Bijlage 1.2: Technische eisen aansluiting webshop

INFORMATIEBEVEILIGING	
NR.	**OMSCHRIJVING**
1.	Inschrijver is bekend met de wetgeving bescherming persoonsgegevens en heeft procedures beschikbaar indien er een melding dient plaats te vinden.
2.	De beherende partij / hostende partij van de webwinkel beschikt over een ISO27001 of een minimaal gelijkwaardig certificaat

BESCHIKBAARHEID	
NR.	**OMSCHRIJVING**
3.	Met betrekking tot de beschikbaarheid van het productie systeem geldt het volgende: - Beschikbaarheidsvenster: 00-24.00, 365 dagen per jaar; - Beschikbaarheidseis: 97%; - Ultimo mag de Productie omgeving (inclusief onderliggende infra) in een jaar tijd maximaal 60 uur niet beschikbaar zijn tussen 09.00 en 17.00. Dit afgezien van de afgestemde onderhouds-vensters.
4.	Met betrekking tot de beschikbaarheid van het OTA systeem geldt het volgende Beschikbaarheidsvenster: 09.00-17.00 werkdagen; Beschikbaarheidseis: 95,0%; - Ultimo mag de OTA-omgeving (inclusief onderliggende infra) in een jaar tijd maximaal 100 uur niet beschikbaar zijn tussen 09.00 en 17.00 op werkdagen. Dit afgezien van de afgestemde onderhouds-vensters.
5.	Het datacenter waar de module gehost wordt bevindt zich binnen de Europese Economische Ruimte.

WEB- EN PORTAL	
NR.	**OMSCHRIJVING**
6.	De inschrijver garandeert dat het dataverkeer binnen het vaste bedrag per maand is opgenomen.
7.	De inschrijver monitort de webomgeving dagelijks en schakelt indien nodig extra capaciteit bij om de webdienst naar behoren te laten werken.
8.	De Opdrachtnemer stelt in productie één versie beschikbaar van de dienst aan de medewerkers van Opdrachtgever.
9.	De Opdrachtnemer stelt de eerstvolgende versie op tijd beschikbaar van de dienst aan een klein deel van de gebruikers om een gebruikersacceptatie (GAT) mogelijk te maken.
10.	De verbinding van en naar de website dient beveiligd en versleuteld te zijn d.m.v. geldige certificaten en TLS verbinding over TCP poort 443.
11.	Medewerkers van Opdrachtgever hebben een eigen inlog op het portal en kunnen beheer uitvoeren over gebruikersaccounts en aangeboden diensten in het systeem. Er is binnen het portal een verschil in machtiging mogelijk.
12.	Het inlogaccount is niet herleidbaar naar Opdrachtgever. Eventueel biedt inschrijver een mogelijkheid tot SSO. Bij het gebruik van SSO hanteert Opdrachtgever aanvullende eisen.

13.	De oplossing kan worden benaderd via elke moderne standaard-browser (marktconform) en kan daarmee zonder plug-ins juist, volledig en optimaal worden gebruikt, onafhankelijk van de onderliggende hardware (waarbij de term "modern" niet blijft hangen op het moment van de initiële ingebruikname maar voortdurend de actualiteit volgt).

