**Handreiking programma van eisen Haven**

**Versie 1.0, gepubliceerd op de Haven website op 18 augustus 2022**

**Disclaimer**

U kunt na de nodige aanpassingen te hebben gedaan dit document invoegen in een aanvraag evenals bijvoorbeeld algemene voorwaarden. Let op: er kunnen geen rechten worden ontleend aan deze handreiking. Het is van belang dat u inhoudelijk het document doorneemt en waar nodig aanpast.

**Introductie**

Gemeenten maken gebruik van verschillende soorten platforms waarop hun applicaties draaien. De werking van deze platforms is echter zodanig verschillend dat het nodig kan zijn een applicatie aan te passen voordat deze succesvol op het gewenste platform gebruikt kan worden. Dit is niet alleen kostbaar, tijdrovend en omslachtig, maar werkt ook belemmerend voor de gezamenlijke ontwikkeling en het onderling hergebruik van applicaties door gemeenten.

Om hier een oplossing voor te bieden is, als onderdeel van de door VNG Realisatie uitgevoerde Common Ground activiteiten, Haven ontwikkeld (zie ook https://haven.commonground.nl). Haven kan worden geïnstalleerd op de meest gebruikte platforms en vormt dan een nieuwe laag waarop applicaties kunnen worden geïnstalleerd. Een applicatie die op Haven geïnstalleerd kan worden, kan daarmee ook worden geïnstalleerd op ieder (ander) onderliggend platform waarop Haven is geïnstalleerd.

Voordat gemeenten echter gebruik kunnen maken van de voordelen van Haven, zal Haven moeten worden geïnstalleerd op in gebruik zijnde of nieuwe platforms, en vervolgens worden beheerd. In dit document wordt aan gemeenten die gebruik willen gaan maken van Haven een suggestie gedaan van eisen die gesteld kunnen worden aan een opdrachtnemer die Haven installeert en beheert. Omdat de IT-infrastructuren van gemeenten verschillend zijn en worden geleverd/ondersteund door verschillende partijen, is het niet mogelijk één universele set eisen op te stellen die passend is voor iedere situatie. Gebruikers van dit document zullen daarom steeds kritisch moeten kijken welke eisen in hun situatie bruikbaar zijn en of de eisen inhoudelijk goed aansluiten bij eventuele andere afspraken die met leveranciers van aan Haven gerelateerde infrastructuur zijn gemaakt.

1. **Beveiligingseisen**

|  |  |
| --- | --- |
| **nr** | **Omschrijving** |
| 1-1 | De opdrachtnemer dient te zijn gecertificeerd volgens de NEN-ISO/IEC 27001 norm voor informatiebeveiliging, of de opdrachtnemer dient een gelijkwaardig, op de NEN-ISO/IEC 27001 norm gebaseerd managementsysteem voor informatieveiligheid te hebben geïmplementeerd. |
| 1-2 | De opdrachtnemer dient een actueel beveiligingsbeleid te hanteren dat is gebaseerd op de Code voor Informatiebeveiliging, NEN-ISO/IEC 27002. |
| 1-3 | De opdrachtnemer staat ervoor in dat de opdrachtgever met de door opdrachtnemer geleverde dienstverlening kan voldoen aan de Baseline Informatiebeveiliging Overheid (BIO, op het moment van publicatie van dit document te vinden op https://www.informatiebeveiligingsdienst.nl/product/baseline-informatiebeveiliging-overheid-bio/), of de eventuele toekomstige opvolgers van de BIO. Uitgangspunt hierbij is dat de scope en reikwijdte van deze eventuele opvolgers van de BIO niet wezenlijk wijzigen en net als de BIO een afgeleide zullen zijn van NEN-ISO/IEC 27001 en 27002 standaarden. |
| 1-4 | Als de dienstverlening (gedeeltelijk) door de opdrachtnemer beheerd wordt (bijv. bij hosting), of het dienstverlening betreft die door de opdrachtnemer verricht wordt, staat de opdrachtnemer er (voor dat deel) voor in dat de dienstverlening voldoet aan de in de vorige eis bedoelde norm voor informatiebeveiliging (BIO). |
| 1-5 | De opdrachtnemer legt ten minste een algemene beschrijving van de in de vorige eis bedoelde getroffen technische en organisatorische beveiligingsmaatregelen schriftelijk vast en geeft deze ter inzage aan de opdrachtgever. |
| 1-6 | Als een specifieke beveiligingsmaatregel van de opdrachtnemer voldoet aan de BIO (of de eventuele opvolger van de BIO) maar niet overeenkomt met een door de opdrachtgever voorgeschreven oplossing, dan dient de opdrachtnemer deze maatregel op verzoek van de opdrachtgever aan te passen tenzij de opdrachtnemer relevante, zwaarwegende argumenten heeft om de aanpassing niet door te voeren. Voor een dergelijke aanpassing op basis van een verzoek van de opdrachtgever kan de opdrachtnemer, na het doorlopen van een offertetraject, kosten in rekening kan brengen. |

