WebHare SLA

WebHare bv Hengelosestraat 296 7521 AM Enschede, Nederland info@webhare.nl 053 305 0003
IBAN: NL09 INGB 0008 2421 42 SWIFT/BIC: INGBNL2A BTW: NL8193.19.053.B01
KvK: 08174333 D-U-N-S: 489102945

WebHare

Inhoudsopgave

1 Inleiding

Het doel van deze SLA is het nader specificeren van de eigenschappen van de geboden diensten zoals geldende prestatieniveaus, reactietijden, serviceperiode en beschikbaarheid van de door opdrachtnemer gehoste sites van opdrachtgever.

WebHare behoudt zich het recht voor deze SLA in de toekomst te wijzigen. Deze SLA en eventueel gewijzigde versies worden gepubliceerd op onze website. WebHare bv past bij al haar softwareleveringen en diensten de algemene voorwaarden uit 2020 van NLdigital toe.

De in de SLA genoemde service levels kunnen alleen nagekomen worden indien de afspraken en procedures tussen opdrachtnemer en opdrachtgever eveneens worden nageleefd.

2 Algemeen

2.1 Rangorde overeenkomsten

In geval van tegenstrijdigheden of onduidelijkheden in de bovengenoemde overeenkomsten prevaleert een overeenkomst van hogere rangorde. De rangorde van de diverse overeenkomsten is hieronder aangegeven.

1. Schriftelijke afspraken tussen opdrachtnemer en opdrachtgever
2. Service Level Agreement

2.2 Omschrijving van de diensten

2.2.1 Dedicated Virtual Server Hosting

Dedicated Virtual Server Hosting is gericht op het onderhouden en monitoren van de voor de diensten aangewende apparatuur, operating system en CMS (WebHare A.P.). Dit betekent dat applicaties op de apparatuur de verantwoordelijkheid zijn van de opdrachtnemer.

2.2.2 Algemene inspanningsplicht van partijen

Opdrachtnemer spant zich ervoor in dat de diensten te allen tijde probleemloos beschikbaar zijn. In het geval dat een storing de beschikbaarheid vermindert, verplicht opdrachtnemer zich tot het oplossen van de storing binnen de in deze SLA overeengekomen termijnen. Opdrachtgever verplicht zich tot het correct omgaan met het ter beschikking gestelde CMS. Opdrachtnemer zorgt dat dit bij normaal gebruik niet leidt tot storingen.

2.2.3 Duur van de Service Level Agreement

De Service Level Agreement gaat in vanaf de aanvang van de dienstverlening en duurt voort tot de dienstverlening beëindigd is.

3 Bepalingen aangaande maintenance en service

3.1 Service-window

Service-window omvat de bereikbaarheid van opdrachtnemer voor meldingen anders dan prioriteit 1 conform de prioriteitentabel onder 3.2.

Window	Omschrijving
Window	Maandag t/m vrijdag van 09:00 tot 17:00 uur, m.u.v. officiële feestdagen in Nederland.
Service-uur	Een uur dat valt binnen het service-window.

3.2 Prioriteitentabel

Aanduiding van prioriteiten zoals gedefinieerd binnen deze SLA.

Prioriteit	Betekenis
P1	Uitval van de dienstverlening (bedrijfskritisch / security incident)
P2	Gedeeltelijk onderbroken / verminderde prestatie (bedrijfskritisch)
P3	Problemen met beperkte gevolgen voor opdrachtgever (operational issue)
P4	Vraag / wijzigingsverzoek

3.3 Maintenance window

Opdrachtnemer streeft ernaar updates binnen het maintenance window (onderhoudsvenster) uit te voeren.

Window	Omschrijving
Window	Maandag tussen 17:00 en 20:00 uur.

3.4 Reactietijdentabel

Reactietijden zoals gedefinieerd binnen deze SLA.