TECHNISCHE EISEN WEBSERVER	
NR.	**OMSCHRIJVING**
14.	Opdrachtgever streeft naar een langdurige score van 100% op internet.nl, ook in de verdere toekomst. De immer verdergaande beveiligingseisen zullen doorgaand met de inschrijver besproken worden.
15.	De website is bereikbaar via IPv4 en IPv6.
16.	HTTP compressie dient uitgeschakeld te zijn op de webservers.
17.	Alle websites en portalpagina's dienen ten alle tijden te bereiken zijn via HTTPS poort 443 en geen andere poort.
18.	Indien niet alle informatie via een beveiligde verbinding wordt uitgewisseld, vindt er een permanente redirect plaats van http naar https.
19.	De webserver waarop de webapplicatie draait dient voorzien te zijn van een HSTS-policy. Dit zorgt er voor dat bij een terugkerend bezoek van een klant de browser direct naar HTTPS verbind.
20.	De webapplicatie ondersteunt TLS 1.2 en TLS 1.3. Deze versies van SSL/TLS bieden betere veiligheidsvoorzieningen.
21.	De webserver(s) ondersteunen alleen voldoende veilige cipher suites. Voor meer informatie zie 'TLS-richtlijnen van NCSC', richtlijn B2-1 t/m B2-4. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1.
22.	De webserver(s) ondersteunen voldoende veilige Diffie-Hellman-parameters voor sleuteluitwisseling. Voor meer informatie zie 'TLS-richtlijnen van NCSC', richtlijnen B4-1 t/m 4-2. https://www.ncsc.nl/documenten/publicaties/2021/januari/19/ict-beveiligingsrichtlijnen-voor-transport-layer-security-2.1.
23.	Er mag geen gebruik gemaakt worden van SSLv1, SSLv2, SSLv3, TLS1.0 en TLS1.1.
24.	TLS compressie dient uitgeschakeld te zijn.
25.	De webserver waarop de webapplicatie draait dient voorzien te zijn van een HSTS-policy. Dit zorgt ervoor dat bij een terugkerend bezoek van een klant de browser direct naar HTTPS verbindt.
26.	De portal en webdienst dienen minimaal aan A+ te scoren op de Qualys SSL labs – SSL Server Test website.
27.	Het is niet toegestaan om additionele applicaties te leveren voor bijvoorbeeld beheer in de on-premise omgeving van Opdrachtgever. De inschrijver garandeert dat alle functionaliteiten volledig zijn ondergebrachtin de website / portal / beheerwebsite. Er dient een webapplicatie geleverd te worden waar we onder verstaan dat deze via een webbrowser ontsloten kan worden.
28.	Inschrijver verplicht zich tot het gebruiken van veilige cookies of apps.
29.	De webapplicatie maakt gebruik van invoervalidatie om verdachte tekens, karakters of commando's uit te sluiten.
30.	De inschrijver kan en gaat gebruik maken van een gedelegeerd sub-domein {subdomein}.staatsbosbeheer.nl en voert daar ook het technisch beheer over uit. Opdrachtgever blijft eigenaar van {subdomein}.staatsbosbeheer.nl.
31.	De webserver biedt veilig ingestelde X-Frame-Options aan.

32.	De webserver biedt X-Content-Type-Options aan.
33.	De webserver biedt veilig ingestelde X-XSS-Protection aan.
34.	De webserver biedt Content-Security-Policy (CSP) aan.
35.	De webserver biedt Referrer-Policy aan.

EISEN DNS	
NR.	**OMSCHRIJVING**
36.	Inschrijver gaat er mee akkoord dat het DNS beheer en hosting niet wordt overgedragen aan de inschrijver. Opdrachtgever blijft eigenaar van domeinnaam.
37.	DNS aanvragen en wijzigingen verlopen via Opdrachtgever afd. ICT.
38.	Opdrachtgever gebruikt DNSSec op het domein @staatsbosbeheer.nl en alle andere domeinnamen die gehost gaan worden bij inschrijver. Inschrijver ondersteunt DNSSec en alle aanpalende instellingen en configuraties die daarmee gemoeid zijn. Denk daarbij aan DANE, DMARC en DKIM.
39.	Op domeinnamen van inschrijver die gebruikt worden door Opdrachtgever medewerkers dient ook DNSSec ingesteld en ondersteund te worden. Denk daarbij aan domeinnamen waar functioneel beheerders toegang tot het CMS krijgen.

CERTIFICATEN	
NR.	**OMSCHRIJVING**
40.	Opdrachtgever is eigenaar van certificaten en vraagt alle benodigde certificaten aan. De inschrijver levert tijdig de CSR's aan met als basis de volgende instellingen: Organisatie Unit (OU): BackOffice ICT Organisatie (O): Opdrachtgever Locatie (L): Amersfoort Provincie (S): Utrecht Land (C): NL.
41.	Voor afgeschermde ontwikkel en testomgevingen zijn Let's Encrypt of gelijksoortige certificaten toegestaan die de inschrijver zelf mag aanvragen. Voor Productie systemen die publiekelijk toegankelijk zijn dienen altijd minimaal bedrijf gevalideerde certificaten aangevraagd te worden bij Opdrachtgever.
42.	Certificaten die nodig zijn voor de werking van functionaliteiten op @staatsbosbeheer.nl worden op verzoek door Opdrachtgever aangeschaft en overhandigd. Het is niet toegestaan om zelf certificaten aan te vragen en/of gebruik te maken van Let's Encrypt of gelijksoortige diensten. De aanschafkosten voor deze certificaten worden door Opdrachtgever gedragen.