1. **Implementatie**

|  |  |
| --- | --- |
| **nr** | **Omschrijving** |
| 2-1 | De opdrachtnemer heeft kennisgenomen van de informatie die over Haven beschikbaar is op <https://haven.commonground.nl> en verklaart door het aannemen van de opdracht dat hij met deze informatie in staat is een Haven omgeving te installeren op het (de) in de opdracht aangegeven platform(s). |
| 2-2 | De opdrachtnemer implementeert Haven op het (de) door de opdrachtgever aangewezen platform(s), na door de opdrachtgever, voor zover nodig, te zijn voorzien van de hiervoor benodigde toegangsrechten. |
| 2-3 | De opdrachtnemer toont met behulp van de Haven Compliancy Checker aan de opdrachtgever aan dat de nieuw geïnstalleerde Haven omgeving voldoet aan de Haven standaard. |

1. **Beheer – technisch/functioneel**

*De gebruiker van dit document kan indien gewenst zelf eisen toevoegen om integratie met andere door hem gebruikte systemen te borgen. Denk hierbij bijvoorbeeld aan integratie met een eigen Active Directory omgeving om via deze omgeving in de Haven omgeving in te loggen. De gebruiker dient zelf vast te stellen welke integratiemogelijkheden hij wenst en eventueel af te stemmen met potentiële leveranciers of zij de gewenste integratiemogelijkheden kunnen bieden.*

|  |  |
| --- | --- |
| **nr** | **Omschrijving** |
| 3-1 | De opdrachtnemer hanteert een upgradestrategie waarmee wordt geborgd dat de opdrachtgever/gebruiker geen downtime ervaart. |
| 3-2 | De opdrachtnemer draagt zorg voor de aanwezigheid van een up-to-date geheel van systemen/componenten waarmee professioneel beheer van de Haven omgeving kan worden uitgevoerd, waaronder in ieder geval een logging oplossing. |
| 3-3 | De opdrachtnemer controleert iedere kalendermaand met behulp van de Haven Compliancy Checker of de door hem beheerde Haven omgeving nog voldoet aan de Haven standaard. Het resultaat hiervan wordt binnen een dag na uitvoering van de check gerapporteerd aan de opdrachtgever. |
| 3-4 | Als uit de Haven Compliancy Checker blijkt dat niet (meer) wordt voldaan aan de Haven standaard dan meldt de opdrachtnemer dit direct na constatering aan de opdrachtgever. De opdrachtnemer zorgt er daarnaast voor dat de Haven omgeving binnen drie kalendermaanden alsnog/weer aan de Haven standaard voldoet. |
| 3-5 | De opdrachtnemer dient ervoor te zorgen dat een major release van Haven binnen uiterlijk drie kalendermaanden is doorgevoerd op de door hem beheerde Haven omgeving. |
| 3-6 | De opdrachtnemer dient ervoor te zorgen dat een patch of minor release van Haven binnen uiterlijk één kalendermaand is doorgevoerd op de door hem beheerde Haven omgeving. |
| 3-7 | De opdrachtnemer verschaft op verzoek van de opdrachtgever aan een leverancier van een applicatie alle toegangsrechten die nodig zijn om de betreffende applicatie te kunnen installeren en beheren op de door de opdrachtnemer beheerde Haven omgeving. |
| 3-8 | De opdrachtnemer verschaft op verzoek van de opdrachtgever aan een auditor alle toegangsrechten die nodig zijn voor het uitvoeren van een audit op de door de opdrachtnemer beheerde Haven omgeving. |

