de Opdrachtgever maar onder de verantwoordelijkheid van MagnaFacta beheerstaken overneemt. Engon en MagnaFacta werken samen onder de naam CareFacts, hierna gezamenlijk te noemen de **Applicatiebeheerders**.

# Achtergronden

Dit project betreft het hosten van een webapplicatie, gebaseerd op het open source GemsTracker project ([www.gemstracker.org](http://www.gemstracker.org)) en ingericht volgens de methodiek van CareFacts ([www.carefacts.nl](http://www.carefacts.nl)). Het project maakt privacygevoelige patiënt behandel­informatie toegankelijk middels een webapplicatie. Als zodanig dient de hosting te voldoen aan strenge veiligheidsnormen zoals NEN 7510.

De Opdrachtgever sluit een direct contract met de Hosting provider voor het aanbieden van en onderhouden van de website(s) waar de webapplicatie op draait. De Opdrachtgever houdt het eigendom van de webapplicatie en de gegevens.

De Hosting provider is verantwoordelijk voor de oplevering van een veilige hosting omgeving, maar heeft geen kennis van de gebruikte webapplicatie. Daarom sluit de Opdracht­gever een tweede overeenkomst met de Applicatiebeheerders die wel over de benodigde kennis beschikken om de applicatie te onderhouden.

Dit document bevat geen financiële afspraken, maar beschrijft de taakverdeling tussen de Opdrachtgever, de Hosting provider en de Applicatiebeheerders om de in deze overeen­komst genoemde verantwoorde­lijkheden van de partijen vast te leggen. Overige taken en verantwoordelijkheden dient de Opdrachtgever zelf aan de Hosting provider dan wel de Applicatie­beheerders toe te kennen.

# Taakverdeling

## Algemeen

Zowel Hosting provider als de Applicatiebeheerders zullen het plegen van onderhoud in overleg met en na goedkeuring van de Opdrachtgever uitvoeren,   
***met uitzondering wanneer onmiddellijke actie vereist is in verband met beveiliging,***   
indien de Opdrachtgever niet snel genoeg te bereiken is.

De Hosting provider zal de Applicatiebeheerders op de hoogte stellen van onderhoud. De Applicatiebeheerders zullen de Hosting provider op de hoogte stellen indien applicatie onderhoud mogelijk repercussies heeft voor het beheer van de server, bijvoorbeeld als de installatie van nieuwe applicaties vereist is.

## Taken van de Opdrachtgever

1. Het kiezen van een Hosting provider die de vereiste beveiliging levert.
2. Het kiezen voor Applicatiebeheerders met de kennis om de applicatie in te richten, te beveiligen en te onderhouden.
3. Het aanstellen van contactperso(o)n(en) met de Hosting provider de Applicatie­beheerders.
4. Het regelen van toegang tot de applicatie voor anderen dan de Applicatie­beheer­ders.
5. Het inlichten van zowel de Hosting provider als de Applicatiebeheerders bij het vermoeden van ongeoorloofde toegang.
6. Het extern laten testen van de applicatie en de server op veiligheid.
7. Het (laten) auditen van het gebruik van de applicatie door bevoegde gebruikers.

## Taken van de Hosting provider

1. Onderhoud van de gebruikte hardware.
2. Bescherming middels een firewall, inclusief IP-level bescherming van taken zoals SSH, phpMyAdmin toegang en andere taken doorgegeven door de Applicatie­beheerders en de Opdrachtgever.
3. Detectie van inbraakpogingen via de firewall en het inlichten van de Opdrachtgever en de Applicatiebeheerders over inbraakpogingen.
4. Het volgens geldende normen veilig inrichten van het besturingssysteem, de webserver, de database server en de PHP-software.
5. Het uitvoeren van updates aan het besturingssysteem, de webserver, de database server en de PHP-software, na goedkeuring van de Opdrachtgever en inlichting van de Applicatiebeheerders.
6. Het eventueel zonder overleg uitvoeren van updates aan het besturingssysteem, de webserver, de database server en de PHP-software indien onmiddellijke actie vereist is voor een veiligheidslek en de Opdrachtgever niet op tijd bereikt kan worden.
7. Het informeren van de Applicatiebeheerders en de Opdrachtgever bij geconsta­teerde veiligheidslekken en gedetecteerde aanvallen, inclusief lekken geïntroduceerd door de Applicatiebeheerders dan wel de Opdrachtgever.
8. Installatie en beheer van software benodigd voor applicatie beheer zoals Git (git-scm.com), Composer (getcomposer.org) en phpMyAdmin (phpmyadmin.net) en andere applicaties op verzoek van de Applicatiebeheerders en de Opdrachtgever.
9. Inrichten en onderhouden van systeemgebruikers voor de gebruikte applicaties.
10. De server inrichten voor het versturen van e-mail vanuit de applicatie.
11. Cron opdrachten instellen op verzoek van de Applicatiebeheerders en de Opdracht­gever.
12. Het inrichten, beveiligen, monitoren en onderhouden op netwerkniveau van verbindingen met andere systemen, zoals VPN en IPSec-verbindingen.
13. De Applicatiebeheerders en indien gewenst de Opdrachtgever toegang geven tot de server voor applicatie beheer middels een SSH-account en voor database beheer middels een MySQL administratief account.
14. Toegang tot de server van derden tegenhouden.
15. De Opdrachtgever te ondersteunen bij security audits.

## Taken van de Applicatiebeheerders

1. Het volgens geldende normen veilig inrichten van applicatie en het inlichten van de Hosting provider en de Opdrachtgever indien hiervoor wijzigingen nodig zijn op de server die de Applicatiebeheerders niet zelf kunnen uitvoeren.
2. Het volgens geldende normen veilig en privacy gericht inrichten van MySQL databases voor gebruik door de applicatie onderdelen.
3. Onderhoud van de applicatiesoftware, na overleg met de opdrachtgever.
4. Het informeren van de Hosting provider en de Opdrachtgever bij geconstateerde veiligheidslekken en gedetecteerde aanvallen, inclusief lekken geïntroduceerd door de Hosting provider dan wel de Opdrachtgever.
5. Het eventueel zonder overleg uitvoeren van onderhoud, indien onmiddellijke actie vereist is voor een veiligheidslek en de Opdrachtgever niet op tijd bereikt kan worden.
6. De Opdrachtgever toegangsrechten geven om gebruikers aan te maken, te onder­houden en te deactiveren.
7. Op verzoek van de Opdrachtgever toegangsrechten van gebruikers intrekken of wijzigen.
8. De Opdrachtgever voor te lichten over het gebruik van de applicatie, inclusief voor­lichting over het veilig gebruik van de applicatie.
9. De Opdrachtgever te waarschuwen indien onveilig gebruik van de applicatie gecon­sta­teerd wordt.
10. Het inrichten, beveiligen en onderhouden van applicatiesoftware voor verbindingen met andere systemen.
11. Het (functioneel) monitoren van verbindingen met andere systemen.
12. De Opdrachtgever te ondersteunen bij security audits.

# Ondert**e**kening

|  |  |  |
| --- | --- | --- |
| Namens de Opdrachtgever | | |
|  | Datum | Plaats |
|  | | |
| Namens de Hosting provider | | |
|  | Datum | Plaats |
|  | | |
| Namens de Applicatiebeheerders | | |
| Matijs de Jong | Datum | Plaats |