Generieke eisen en richtlijnen bij marktconsultatie of aanbesteding

Informatiebeveiliging, privacy, architectuur, informatievoorziening en servicemanagement

Versie: november 2025

Voorwoord

NHL Stenden Hogeschool is een middelgrote hogeschool in het Noorden van het land. Naast een sterke regionale functie is de hogeschool ook nationaal en vooral internationaal georiënteerd. De hogeschool heeft als doel studenten op te leiden tot de Nederlandse wettelijke associate degree, bachelor- en mastergraden door middel van voltijd, duaal en deeltijd, bekostigd en niet-bekostigd onderwijs. NHL Stenden heeft ongeveer 24.000 studenten en 2.200 medewerkers. De opleidingen zijn georganiseerd in academies. Binnen de academies zorgen de lectoraten, onderzoeksgroepen en Centres of Expertise (CoE) met (gesubsidieerde) onderzoeksprojecten voor de verbinding tussen onderwijs, onderzoek, het bedrijfsleven en maatschappelijke organisaties. Voor meer informatie, zie http://www.nhlstenden.com

Betrouwbare informatievoorziening wordt geleverd door informatieverwerkende systemen van verschillende Inschrijvers. Deze systemen zijn niet alleen binnen NHL Stenden digitaal met elkaar verbonden, maar mogelijk ook met daarbuiten gelegen systemen en sectorbrede voorzieningen (StudieLink, NPuls, Surf). Aanvullend krijgt de onderwijssector te maken met strengere securityeisen, zoals het Surf Toetsingskader en NIS2. NHL Stenden streeft naar een wendbaar, efficiënt en schaalbaar digitaal landschap dat adequaat meebeweegt met externe ontwikkelingen. We richten ons op het vertalen van de organisatiedoelen, zoals geformuleerd in het Strategisch Instellingsplan, naar passende IT-oplossingen en innovaties. En afsluitend, vanwege de krapte in de arbeidsmarkt en de steeds snellere ontwikkelingen in de digitale mogelijkheden (en bedreigingen) maakt NHL Stenden een transitie door van traditionele beheerorganisatie naar een regie-voerende organisatie.

Al met al is het noodzakelijk om duidelijke richtlijnen en voorwaarden te beschrijven, indien producten van externe Inschrijvers deel gaan uitmaken van de IV-keten van NHL Stenden.

Van onze IT-partners verwachten we dan ook dat zij proactief met ons meedenken vanuit hun kennis en ervaring. We zoeken Inschrijvers die ons gevraagd en ongevraagd adviseren over zaken als informatiemanagement, Enterprise architectuur, integratievraagstukken, informatiebeveiliging en de adoptie van nieuwe technologie, steeds in lijn met onze organisatiedoelstellingen.

Met dit document geven we u inzicht in onze voorwaarden, architectuurprincipes en standaarden op het gebied van privacy, informatiebeveiliging, informatievoorziening en IT-servicemanagement.

Wij kijken uit naar een constructieve en inspirerende samenwerking!