1. **Beheer - Incidentafhandeling**

|  |  |
| --- | --- |
| 4-1 | De opdrachtnemer dient een incidentdesk te hebben. De incidentdesk is een centraal punt bij de opdrachtnemer voor het aanmelden en afmelden van alle incidenten betreffende alle producten en diensten die de opdrachtnemer levert. De incidentdesk verschaft tevens statusinformatie over de aangemelde incidenten. |
| 4-2 | De incidentdesk dient via verschillende communicatiemiddelen (minimaal: telefoon, e-mail en online) bereikbaar te zijn. |
| 4-3 | De opdrachtgever en door de opdrachtgever geautoriseerde contactpersonen dienen 7 dagen per week, 24 uur per dag in contact te kunnen treden met de incidentdesk. |
| 4-4 | Bij telefonisch contact vanuit Nederland dient de incidentdesk gratis of tegen het reguliere tarief voor bellen binnen Nederland bereikbaar te zijn (geen internationale nummers, geen betaalde servicenummers). |
| 4-5 | De opdrachtnemer dient ieder aangemeld incident in behandeling te nemen, ook als het incident (mogelijk) betrekking heeft op het onderliggende platform waar Haven op draait of betrekking heeft op een applicatie die op Haven draait. |
| 4-6 | Als de opdrachtnemer concludeert dat het aangemelde incident niet door de door hem beheerde Haven omgeving wordt veroorzaakt, maar wordt veroorzaakt door andere door hem beheerde infrastructuur (bijvoorbeeld het onderliggende platform of een op Haven draaiende applicatie), dan wordt het incident beschouwd als direct op de juiste manier te zijn aangemeld en dient de opdrachtnemer het incident op te lossen binnen dezelfde kaders die gelden voor het rechtstreeks aanmelden van incidenten bij de betreffende andere infrastructuur. |
| 4-7 | Als de opdrachtnemer ervan overtuigd is dat het aangemelde incident niet wordt veroorzaakt door de door hem beheerde Haven omgeving, maar door infrastructuur (bijvoorbeeld het onderliggende platform of een op Haven draaiende applicatie) die niet door de opdrachtnemer wordt beheerd, dan dient de opdrachtnemer de aanmelder van het incident hiervan op de hoogte te brengen. De opdrachtnemer dient bij terugmelding onderbouwd aan te geven op welke infrastructuur het incident wel betrekking heeft. |
| 4-8 | De opdrachtnemer dient bij hem aangemelde incidenten die geen betrekking hebben op door hem beheerde infrastructuur op verzoek van de opdrachtgever aan te melden bij de beheerder van de infrastructuur waar het incident wel betrekking op heeft. De opdrachtgever verstrekt hiertoe de contactgegevens van de beheerder van de bedoelde andere infrastructuur. |
| 4-9 | Als de opdrachtnemer onterecht heeft aangegeven dat een bij hem aangemeld incident geen betrekking heeft op door hem beheerde infrastructuur, dan wordt het incident opnieuw bij de opdrachtnemer aangemeld. Het moment waarop het incident initieel is aangemeld (dus voordat de onterechte afwijzing heeft plaatsgevonden) geldt in dit geval als het startmoment van het opnieuw aangemelde incident. |

1. **Beheer - overleg**

|  |  |
| --- | --- |
| **nr** | **Omschrijving** |
| 5-1 | Tussen de opdrachtgever en de opdrachtnemer vindt één keer per kwartaal overleg plaats. Dit overleg spitst zich toe op de overeenkomst, waarbij onder meer gesproken kan worden over:  - aanpassingen aan de overeenkomst;  - marktconformiteit;  - performance van de dienstverlening in het algemeen;  - financiën;  - rapportages;  - servicelevels.  Als daar aanleiding toe is kan op verzoek van de opdrachtgever of de opdrachtnemer de frequentie van dit overleg tijdelijk worden verhoogd. |
| 5-2 | Het overleg tussen de opdrachtgever en de opdrachtnemer vindt digitaal plaats, tenzij één van de partijen van mening is dat een digitaal overleg onvoldoende effectief is. In dat geval dient het overleg fysiek plaats te vinden op een door de opdrachtgever aan te wijzen locatie. |

1. **Servicelevels**

*Hieronder volgt een aantal servicelevels die de gebruiker van dit document kan opnemen. De keuze welke servicelevels worden ingezet en de exacte invulling ervan kunnen echter per gebruiker verschillen, bijvoorbeeld omdat een gebruiker ze in lijn wil brengen met andere al bestaande servicelevels of omdat een gebruiker leveranciers op een andere manier (met andere servicelevels) wenst aan te sturen. De gebruiker van het document dient daarom zelf vast te stellen:*

* *Of hij het servicelevel van toepassing wil verklaren.*
* *Wat de waarde van het servicelevel dient te zijn (bijvoorbeeld oplossing van een incident binnen één uur, twee uur of anders).*
* *Wat de consequentie is als niet aan het servicelevel wordt voldaan (bijvoorbeeld een boete ter hoogte van 3% van de hoogte van de eerstkomende maandfactuur, een boete van € 100,- per overschrijding van het servicelevel, of anders).*

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| 6-1 | De compliancy van de door de opdrachtnemer beheerde Haven omgeving dient te allen tijde te kunnen worden aangetoond met de Haven Compliancy Checker. |
| 6-2 | Een aangemeld incident dat betrekking heeft op de door de opdrachtnemer beheerde Haven omgeving dient binnen één uur nadat het incident is aangemeld te zijn opgelost. |
| 6-3 | De opdrachtnemer dient de aanmelder van een incident binnen een half uur nadat het incident is aangemeld ervan op de hoogte te brengen als het aangemelde incident geen betrekking heeft op de door de opdrachtnemer beheerde Haven omgeving of een andere door de opdrachtnemer beheerde infrastructuurcomponent. |
| 6-4 | De opdrachtnemer dient een bij hem aangemeld incident dat geen betrekking heeft op door hem beheerde infrastructuur binnen een half uur nadat het incident is aangemeld aan te melden bij de beheerder van de infrastructuur waar het incident wel betrekking op heeft (uitsluitend als de opdrachtgever hierom heeft verzocht, de juiste contactgegevens beschikbaar heeft gesteld en de openingstijden van de incidentdesk van de beheerder van de infrastructuur waarop het incident wel betrekking heeft dit mogelijk maken). |

