

## Programma van Eisen

In het Programma van Eisen en Wensen is gekozen voor een tweedeling: de (harde) eisen en de wensen. Een eis heeft een uitsluitend karakter. Het niet voldoen aan een eis is voor Opdrachtgever aanleiding de offerte uit te sluiten van verdere beoordeling.

Opdrachtnemer hoeft geen toelichting te geven bij het Programma van Eisen en kan volstaan met het indienen van inschrijving, waarmee Opdrachtnemer verklaart onvoorwaardelijk in te stemmen met en te voldoen aan alle gestelde eisen.

### Programma van eisen:

1. Algemeen	
Nr.	Eisen
1.1	Opdrachtnemer verzorgt het beheer van de Drupal-platformen, specifiek Drupal 11, inclusief updates en modulebeheer met vroegtijdige signalering.
1.2	Alle maatwerkprogrammatuur, inclusief auteursrechten en intellectueel eigendom, blijft te allen tijde eigendom van Opdrachtgever.
1.3	Opdrachtnemer is verantwoordelijk voor de goede werking van de website en hanteert professioneel change management met uitvoerige testprocedures.
1.4	Werkzaamheden worden uitsluitend uitgevoerd na schriftelijke goedkeuring van Opdrachtgever.
1.5	De website en functionaliteiten dienen volledig responsive te zijn en goed te functioneren op mobiele apparaten.
1.6	Alle doorgevoerde wijzigingen en aanpassingen worden volledig gedocumenteerd.
1.7	Inschrijver mag gebruikmaken van internationale medewerkers, mits de contactpersonen vloeiend Nederlands spreken en communiceren met het team van Opdrachtgever.
1.8	Het is Opdrachtnemer en eventuele onderaannemers niet toegestaan om vertrouwelijke gegevens, materialen of concepten van Opdrachtgever te verwerken via open AI-omgevingen of platforms waarbij data extern wordt opgeslagen of getraind, zoals openbare generatieve AI-tools (bijv. OpenAI, Google Gemini, etc.), tenzij expliciet schriftelijk toestemming is verkregen van Opdrachtgever. Opdrachtnemer dient passende technische en organisatorische maatregelen te treffen om de vertrouwelijkheid van de gegevens van de opdrachtgever te waarborgen.
1.9	Authenticiteit en menselijkheid staan voor Opdrachtgever centraal. Opdrachtgever verlangt dat alle creatieve uitingen zoals fotografie, videografie, stemmen, teksten, etc. echte verhalen en echte mensen bevatten (studenten, medewerkers, alumni of stakeholders). Het gebruik van gegenereerde content (zoals AI-gegenereerde beelden, deepfakes, stemmen of complete teksten) is niet toegestaan, tenzij expliciete schriftelijke toestemming is verleend door Opdrachtgever. De inzet van AI-technologieën door Opdrachtnemer is uitsluitend toegestaan als hulpmiddel ter bevordering van efficiëntie (zoals voor tekstcorrectie, inspiratie, beeldbewerking (in overleg) of planning).

2. Architectuur	
Nr.	Eisen
2.1.	De website draait op een architectuur waarin maatwerk zoveel mogelijk wordt beperkt en indien noodzakelijk herbruikbaar is binnen verschillende domeinen.
2.2	Standaard koppelvlakken worden gebruikt; Betreffende een koppeling met Microsoft Dynamics (aanmeldingen evenementen en Cursussen, inladen informatie over Cursussen en startmomenten) en koppelingen met Surfconext (inloggen Drupal en Interne cursussen).
2.3	De website moet voldoen aan geldende beveiligingsnormen en best practices voor informatiebeveiliging.
2.4	Alle functionaliteiten dienen te voldoen aan de AVG/GDPR en relevante Europese wet- en regelgeving.
2.5	Alle functionaliteiten dienen te voldoen aan de WCAG wetgeving die voor ons als hogeschool van toepassing is. Minimaal niveau AA.