Met vriendelijke groet,

CIO-Office
NHL Stenden Hogeschool

1. PRIVACY	
Verwerking van persoonsgegevens is noodzakelijk voor de bedrijfsprocessen van instellingen van onderwijs en onderzoek zoals NHL Stenden. Dit dient met de grootste zorgvuldigheid te gebeuren omdat misbruik van persoonsgegevens grote schade kan berokkenen aan studenten, medewerkers en andere betrokkenen bij NHL Stenden, maar ook bij NHL Stenden als organisatie. We hechten dan ook veel waarde aan het beschermen van de persoonsgegevens die aan ons worden verstrekt en aan de wijze waarop persoonsgegevens worden verwerkt.	
1.1	**AVG:** Inschrijver voldoet aan de Algemene Verordening Gegevensbescherming.
1.2	**Privacybeleid:** Inschrijver heeft een privacybeleid opgesteld en voert deze uit conform de vereisten van de AVG. Het privacybeleid beschrijft hoe de organisatie uitvoering geeft aan de privacy beginselen die in artikel 5 lid 1 AVG zijn vastgelegd en bevat tenminste de volgende aspecten: • Rollen en verantwoordelijkheden met betrekking tot de verwerking van persoonsgegevens; • Organisatorische maatregelen; • Training en bewustwording; • Datalekken; • Interne controle op naleving van het beleid.
1.3	**Overeenkomst met betrekking tot de verwerking van persoonsgegevens:** Indien Inschrijver de rol van verwerker vervult in de zin van de AVG, ondertekent Inschrijver de door NHL Stenden voorgeschreven verwerkersovereenkomst conform het SURF-template 'verwerkersovereenkomst'. Bij toegang tot of verwerking van persoonsgegevens zonder dat Inschrijver de rol van verwerker vervult in de zin van de AVG, wordt een geheimhoudingsbepaling overeengekomen. Is er sprake van gezamenlijke verwerkingsverantwoordelijkheid van Inschrijver en NHL Stenden, dan wordt een overeenkomst gesloten conform het SURF-template 'Gezamenlijke Verwerkingsverantwoordelijken Overeenkomst'.
1.4	**DPIA-ondersteuning:** Waar daar door NHL Stenden om wordt gevraagd, wordt medewerking verleend aan Data Protection Impact Assessments.
1.5	**Europese Economische Ruimte (EER):** Inschrijver verwerkt persoonsgegevens enkel binnen de Europese Economische Ruimte en is geen dochteronderneming van een buiten de EER gevestigde moederonderneming.
1.6	**Privacy by Design & by Default**: Systemen moeten – in lijn met de AVG – privacybeschermende instellingen als standaard hebben (privacy by design en privacy by default).
1.7	**Exit-strategie en Vendor Lock-in:** Inschrijver draagt er zorg voor dat, bij ontbinding van het contract, bij een van rechtswege eindigen van de overeenkomst of bij het wijzigen van enige vorm van opslag, NHL Stenden-gegevens op een gecertificeerde wijze worden gewist of overgedragen van alle niet meer in gebruik zijnde opslagmiddelen. De bewijsvoering van de verwijderde gegevens wordt overgedragen aan NHL Stenden. • **Data-overdracht**: Procedures voor volledige data-overdracht (export in gangbare formaten) • **Data vernietiging**: Certificaat van vernietiging na beëindiging contract • **Standaarden**: Gebruik van open standaarden waar mogelijk • **Exportfunctionaliteit**: Mogelijkheid tot complete export op elk moment
1.8	**Rechten van betrokkenen** Uw dienst of applicatie biedt de technische mogelijkheid om adequaat te reageren op een verzoek tot uitoefening van een van deze rechten.