Prioriteit	Reactietijd	Oplostijd	Betekenis
P1	< 60 minuten	< 12 uur	Melding uitsluitend via telefoon en/of overeengekomen meldingsprocedure.
P2	< 2 service-uren	< 8 service-uren	Melding via telefoon, support@webhare.nl of gitlab.webhare.com issue tracker. Tijdens service-window.
P3	< 16 service-uren	< 8 service-uren	Melding via telefoon, support@webhare.nl of gitlab.webhare.com issue tracker. Tijdens service-window.

P4	2 werkdagen	Best effort	Melding via telefoon, support@webhare.nl of gitlab.webhare.com issue tracker. Tijdens service-window.

Reactietijd: Deze tijd begint te tellen vanaf het moment dat het incident is aangemeld totdat gestart wordt met werken aan een oplossing voor het incident.

Oplostijd: Deze tijd begint te tellen vanaf het moment dat het incident is aangemeld totdat het incident is opgelost. Dit is exclusief de tijd die benodigd is voor uitlevering, testen en acceptatie door de opdrachtgever.

In het geval een reactie- en/of oplostijd niet gerealiseerd kan worden, dan verplicht opdrachtnemer zich per omgaand contact, bij voorkeur telefonisch, met opdrachtgever hieromtrent op te nemen.

3.5 Back-up

Tenzij anders overeengekomen, worden data back-ups dagelijks gemaakt. Een back-up wordt gemaakt met als doel het herstel bij catastrofale gebeurtenissen en zal dan ook altijd integraal worden teruggezet. Voor het terughalen van data op verzoek van opdrachtgever kunnen supportkosten of hostingkosten (voor een extra server waarop de back-up beschikbaar wordt gemaakt) in rekening worden gebracht.

3.6 Onderhoud

Voor alle vitale onderdelen van de centrale infrastructuur van opdrachtnemer geldt dat gepland onderhoud op tijden plaatsvindt wanneer de gebruikers er zo weinig mogelijk last van hebben.

Onder gepland onderhoud vallen preventief onderhoud (het aanpassen van systemen aan omstandigheden die zijn gewijzigd of zullen wijzigen) en innovatief onderhoud (het toevoegen of verbeteren van de prestaties van de systemen).

Opdrachtnemer beoogt om bij onderhoudswerkzaamheden aan haar netwerk, servers of andere relevante apparatuur de merkbare invloed op de dienstverlening richting de opdrachtgever tot het uiterste minimum te beperken door de volgende maatregelen te hanteren:

- belangrijke handelingen worden, voor zover mogelijk, buiten kantoortijden uitgevoerd;
- merkbare onderhoudswerkzaamheden worden tot een absoluut noodzakelijk minimum beperkt;
- onderhoudswerkzaamheden zullen zoveel mogelijk worden gecombineerd.

Tijdens het onderhoud kan er merkbare invloed zijn op de dienstverlening (prioriteitsniveau 2 of 3), opdrachtnemer spant zich in dat er geen uitval van de dienst zal plaatsvinden (prioriteitsniveau 1).

3.6.1 Gepland onderhoud

Gepland onderhoud waarbij meer dan 15 minuten uitval wordt verwacht, zal de volgende informatie bevatten en minimaal 2 weken voor aanvang van de werkzaamheden worden aangekondigd:
- tijdskader waarin het gepland onderhoud zal plaatsvinden;
- verwachte feitelijke duur van het gepland onderhoud;
- de diensten waarop het geplande onderhoud van invloed zal zijn.

Gepland onderhoud is uitgesloten van de beschikbaarheidsberekeningen tenzij de periode voor het geplande onderhoud wordt overschreden en de hostingdienst daardoor voor de opdrachtgever niet beschikbaar is.

3.6.2 Noodonderhoud

Noodonderhoud kan nodig zijn wanneer omstandigheden onmiddellijk ingrijpen vereisen. In een dergelijke situatie wordt de opdrachtgever zo spoedig mogelijk geïnformeerd (zie: reactietijden). Onbeschikbaarheid tijdens noodonderhoud telt mee in de beschikbaarheidsberekening.