<b>3. Techniek</b>	
<b>Nr.</b>	<b>Eisen</b>
3.1	Er wordt gewerkt met open standaarden volgens de richtlijnen van het Forum Standaardisatie.
3.2	Opdrachtnemer moet aantoonbare kennis en ervaring hebben met Google Tag Manager (GTM) en Google Analytics 4 (GA4).
3.3	Code dient te voldoen aan best practices voor softwareontwikkeling en modulair en gedocumenteerd te zijn.
3.5	Beveiligingsbeleid omvat proactieve monitoring op kwetsbaarheden, advisering over dreigingen en risico's, en up-to-date kennis.
3.6	Alle communicatie moet versleuteld plaatsvinden met TLS (HTTPS) om de vertrouwelijkheid en integriteit van de gegevens te waarborgen.
3.7	Gebruikersidentiteit wordt gecontroleerd via een koppeling met Surfconext, met een fallback-mogelijkheid voor Multi-Factor Authenticatie (MFA) in geval van uitval van Surfconext.
3.8	Er wordt een gedetailleerd rollen- en toegangscontrolesysteem toegepast, waarbij gebruikers alleen de minimale benodigde rechten hebben voor hun werk.
3.9	Sessies duren maximaal 1 etmaal en worden veilig beheerd, waarbij sessie-ID's correct worden beveiligd en sessies tijdig verlopen.
3.10	Alle invoer van gegevens wordt gevalideerd en voldoet aan het verwachte formaat en type. De uitvoer van gegevens wordt beperkt tot de noodzakelijke gegevens.
3.11	Toegang tot systeemconfiguratiebestanden wordt beperkt en foutmeldingen worden verborgen voor eindgebruikers.
3.12	Het systeem genereert uitgebreide logbestanden van belangrijke activiteiten zoals inloggen, wijzigingen in gegevens en systeemconfiguraties. Logs worden veilig opgeslagen en regelmatig gecontroleerd.
3.13	Er wordt een continu patchmanagementproces toegepast voor het snel toepassen van beveiligingsupdates en het dichten van kwetsbaarheden. Automatische updates worden toegepast waar mogelijk.
3.14	Er wordt een WAF of cloudgebaseerde DDoS-bescherming geïmplementeerd, met rate-limiting om overbelasting te voorkomen.
3.15	API's worden beveiligd met OAuth/API keys, met toegangsbewaking en rate-limiting om kwaadaardig verkeer te voorkomen.
3.16	Alle bestandstypes worden gecontroleerd, geüploade bestanden worden gescand op virussen, en bestandsgrootte wordt beperkt.
3.17	Periodieke penetratietests en beveiligingsbeoordelingen worden uitgevoerd om kwetsbaarheden tijdig te identificeren en op te lossen.
3.18	Er is een limiet op mislukte inloggopingen, waarna accounts tijdelijk worden vergrendeld en herstel via e-mail of MFA mogelijk is.
3.19	Beveiliging tegen Cross-Site Scripting (XSS) en Cross-Site Request Forgery (CSRF)
3.20	Gebruikersinvoer wordt gevalideerd, en formulieren worden beveiligd met CSRF-tokens en Content Security Policy (CSP).
3.21	E-mailcommunicatie wordt via versleutelde kanalen (TLS) verzonden, met regelmatige controles van de e-mailserverconfiguratie.

<b>4. Beheer &amp; Gebruik van AI in het ontwikkel- en beheerproces</b>	
<b>Nr.</b>	<b>Eisen</b>
4.1	Opdrachtnemer voert regulier beheer en onderhoud uit op Drupal 11 en gerelateerde modules.
4.2	Wijzigingen en aanpassingen worden uitgevoerd volgens een OTAP-omgeving.
4.3	Opdrachtnemer beschikt over een serviceportaal voor meldingen en verzoeken (zoals JIRA of Topdesk).
4.4	Opdrachtnemer voert regulier beheer en onderhoud uit op Drupal 11 en gerelateerde modules.
4.5	De opdrachtnemer dient het gebruik van AI-tools in het ontwikkel-, beheer- en contentproductieproces vooraf te melden en te laten goedkeuren door de opdrachtgever.
4.6	De opdrachtnemer dient op verzoek inzicht te geven in welke AI-tools worden ingezet, met welk doel, en hoe gegenereerde output wordt gecontroleerd op kwaliteit, betrouwbaarheid en auteursrechten.
4.7	Het gebruik van AI-tools die data buiten de EU verwerken of opslaan is niet toegestaan, tenzij uitdrukkelijk schriftelijk goedgekeurd door de opdrachtgever.
4.8	Er mag geen vertrouwelijke of persoonsgebonden data via publieke AI-modellen of externe AI-platforms (zoals ChatGPT, Gemini, Copilot) worden verwerkt zonder expliciete toestemming van de opdrachtgever.
4.9	Het gebruik van generatieve AI (zoals tekst-, beeld- of codegeneratie) mag uitsluitend ondersteunend zijn aan werkzaamheden en nooit zonder menselijke controle tot publicatie leiden.
4.10	Code gegenereerd met behulp van AI dient altijd door een developer gecontroleerd te worden voordat dit in productie wordt genomen.
4.11	AI-gegenereerde content (zoals code, teksten of beelden) dient vrij te zijn van auteursrechtelijke beperkingen. De opdrachtnemer blijft verantwoordelijk voor eventuele claims vanuit auteursrechten of licenties die voortvloeien uit het gebruik van AI-tools.

