# BIJLAGE ~~9~~ 10 – Programma van Eisen

In deze bijlage worden de eisen beschreven die van toepassing zijn op de uitvoering van de opdracht voor het leveren van hostingdiensten ten behoeve van websites van ICTU. De eisen zijn onderverdeeld in verschillende categorieën, waarbij de eisen zijn doorlopend genummerd per hoofdstuk voor overzichtelijkheid en duidelijkheid.

## Inhoudsopgave

## 0. Definitie

| | |
|---|---|
| Project | Een afzonderlijke website die wordt gehost binnen multiplatform omgeving die wordt opgeleverd. Elke website geldt als een zelfstandig project en beschikt over een eigen, gescheiden omgeving met aparte useraccounts, configuraties, rapportages en toegangsrechten. |

## 1. Algemeen

| Nummer | Algemeen |
|---|---|
| **1.1** | Opdrachtnemer mag zonder uitdrukkelijke voorafgaande schriftelijke toestemming van ICTU geen gebruik maken van de naam en/of het logo van ICTU. |
| **1.2** | De inzet van onderaannemers is alleen toegestaan na schriftelijke toestemming van ICTU. Opdrachtnemer blijft eindverantwoordelijk. |
| **1.3** | Opdrachtnemer verleent volledige medewerking bij overdracht aan een opvolgende leverancier. Er mogen geen aanvullende kosten worden gerekend voor ondersteuning bij een exit. |
| **1.4** | Bij een exit draagt Opdrachtnemer zorg voor een volledige en correcte overdracht van alle relevante gegevens aan ICTU of een door ICTU aangewezen partij. |
| **1.5** | **Migratie-eisen bij Exit**<br>Opdrachtnemer stelt samen met ICTU een exitplan op dat onderdeel vormt van de overeenkomst. Dit plan bevat termijnen, verantwoordelijkheden en een migratieprocedure om continuïteit te waarborgen.<br><br>Alle relevante gegevens, configuraties, documentatie en logbestanden worden volledig en in digitaal leesbaar formaat overgedragen wat algemeen gangbaar is in hun respectievelijke soort.<br><br>• De overdracht wordt zo uitgevoerd dat de continuïteit van de dienstverlening niet in gevaar komt.<br>• De opdrachtnemer verleent redelijke ondersteuning aan de nieuwe partij tijdens de overdrachtsperiode.<br>• Er wordt een overdrachtsdossier opgeleverd met een overzicht van systemen, accounts, wachtwoorden, procedures en afhankelijkheden.<br>• De opdrachtgever of diens vertegenwoordiger krijgt gelegenheid om de volledigheid en juistheid van de overdracht te verifiëren.<br>• De overdracht vindt plaats binnen vooraf afgesproken termijnen, op basis van een gezamenlijk overeengekomen migratieplan. |
| **1.6** | De diensten worden geleverd vanuit datacenters binnen de Europese Economische Ruimte (EER), inclusief een uitwijklocatie, en voldoet tevens aan de Nederlandse wet- en regelgeving. |

## 2. Communicatie

| Nummer | Communicatie |
|---|---|
| **2.1** | Opdrachtnemer wijst een vast aanspreekpunt en plaatsvervanger aan voor de uitvoering van de overeenkomst. |
| **2.2** | Minimaal één keer per kwartaal vindt overleg plaats tussen ICTU en Opdrachtnemer volgens een vaste agenda. |
| **2.3** | In alle communicatie wordt het VP-nummer van ICTU vermeld. |
| **2.4** | Alle communicatie met ICTU vindt plaats in het Nederlands, tenzij anders overeengekomen. |
| **2.5** | Opdrachtnemer communiceert proactief over wijzigingen in protocollen, standaarden of beveiligingsmaatregelen of -richtlijnen die impact hebben op de dienstverlening van ICTU. |
| | |