3.7 Preventie

Opdrachtnemer monitort de server en gebruikte software voor mogelijke (toekomstige) problemen die de beschikbaarheid kunnen beïnvloeden. Onderhoud dat nodig is voor deze preventie (denk bv. aan veiligheidsupdates) wordt bij voorkeur tijdens gepland onderhoud uitgevoerd maar kan een reden zijn voor noodonderhoud indien het anders gelopen risico dit vereist.

3.8 Uitsluitingen

Uitgesloten van deze overeenkomst zijn:

- Ontwikkel-, test- en acceptatieomgevingen
- Eventueel aangeboden e-mail voorzieningen behorende bij domeinregistratie (e-mail via de (portal).webhare.com servers)

4 Beschikbaarheid

4.1 Garantie van beschikbaarheid

Voor de beschikbaarheid van de hostingomgeving geldt een garantie zoals is opgenomen in 4.2 beschikbaarheid op maandbasis. De procedure voor het beschikbaar stellen van het netwerk en de systeemomgeving zijn opgenomen in de overeenkomst tussen opdrachtgever en opdrachtnemer.

Opdrachtnemer garandeert niet dat er altijd communicatie over het internet mogelijk is of dat er altijd een verbinding tot stand kan worden gebracht met een andere machine aangesloten op het internet. Beschikbaarheid wordt uitsluitend bepaald vanuit het netwerk van opdrachtnemer zelf.

De verantwoordelijkheid van opdrachtnemer met betrekking tot beschikbaarheid zoals geformuleerd in deze SLA zijn niet van toepassing op storingen indien:

- geplande werkzaamheden worden uitgevoerd in het maintenance window;
- de storing optreedt als gevolg van storing in de telecommunicatie infrastructuur van derden, anders dan door de leverancier gekozen hostingpartners;
- een uitval veroorzaakt wordt door het wegvallen van eventuele VPN verbindingen tussen systemen van opdrachtnemer en opdrachtgever, tenzij die storing aan opdrachtnemer te verwijten valt;
- een uitval veroorzaakt wordt door ongeautoriseerde wijzigingen door personeel van de opdrachtgever in het CMS van de opdrachtnemer;
- deze gevolg zijn van handelen in in strijd met deze SLA of de algemene voorwaarden;
- overmacht, onder overmacht wordt verstaan een tekortkoming die opdrachtnemer niet kan worden toegerekend, indien zij niet is te wijten aan zijn schuld, noch krachtens wet, rechtshandeling of in het verkeer geldende opvattingen voor zijn rekening komt.

4.2 Beschikbaarheid

Er wordt een beschikbaarheid gegarandeerd van minimaal 99,5%. Beschikbaarheid wordt als volgt gemeten: de website is niet beschikbaar als deze niet of niet goed functioneert vanwege een (technische) storing. De niet-beschikbaarheid gaat in op moment dat een monitoringsysteem (bv. Nagios) het constateert. De beschikbaarheid wordt per kalendermaand gemeten.
Bij ernstige calamiteiten kan opdrachtnemer (tijdelijk of permanent) op een andere fysieke locatie hosten binnen de 3.4 gestelde reactietijd.

4.3 Boete bij niet-beschikbaarheid

Wanneer de beschikbaarheid zoals gegarandeerd in 4.2 niet gehaald wordt, zal opdrachtnemer op verzoek aan de opdrachtgever 10% van de maandelijkse prijs (exclusief BTW) terugbetalen voor elke halve procentpunt aan niet-beschikbaarheid onder de gegarandeerde beschikbaarheid, tot een maximum van 75% van het die maand voor de hosting gefactureerde bedrag.
Als een opdrachtgever in aanmerking meent te komen voor een vergoeding, dient deze de claim (op straffe van verval) uiterlijk binnen drie maanden na constatering van de tekortkoming schriftelijk of als klacht naar informatiebeveiliging@webhare.nl gemaild aan opdrachtnemer kenbaar te maken.
De vergoeding zal worden terugbetaald middels een creditering op de eerstvolgende factuur.