WEB en API	
NR.	**OMSCHRIJVING**
43.	Bij gebruik van API is het geboden webproduct via REST webservices te benaderen en gebruikt daarbij JSON als in- en uitvoer formaat.
44.	De REST webservice is voldoende gedocumenteerd zodat interfacebouwers in staat zijn om gebruikt te maken van de REST API.
45.	De verbinding van en naar de REST API dient beveiligd en versleuteld te zijn d.m.v. geldige certificaten en TLS verbinding.

MAIL	
NR.	**OMSCHRIJVING**

46.	Om systeemmeldingen uit de webapplicatie te kunnen versturen dient de inschrijver gebruik te maken van een eigen subdomein wat in gedelegeerd beheer is bij inschrijver. ({subdomein}.staatsbosbeheer.nl). U kunt bijvoorbeeld mails versturen vanuit info@{subdomein}.staatsbosbeheer.nl. Denk daarbij aan: aanmelden nieuw account, wachtwoord wijzigen, bevestiging bestelling, etc.
47.	Inschrijver dient TLSA-record op te nemen in DNS ten aanzien van DANE zodat de authenticiteit van een certificaat ook via het DNS TLSA-record gevalideerd kan worden.
48.	Indien er bulk e-mail verstuurd wordt vanuit de webapplicatie dient deze verspreid te worden over uren heen om spamfilters niet op ratelimits te triggeren.
49.	Inschrijver dient echtheidswaarmerken op te nemen tegen e-mailvervalsing. (DMARC, DKIM en SPF). Dit zorgt ervoor dat ontvangers daardoor betrouwbaar phishing- of spammails, die onze domeinnaam ({subdomein}.staatsbosbeheer.nl) in hun afzenderadres misbruiken, kunnen scheiden van echte e-mails.
50.	

BACK-UP AND DISASTER RECOVERY	
NR.	**OMSCHRIJVING**
51.	Het is mogelijk dat het datacenter waar u onze omgeving host problemen ondervindt, zoals algehele regionale stroomuitval, aardbeving, overstroming etc., maar ook uitval van core componenten, zoals core routers of primaire verbindingen naar het internet. Dit noemen wij een calamiteit. Bij calamiteiten geldt de volgende beschikbaarheidseis: RTO: Maximale duur van onbeschikbaarheid omgeving 1 werkdag RPO: Maximaal dataverlies 1 dag.
52.	De inschrijver zorgt dat op verzoek van Opdrachtgever een backup kan worden teruggeplaatst, iedere nacht tot maximaal 7 dagen terug.
53.	De inschrijver garandeert dat Bron-data & back-updata zich nooit op dezelfde fysieke datacenter locatie bevinden.

SECURITY INFRASTRUCTUUR	
NR.	**OMSCHRIJVING**
54.	De inschrijver garandeert dat de firewall bescherming biedt tegen virussen, malware, trojans en exploits op bekend en onbekend internet verkeer.
55.	De inschrijver rapporteert 1 x per 3 maanden een overzicht met daarin de volgende gegevens: Aantal gedetecteerde aanvallen; Type aanvallen; Succesfactor van de aanval; Genomen maatregelen om de aanvallen af te slaan; Aantal onsuccesvolle aanmeldingen.
56.	De Opdrachtnemer is in staat om rapportages te overleggen over uptime, performance, login info, back-up en beveiligingsincidenten. De Opdrachtnemer is in staat om verschillende rapportages te maken indien Opdrachtgever daar om vraagt.
57.	De inschrijver overlegt minimaal 1 keer per jaar een rapport waaruit blijkt dat de inschrijver en haar producten en diensten voldoen aan de laatste beveiliging niveaus voor websites, infrastructuur en certificaten.
58.	Opdrachtgever voert periodiek pentesten uit. De inschrijver is akkoord met deze pentesten en tekent daartoe op verzoek een verklaring van geen bezwaar.