2. SECURITY	
De steeds verder gaande digitalisering van het onderwijs vraagt om flexibele, innovatieve IT. Tegelijkertijd is het onderwijs de laatste jaren steeds vaker doelwit van cyberaanvallen. Afspraken binnen de sector over cyberweer-baarheid en de nieuwe Cyberbeveiligingswet sturen dan ook op cybervolwassenheid binnen het hoger onderwijs.	
2.1	**Cybersecurity & Inschrijversketen (NIS2):** De nieuwe NIS2 wetgeving is van toepassing verklaard op het hoger onderwijs van Nederland en zal naar verwachting begin 2026 in werking treden. Daarnaast is in de Vereniging van Hogescholen (VH) afgesproken dat alle hogescholen voor eind 2028 door moeten groeien naar een cybervolwassenheidsniveau (CMM 3) zoals omschreven in het Surf Toetsingskader Informatiebeveiliging. Van Inschrijvers wordt vereist dat zij ook minimaal aan deze normen voldoen. **1. Beveiligingsstandaarden:** Inschrijver garandeert dat zij beschikt over passende technische en organisatorische beveiligingsmaatregelen conform algemeen erkende standaarden, waaronder ten minste één van de volgende: ISO/IEC 27001,SOC2 Type II of vergelijkbare norm. **2. Incidentmelding:** Inschrijver rapporteert iedere beveiligingsincident met (potentiële) impact op de afgenomen dienst **onmiddellijk**, maar uiterlijk binnen **24 uur** na ontdekking, inclusief aard, impact en getroffen maatregelen. **3. Audit- en inspectierecht:** NHL Stenden heeft het recht om, maximaal eenmaal per jaar en aanvullend bij ernstige incidenten: • een **audit** (remote of on-site) uit te voeren of te laten uitvoeren; • relevante beveiligingsdocumentatie op te vragen, waaronder SOC-rapportages, ISAE3402-verklaringen, penetratietests en security policies. Inschrijver verleent volledige medewerking. Indien auditrapporten reeds beschikbaar zijn, mogen deze worden gebruikt ter vervanging van fysieke audits, mits de scope relevant en actueel is. **4. Sub-leverancier:** Inschrijver draagt er zorg voor dat alle sub-leveranciers die bijdragen aan de uitvoering van de overeenkomst minimaal gelijkwaardige beveiligingsmaatregelen toepassen. Inschrijver blijft volledig verantwoordelijk voor de naleving. **5. Kwetsbaarheden & patching:** Inschrijver past kritieke beveiligingspatches toe binnen maximaal 7 dagen en overige patches binnen 30 dagen. Inschrijver verstrekt op verzoek bewijs van patchbeheer. **6. Continuïteit & herstel:** Inschrijver beschikt over een actueel business continuity plan en disaster recovery plan, inclusief jaarlijkse testen. Recovery time objectives (RTO/RPO) worden contractueel vastgelegd. **7. Informatieverstrekking aan toezichthouders:** Indien een NIS2-toezichthouder informatie opvraagt over de beveiligingsmaatregelen in de keten, zal Inschrijver tijdig alle benodigde informatie beschikbaar stellen.
2.2	**Security by Default:** Bij de inrichting van de applicatie wordt gewerkt volgens het principe van Security by default. Dit betekent dat alle instellingen van meet af veilig worden ingesteld en dat er passende technische en organisatorische maatregelen worden genomen om de verwerking van gegevens zo veilig mogelijk te maken. Doorgifte van gegevens aan derde partijen gebeurt volgens passende technische en organisatorische maatregelen. Beveiligingsmaatregelen zijn gedocumenteerd, worden regelmatig bijgewerkt en kunnen te allen tijde worden opgevraagd door NHL Stenden.
2.3	**STITCH:** De Surf Community voor Cybersecurity professionals (SCIRT) hanteert een checklist voor software en diensten om te voldoen aan minimale security vereisten: de Security Technical IT CHecklist (STITCH). Het betreft een baseline. Inschrijver toont aan dat hij minimaal volgens deze beveiligingsmaatregelen werkt.
2.4	**Informatiebeveiliging:** Inschrijver werkt actief aan informatiebeveiliging, waaronder minimaal: • Beveiligingsbeleid: Gedocumenteerd informatiebeveiligingsbeleid beschikbaar • Risicoanalyse: Periodieke uitvoering en documentatie van risicoanalyses • Vulnerability Management: Actieve scanning op kwetsbaarheden, kritieke kwetsbaarheden verholpen binnen 48 uur, hoge prioriteit binnen 7 dagen; jaarlijkse penetratietests door onafhankelijke partij • Patch management conform branche-standaarden (toetsingskader / ISO27001-2) • Incident response plan: Gedocumenteerd plan voor afhandeling beveiligingsincidenten • Disaster recovery plan: Gedocumenteerd disaster recovery plan met RTO en RPO specificaties • Bewustwording en Training: Duidelijke gebruikershandleidingen voor eindgebruikers en Security awareness trainingen voor het eigen personeel
2.5	**Dataopslag en -verwerking:** • Back-up procedures: Geautomatiseerde back-ups met minimaal dagelijkse frequentie, retentietijd van een half jaar en backup conform 3-2-1 methode ingeregeld. Encryptie dient hierbij toegepast te worden en periodiek dient er een restore test te worden uitgevoerd ter controle van de backup.