## 3. Informatiebeveiliging

| Nummer | Informatiebeveiliging |
|---|---|
| **3.1** | De hostingomgeving voldoet aan de Baseline Informatiebeveiliging Overheid (BIO) en is ISO 27001:2022-gecertificeerd. Leverancier toont jaarlijks aan dat certificering actueel is en dat interne audits zijn uitgevoerd. |
| **3.2** | De infrastructuur is “secure by design” ingericht, met minimale services, Sterke wachtwoorden: Alle accounts en services moeten gebruikmaken van sterke, unieke wachtwoorden conform geldende richtlijnen (bijv. NIST of OWASP). en gescheiden omgevingen per Project. Dit geldt ook voor mail- en databaseservers. Multi-Factor Authenticatie (MFA) is verplicht voor alle beheerdersinterfaces en toegang tot productieomgevingen. |
| **3.3** | De hostingomgeving moet voorzien zijn van *at rest*-versleuteling voor alle databases die (persoons)gegevens bevatten. Dit betekent dat data die is opgeslagen op schijf, inclusief back-ups en tijdelijke bestanden, versleuteld wordt met een sterk algoritme (bij voorkeur AES-256 of gelijkwaardig). De gebruikte sleutels moeten veilig worden beheerd en niet op hetzelfde systeem worden opgeslagen als de versleutelde data. Versleuteling mag geen negatieve invloed hebben op de beschikbaarheid, performance of integriteit van de data. |
| **3.4** | Leverancier implementeert een OpenVPN oplossing waarmee meerdere website beheerders simultaan gebruik van kunnen maken. De OpenVPN oplossing moet een SAML of OIDC-integratie ondersteunen voor toegang. |
| **3.5** | Leverancier zorgt ervoor dat de SSH, FTPS en HTTPS van de ‘management’ interfaces c.q. pagina’s enkel te benaderen zijn via de OpenVPN en niet publiekelijk benaderbaar zijn zonder tussenkomst van de OpenVPN oplossing uit artikel 3.4. Daarbij zijn firewall- en DDoS-bescherming verplicht geconfigureerd. |
| **3.6** | voor elk Project moeten useraccounts strikt gescheiden worden en beheerd worden volgens het principe van minimale toegang. Daarnaast moet het mogelijk zijn per project een volledige TAP-straat (Test, Acceptatie en Productie) in te richten. Elke projectomgeving beschikt over eigen useraccounts, rapportages en logging, zodat beheer, toegang en controle onafhankelijk en veilig zijn ingericht. |

| Nummer | Informatiebeveiliging |
|---|---|
| **3.7** | Opdrachtnemer garandeert dat er geen technische belemmeringen zijn om voor door ICTU geplaatste websites een 100% score te behalen op http://internet.nl. |
| **3.8** | Alle communicatie van en naar de hostingomgeving verloop via versleutelde berichten conform 'pas-toe-of-leg-uit' principe van Forum van Standaardisatie (link). Ook implementeert en onderhoudt de leverancier de standaarden en protocollen uit de 'open standaarden'-lijst van Forum van Standaardisatie, waar van toepassing. |
| **3.9** | ICTU voert zelf jaarlijks een pentest uit op de omgeving. De resultaten en het plan van aanpak met verbetermaatregelen wordt binnen 1 maand na afloop van de test gedeeld met de opdrachtnemer ter actie. Prioritering wordt op urgentie in overleg bepaald. |
| **3.10** | Alle persoonsgegevens worden uitsluitend verwerkt binnen de Europese Economische Ruimte (EER). |