1. **Rapportage**

|  |  |
| --- | --- |
| **nr** | **Omschrijving** |
| 7-1 | De opdrachtnemer rapporteert binnen 10 dagen na het verstrijken van een maand over de beschikbaarheid van de door hem beheerde Haven omgeving over de zojuist verstreken maand. In deze rapportage wordt de opdrachtgever in ieder geval geïnformeerd over:   * Het beschikbaarheidspercentage  (aantal minuten dat de omgeving beschikbaar is geweest gedeeld door het totaal minuten van de maand). * De perioden waarin de Haven omgeving niet beschikbaar is geweest. * De perioden waarin sprake is geweest van gepland en vooraf met de opdrachtgever overeengekomen onderhoud. |
| 7-2 | De opdrachtnemer rapporteert binnen 10 dagen na het verstrijken van een maand over de incidenten die bij hem zijn aangemeld in de zojuist verstreken maand. In deze rapportage wordt de opdrachtgever in ieder geval geïnformeerd over:   * Het aantal aangemelde incidenten. * Het aantal incidenten dat geen betrekking had op door de opdrachtnemer beheerde infrastructuur. * De oplosduur van ieder aangemeld incident dat door de opdrachtnemer zelf is opgelost. * De hoeveelheid verstreken tijd voordat bij de aanmelder van een incident is aangegeven dat het aangemelde incident geen betrekking had op door de opdrachtnemer beheerde infrastructuur. * De hoeveelheid verstreken tijd voordat een incident dat geen betrekking had op door de opdrachtnemer beheerde infrastructuur is aangemeld bij de beheerder van de infrastructuur waarop het incident wel betrekking had (indien van toepassing). |

1. **Audit**

|  |  |
| --- | --- |
| **Nr** | **Omschrijving** |
| 8-1 | De opdrachtgever heeft het recht om bij de opdrachtnemer zelf een audit uit te voeren of door een derde partij een audit uit te laten voeren. |
| 8-2 | Een audit dient plaats te kunnen vinden op de door de opdrachtnemer beheerde Haven omgeving. Aanleiding hiervoor kan bijvoorbeeld zijn:   1. Gerede twijfel bij de opdrachtgever of de Haven omgeving op de juiste manier is geïmplementeerd en ingericht. 2. Gerede twijfel bij de opdrachtgever of de Haven omgeving op de juiste manier functioneert. 3. Overschrijding van de overeengekomen servicelevels. 4. Een verplichting om een audit in te zetten indien dat voor de interne verantwoording van de opdrachtgever noodzakelijk is of dit door een Rekenkamer wordt vereist.   De opdrachtgever zal vooraf aan de opdrachtnemer kenbaar maken wat de aanleiding voor het houden van de audit is. De opdrachtgever zal de scope van de audit beperken tot datgene wat nodig is om een antwoord te krijgen op vragen die verband houden met de aanleiding van de audit. |
| 8-3 | Een audit kan plaatsvinden op andere systemen dan de Haven omgeving die in het kader van de dienstverlening worden gebruikt. Hieronder worden ook niet-elektronisch systemen, zoals bijvoorbeeld een gehanteerd kwaliteitssysteem, bedoeld. Aanleiding hiervoor kan bijvoorbeeld zijn:   1. Gerede twijfel over de juistheid van een factuur of rapportage. 2. Gerede twijfel of het door de opdrachtnemer uitgevoerde kwaliteitsmanagement van voldoende niveau om de geëiste kwaliteit van de dienstverlening te waarborgen. 3. Gerede twijfel of de maatregelen die de opdrachtnemer heeft getroffen op het gebied van informatiebeveiliging passen bij de eisen die door de opdrachtgever aan informatiebeveiliging zijn gesteld. 4. Een verplichting om een audit in te zetten indien dat voor de interne verantwoording van de opdrachtgever noodzakelijk is of dit door een Rekenkamer wordt vereist.   De opdrachtgever zal vooraf aan de opdrachtnemer kenbaar maken wat de aanleiding voor het houden van de audit is. De opdrachtgever zal de scope van de audit beperken tot datgene wat nodig is om een antwoord te krijgen op vragen die verband houden met de aanleiding van de audit. |