5 Incident management

5.1 Doel

Incident management heeft tot doel (dreigende) storingen in de dienstverlening aan opdrachtgever zo snel mogelijk te verhelpen. De opdrachtgever moet zo min mogelijk hinder van storingen ondervinden en zo snel mogelijk met de normale werkzaamheden door kunnen gaan.
Dit wordt gedaan door het aannemen, beoordelen, oplossen en afmelden van meldingen van opdrachtgever.

5.2 Invoer

Een melding van opdrachtgever dient te worden ingediend via één van de door opdrachtnemer aangewezen kanalen. In ieder geval aangewezen zijn: het standaard telefoonnummer van opdrachtnemer, per e-mailadres support@webhare.nl en het issue tracker systeem Gitlab.

De melding moet de volgende onderdelen bevatten:

- naam melder;
- telefoonnummer en e-mailadres melder;
- de datum (evt. tijdstip) waarop het incident ontstaan is;
- omschrijving van het incident;
- module waar het incident zich voordoet;
- een geschatte prioriteit van opdrachtgever.

5.3 Uitvoer

Voor het verwerken van problemen, wijzigingen en bugs in het systeem wordt gebruikgemaakt van het issue tracker systeem Gitlab, waardoor de diverse vragen en wijzigingen meteen worden gedocumenteerd, incl. eventuele oplossingen door de opdrachtnemer. Deze informatie kan als naslagwerk worden gebruikt.

Een incident wordt als opgelost beschouwd wanneer:
a) de storing opgeheven is naar het oordeel van opdrachtnemer;
b) een workaround ingevoerd is die de storing minimaliseert én het proces is opgestart voor een structurele maatregel.

6 Beveiliging

6.1 Beveiligingsmaatregelen

Opdrachtnemer erkent het belang van een zeer scherpe beveiliging van de omgeving van de opdrachtgever en beschikt over een ISO 27001 informatiebeveiliging certificering.

Opdrachtnemer houdt zich regelmatig op de hoogte van de laatste informatie omtrent beveiliging. Ten einde een optimale beveiliging te garanderen nemen opdrachtnemer en opdrachtgever de onderstaande maatregelen:

- Opdrachtgever is verantwoordelijk voor de personen die zij door middel van het verlenen van autorisatie, toegang verschaft tot de software die behoort tot de systeemomgeving alsmede de applicaties. Opdrachtgever en opdrachtnemer zullen in gezamenlijk overleg nadere afspraken maken over te hanteren regels en richtlijnen ten aanzien van het door opdrachtgever gewenste beveiligingsbeleid.
- Indien een server is getroffen door een beveiligingsincident, zal opdrachtnemer beraadslagen wat de te volgen stappen zijn, indien het nodig is zullen patches op korte termijn geïnstalleerd worden. Indien hierbij onderbreking van de service van opdrachtnemer plaatsvindt dan wordt opdrachtgever onverwijld hiervan op de hoogte gesteld.
- In het geval van ernstige security problemen, in hardware of software, zal opdrachtnemer beraadslagen wat de te volgen stappen zijn. Indien het nodig is, zullen patches op korte termijn geïnstalleerd worden. Wanneer dit niet toereikend blijkt te zijn zal opdrachtnemer na overleg overgaan tot het opnieuw inrichten van de dienst. Indien hierbij onderbreking van de service van opdrachtnemer plaatsvindt dan wordt opdrachtgever onverwijld hiervan op de hoogte gesteld.
- Opdrachtnemer verleent haar medewerking aan security audits en penetration tests, mits deze de beschikbaarheid van de dienstverlening van opdrachtnemer niet in gevaar brengen en de opdrachtnemer de resultaten eveneens ongefilterd zal ontvangen; zulks ter beoordeling door opdrachtnemer. De kosten van een security audit en penetration test zijn voor opdrachtgever. Verzoeken moeten minstens 2 maanden voorafgaande aan de geplande audit of penetration test schriftelijk worden ingediend. Opdrachtgever dient opdrachtnemer te vrijwaren van alle schadeclaims van derden in verband met een dergelijke audit of test.