## 4. Support en Onderhoud

| Nummer | Support en Onderhoud |
|---|---|
| **4.1** | Opdrachtnemer levert ondersteuning in het Nederlands, zowel mondeling als schriftelijk. Alle supportactiviteiten en communicatie worden uitgevoerd door personen inclusief het opstellen van documentatie; gebruik van AI-gegenereerde antwoorden of geautomatiseerde chatbots voor inhoudelijke ondersteuning is niet toegestaan. |
| **4.2** | Opdrachtnemer is verantwoordelijk voor het volledig beheer en onderhoud van de infrastructuurlaag van de hostingomgeving, inclusief servers, opslag, netwerkcomponenten, virtualisatielaag, besturingssystemen, beveiligingsconfiguraties en monitoring. Dit omvat het uitvoeren van updates, patches, capaciteitsbeheer, performancebewaking en het oplossen van storingen. Monitoring, updates en patchmanagement maken integraal deel uit van de dienstverlening. |
| **4.3** | Opdrachtnemer levert op verzoek een onderhoudswindow en bijbehorende rapportage. |
| **4.4** | Leverancier voert maandelijks patchrondes uit en rapporteert over de status van updates en kwetsbaarheden. |
| **4.5** | Back-ups worden dagelijks gemaakt en minimaal 14 dagen bewaard. |
| **4.6** | Incidenten met prioriteit 1 (productieomgeving: bedrijfsvoering ICTU geblokkeerd) worden binnen 4 uur opgelost of voorzien van een oplossingsplanning. |
| **4.7** | Opdrachtnemer levert per kwartaal een rapportage met de volgende informatie:<br>1. Beschikbaarheid & performance<br>• Uptime<br>• Gemiddelde responstijden<br>• Eventuele downtime, met oorzaken en herstelmaatregelen<br>2. Beveiliging<br>• Overzicht van beveiligingsupdates (CMS, plug-ins, frameworks)<br>• Bevindingen uit security scans of penetratietests<br>• Meldingen van incidenten of datalekken, inclusief opvolging<br>3. Back-ups & herstel<br>• Frequentie van back-ups<br>• Resultaten van test-herstelacties<br>• Eventuele afwijkingen of fouten<br>4. Verkeer & gebruik<br>• Bezoekstatistieken (aantal sessies, piekmomenten)<br>• Bandbreedte- of opslaggebruik<br>• Eventuele overbelasting of afwijkend gedrag.<br>5. Wijzigingen & onderhoud<br>• Uitgevoerde updates, releases of bugfixes<br>• Geplande en uitgevoerde onderhoudsvensters<br>• Impact op de beschikbaarheid<br>6. Verbeterpunten/aanbevelingen<br>• Adviezen voor optimalisatie, beveiliging of stabiliteit<br><br>De rapportages worden gebruikt voor toetsing van de SLA-waarden zoals vastgelegd in artikel 4.8 |
| **4.8** | De volgende SLA-waarden gelden per omgeving en maken integraal onderdeel uit van dit Programma van Eisen: |

| Nummer | Support en Onderhoud |
|---|---|
| | • Productie: minimale beschikbaarheid 99,9% per maand; prioriteit 1-incidenten (productie: bedrijfsvoering ICTU geblokkeerd) ≤ 4 uur; 24/7 monitoring en incidentafhandeling.<br>• Acceptatie: minimale beschikbaarheid 99% per maand; incidenten ≤ 8 uur; ondersteuning binnen kantooruren (ma–vr 08:00–18:00 CET), out-of-hours op best-effort.<br>• Test: minimale beschikbaarheid 95% per maand; incidenten ≤ 24 uur; ondersteuning binnen kantooruren (ma–vr 08:00–18:00 CET).<br><br>Uptime-rapportages, performance-metingen en doorlooptijden voor wijzigingen en service requests worden per kwartaal gerapporteerd conform artikel 4.7 en 4.9. |
| **4.9** | Opdrachtnemer levert per kwartaal een rapportage met de volgende informatie:<br>a. Incidenten & support<br>• Aantal meldingen bij support<br>• Oplostijden (SLA's)<br>• Eventuele structurele problemen of trends |
| **4.10** | Opdrachtnemer moet inzicht hebben in serverload, uptime, IP-blokkades en piekbelastingen, inclusief signalering van mogelijke dreigingen. |