<b>5. Performance Website</b>	
<b>Nr.</b>	<b>Eisen</b>
5.1	De gemiddelde laadtijd van een pagina blijft onder 1,5 seconden, ook na updates en wijzigingen.
5.2	De website functioneert optimaal in gangbare browsers, inclusief de nieuwste versies van Chrome, Firefox, Edge en Safari.

<b>6. Service Level Agreement (SLA)</b>										
<b>Nr.</b>	<b>Eisen</b>									
6.1	Minimale uptime voor de website van 99,8% per maand, 24/7 (exclusief gepland onderhoud).									
6.2	Onderhoud dient minimaal 48 uur van tevoren te worden aangekondigd door de opdrachtnemer.									
6.3	Incidenten dienen in gezamenlijkheid geprioriteerd te worden (bijvoorbeeld: Kritiek / Hoog / Midden / Laag).									
6.4	Bij een kritieke storing geldt:									
	<table border="1"> <thead> <tr> <th></th> <th>Kritiek</th> <th>Niet-kritiek</th> </tr> </thead> <tbody> <tr> <td>Reactietijd</td> <td>2 uur</td> <td>24 uur</td> </tr> <tr> <td>Oplostijd</td> <td>4 uur</td> <td>3 werkdagen</td> </tr> </tbody> </table>		Kritiek	Niet-kritiek	Reactietijd	2 uur	24 uur	Oplostijd	4 uur	3 werkdagen
	Kritiek	Niet-kritiek								
Reactietijd	2 uur	24 uur								
Oplostijd	4 uur	3 werkdagen								
6.5	Telefonische en/of e-mailbereikbaarheid bij storingen: Ma - Vr: 8:00 - 18:00 uur									
6.6	Updates vanuit Drupal, plugins, koppelingen en beveiligingspatches worden door de opdrachtnemer uitgevoerd en vooraf gecommuniceerd.									
6.7	De opdrachtnemer voert proactieve monitoring van foutmeldingen en performanceproblemen uit en communiceert wanneer nodig.									
6.8	De opdrachtnemer zorgt voor versiebeheer inclusief rollbackmogelijkheid bij updates.									
6.9	Downtime bij deployment is altijd in overleg met opdrachtgever.									

<b>7. Communicatie en Samenwerking</b>	
<b>Nr.</b>	<b>Eisen</b>
7.1	Proactieve samenwerking en strategisch meedenken over verbeteringen wordt verwacht vanuit opdrachtnemer.
7.2	Ten behoeve van de overdraagbaarheid moeten de ontwikkelde functionaliteiten goed worden gedocumenteerd door de opdrachtnemer.
7.3	Opdrachtnemer wijst een vast contactpersoon aan als accountverantwoordelijke. Deze contactpersoon is het eerste aanspreekpunt en is verantwoordelijk voor de goede uitvoering van de raamovereenkomst en is beslissingsbevoegd. De Opdrachtnemer dient gedurende werkdagen tussen 8.30 uur en 17.00 uur zowel telefonisch als via e-mail bereikbaar te zijn. Naast de vaste contactpersoon wordt er een vaste vervanger aangewezen.
7.4	Naast een vaste contactpersoon moet directe toegang tot technische developers ook mogelijk zijn.
7.5	NHL Stenden wil jaarlijks afstemming hebben met de opdrachtnemer op strategisch niveau (over de raamovereenkomst). Daarnaast zal er per periode van 4 maanden op tactisch niveau overleg plaatsvinden. De agenda voor deze overleggen wordt in gezamenlijkheid vastgelegd. Operationeel overleg vindt plaats op het moment dat daar behoefte toe bestaat.

<b>8. Financiële eisen</b>	
<b>Nr.</b>	<b>Eisen</b>
8.1	De in de inschrijving op te nemen tarieven/prijzen zijn in Euro, exclusief btw. Opgave van prijzen en berekeningen van toegekende cijfers zal tot maximaal vier cijfers achter de komma plaatsvinden.
8.2.	Alle door Opdrachtnemer gecommuniceerde prijzen omvatten alle mogelijke kosten, belastingen en heffingen (dus in ieder geval inclusief voorrijkosten, arbeidskosten, onderhoudskosten, materiaalkosten, afhandelingskosten, uitvoering, nazorg, inleerkosten, overhead, reis- en andere kosten). Tijdens de gehele contractperiode brengt Opdrachtnemer geen extra kosten in rekening.
8.3	De factuur dient te voldoen aan de eisen zoals opgenomen in de bijlage 4.
8.4	Facturen mogen uitsluitend worden ingediend door de contractpartner/opdrachtnemer zelf. Dit moet dezelfde crediteur zijn aan wie de opdracht is verstrekt. Facturen van een andere crediteur, zoals een onderaannemer of een andere vestiging met een afwijkend crediteurnummer, kunnen wij niet in behandeling nemen.