**5. Facturatie en Prijsstructuur**

| Nummer | Facturatie en Prijsstructuur |
|---|---|
| **5.1** | Facturatie vindt plaats per maand. |
| **5.2** | Offertes bevatten een uitsplitsing van kosten inclusief eventuele mutaties. |
| **5.3** | ICTU kan de marktconformiteit van tarieven voor zover deze niet in de aanbieding is besloten toetsen aan de hand van onderliggende inkoopprijzen of listprijzen. |

## 6. Levering en Technische Specificaties

| Nummer | Levering en Techniek |
|---|---|
| 6.1 | De hostingomgeving ondersteunt diverse CMS'en, waaronder WordPress, Drupal, Joomla, Typo3, Concrete5, MODX, Craft CMS, OctoberCMS, SilverStripe, ProcessWire en Grav. Daarnaast zijn frameworks als Laravel, Symfony, CodeIgniter en Node.js-omgevingen (zoals React, Vue en Next.js) goed compatibel. Plesk biedt automatische installatie, updates, SSL via Let's Encrypt, back-ups en beveiligingsbeheer via de Security Advisor. |
| 6.2 | De hostingomgeving moet zijn ingericht volgens een **TAP-straat** (Test-, Acceptatie- en Productieomgeving). Elke fase heeft een eigen, gescheiden omgeving met bijbehorende configuraties en toegangsrechten. De SLA-waarden voor beschikbaarheid en responstijden die gelden voor deze omgevingen zijn vastgelegd in artikel 4.8. |
| 6.3 | De hostingomgeving moet voldoen aan gangbare performance-eisen:<br>a. Productie: een gemiddelde serverreactietijd (TTFB) van maximaal 500 ms, een totale paginalaadtijd van maximaal 3 seconden bij normale belasting en maximaal 5 seconden onder piekbelasting (95e percentiel). API-verzoeken moeten in 99% van de gevallen binnen 300–600 ms worden afgehandeld.<br>b. Acceptatie- en testomgevingen: performance moet representatief zijn voor productie, maar afwijkingen zijn toegestaan voor validatie en ontwikkelactiviteiten. |
| 6.4 | De hostingomgeving (zie 6.2) moet beschikken over elk minimaal 1 TB aan beschikbare opslagcapaciteit, geschikt voor het opslaan van data, logbestanden en back-ups, met gebruik van snelle en betrouwbare opslag (bij voorkeur SSD of NVMe). |
| 6.5 | De hostingomgeving moet beschikken over een fallbackomgeving die automatisch een statische noodpagina toont zodra de primaire TAP-omgevingen niet beschikbaar zijn. Deze pagina moet minimaal basisinformatie en contactgegevens tonen en onafhankelijk functioneren van de hoofdomgeving, zodat bezoekers altijd een bereikbare melding ontvangen. |
| 6.6 | De hostingomgeving moet zijn voorzien van een actieve anti-DDoS-oplossing die kwaadaardig verkeer detecteert en afweert, zodat de beschikbaarheid van de website en onderliggende diensten behouden blijft tijdens aanvallen. |
| 6.7 | De hostingomgeving moet beschikken over een geavanceerde beveiligingsoplossing voor Linux-webservers, met functies zoals firewall, WAF, IDS/IPS, malwaredetectie, automatische patching en bescherming tegen brute-force-aanvallen. Oplossingen zoals Imunify360 in combinatie met ImunifyAV+ bieden hierbij een geïntegreerde aanpak met continue monitoring, automatische malwareverwijdering en ondersteuning voor beheerpanelen als Plesk, en gelden als referentie voor het gewenste beveiligingsniveau. |
| 6.8 | De hostingomgeving moet beschikken over een managed back-upomgeving die centraal wordt beheerd en bewaakt. Back-ups worden automatisch en periodiek uitgevoerd, versleuteld opgeslagen en getest op herstelbaarheid. Zowel volledige als incrementele back-ups moeten mogelijk zijn, met retentieperioden die aansluiten op de continuïteitseisen van de opdrachtgever. De leverancier is verantwoordelijk voor beheer, monitoring en tijdig herstel bij incidenten. |

| Nummer | Levering en Techniek |
|---|---|
| | Opdrachtnemer levert standaard een retentieperiode van minimaal 90 dagen voor alle back-ups. Deze retentie is inbegrepen in de vaste maandprijs.<br><br>Retentie per omgeving<br>• Productie: minimaal 60 dagen retentie.<br>• Acceptatie: minimaal 14 dagen retentie.<br>• Test: minimaal 7 dagen retentie, best effort herstel, geen formele DRT.<br><br>Opdrachtnemer hanteert minimaal het volgende retentieschema:<br>• Huidige dag: één back-upkopie, beschikbaar tot 24 uur terug.<br>• Huidige week: één back-upkopie per dag, 7 dagen terug beschikbaar.<br>• Afgelopen maand: één back-upkopie per week (bij voorkeur op vrijdag), 4 weken terug beschikbaar.<br>• Bewaarperiode: alle back-ups worden versleuteld opgeslagen en getest op herstelbaarheid.<br><br>Disaster Recovery Test (DRT):<br>• Productieomgeving: minimaal eenmaal per jaar voert opdrachtnemer een disaster recovery test (DRT) uit. Binnen 10 werkdagen na afloop levert opdrachtnemer een rapportage met behaalde RPO/RTO, uitgevoerde stappen, bevindingen, verbetermaatregelen en een oordeel (slaag/niet geslaagd).<br>• Acceptatieomgeving: opdrachtnemer toont aantoonbaar aan dat herstelbaarheid is geborgd (bijvoorbeeld via testrapportage of simulatie).<br>• Testomgeving: opdrachtnemer hanteert een best-effort herstelprocedure; formele DRT-rapportage is hier niet vereist. |
| 6.9 | Binnen de hostingomgeving is het mogelijk om applicaties te installeren ten behoeve van ontwikkeling en testen. |
| 6.10 | Elke Projectomgeving beschikt over een eigen Plesk-configuratie. |
| 6.11 | Capaciteit en data per omgeving:<br>a. De productieomgeving (High Available) ondersteunt minimaal 50.000 unieke bezoekers per dag per project en beschikt over minimaal 10 TB inbound en outbound dataverkeer per maand.<br>b. De acceptatieomgeving beschikt over minimaal 5 TB inbound en outbound dataverkeer per maand.<br>c. De testomgeving beschikt over voldoende capaciteit voor functionele validatie, met minimaal 1 TB inbound en outbound dataverkeer per maand.<br>d. Elke omgeving beschikt over CPU en geheugen (MEM) die in lijn zijn met deze eisen en schaalbaar zijn op basis van belasting. |
| 6.12 | De server kan geconfigureerd worden voor het hosten van mediabestanden voor bijvoorbeeld podcasts (byte-range requests) |
| 6.13 | Opdrachtnemer levert op verzoek productroadmaps van de gebruikte hostingtechnologieën. |
| 6.14 | Een dedicated loadbalancer wordt ingezet voor de ICTU productie hosting omgeving. |

| Nummer | Levering en Techniek |
|---|---|
| 6.15 | Opdrachtnemer dient de productieomgeving zodanig high available te ontwerpen en beheren dat de continuïteit van de dienstverlening gewaarborgd blijft bij uitval van individuele servers of componenten. Beschikbaarheid van de productieomgeving mag niet worden beïnvloed door enkelvoudige storingen in lijn met eis 4.8 |
| 6.16 | De OpenVPN oplossing moet ondersteuning bieden voor SAML of OIDC integratie. |
| 6.17 | Leverancier biedt tooling voor monitoring van uptime, performance en beveiliging per website. |
| 6.18 | Leverancier biedt ondersteuning voor accessibility (WCAG 2.1) en performance optimalisatie (Core Web Vitals). |
| 6.19 | De TAP-straat moet zijn voorzien van adequate DDoS-bescherming, zodat de beschikbaarheid van de dienstverlening gewaarborgd blijft bij (gedistribueerde) denial-of-service-aanvallen. |