	• Datascheiding: De gegevens, configuraties en gebruikers van NHL Stenden moeten bij een multi-tenant omgeving geïsoleerd zijn binnen de gedeelde applicatie en infrastructuur, waardoor er een logische scheiding ontstaat die voorkomt dat andere klanten toegang hebben tot de data van NHL Stenden.
2.6	**Toegangsbeheer en Authenticatie:** Ten aanzien van identificatie en authenticatie gelden specifieke eisen: • Multi-factor authenticatie (MFA): Ondersteuning voor MFA • Single Sign-On (SSO): Ondersteuning voor inlog via SurfConext (SAML 2.0) • Rolgebaseerde toegang: Mogelijkheid tot gedetailleerd rechtenbeheer • Logging van toegang: Audittrails van alle toegang tot persoonsgegevens (minimaal 12 maanden) • Automatische uitlog: Sessies verlopen na inactiviteit (configureerbaar)
2.7	**Netwerk- en Applicatiebeveiliging:** Beschermende maatregelen (geïmplementeerd en onderhouden): • Firewalls: Implementatie van firewalls en intrusion detection/prevention systemen • SOC Siem oplossing tbv detectie afwijkend gedrag en snelle incident response bij kritieke incidenten • DDoS-bescherming: Maatregelen tegen distributed denial of service aanvallen • Secure development: Toepassing van secure coding practices (bijv. OWASP Top 10) • API-beveiliging: Authenticatie en encryptie van API's

3. Architectuur	
NHL Stenden hanteert architectuurprincipes. De inschrijver voldoet hieraan volgens 'Pas toe of leg uit'. Principes zijn voorwaarden, maar als er een goede reden is om beargumenteerd van een principe af te moeten wijken, dan kan de exceptie in overleg afgesproken en vastgelegd worden. NHL Stenden hanteert de Hoger Onderwijs Referentie Architectuur (HORA). De inschrijver neemt kennis van de lagen en modellen van de HORA.	
3.1	**ARP01 Eigenaarschap**: Elk bedrijfsproces (HORA) van NHL Stenden kent een eigenaar. Deze eigenaar is verantwoordelijk voor het kwalitatief uitvoeren van dit bedrijfsproces. Bij inzet van een externe Inschrijver op dit bedrijfsproces zal inschrijver hiervan kennisnemen en zo goed mogelijk beschrijven hoe deze externe inzet bijdraagt aan de kwaliteit van dat bedrijfsproces.
3.2	**ARP02 Kant en klaar:** NHL Stenden streeft naar de inzet van oplossingen die breed in de markt toegepast wordt. We maken hierdoor gebruik van ervaringen en expertise die aan deze oplossing verbonden is. Daarom zijn we tevreden met 80% functionaliteit. Geheel afhankelijk van de vraag is dit principe het uitgangspunt. Mocht de bewezen oplossing niet voldoen en/of er zijn geen alternatieven, dan kan in gesprek mogelijke andere oplossingen/maatwerk besproken worden. In dat geval wordt een risico-impact beschreven, waarin aangegeven wordt of en welk risico er ontstaat door geen marktoplossing in te zetten.
3.3	**ARP03 Volledige ondersteuning**: Voorzieningen, applicaties en systemen worden door Inschrijvers op het meest actuele niveau gehouden. Indien het noodzakelijk is, dan kan, voorzien van argumentatie en besluit, voor een maximale periode van 6 maanden het een-na-hoogste versie-niveau toegepast worden.
3.4	**ARP04 Regievoering**: Vanwege krapte in de arbeidsmarkt en de toenemende complexiteit van digitale bedreigingen streeft NHL Stenden naar managed dienstverlening. De inschrijver geeft aan hoe deze dienstverlening er uit kan zien.
3.5	**ARP05 Cloud first**: Er wordt gebruik gemaakt van schaalbare en flexibele publieke cloud technologie. Slechts beargumenteerd kan on-premise een oplossing zijn.
3.6	**ARP06 Open standaarden en flexibel**: Informatie wordt gedeeld via open standaarden. Proprietary standaarden zijn niet toegestaan, tenzij beargumenteerd is (en besloten) dat er geen andere optie is dan gesloten standaarden.
3.7	**ARP07 Archivering**: Archiefwaardige informatie wordt conform wet- en regelgeving bewaard, volgens het 'archive by design' principe. De inschrijver heeft kennis van de archiefwet. De NHL Stenden archivaris is betrokken voor duiding van de archiefwet in kwestie.
3.8	**ARP08 Data**: Data waarvoor NHL Stenden verantwoordelijk is, wordt veilig bewaard en getransporteerd binnen de EER. Inschrijver zal, wanneer mogelijk, het onderwerp data soevereiniteit in de beantwoording meenemen.
3.9	**ARP09 Centrale datalaag**: Data wordt beschikbaar gesteld via één centrale datalaag van NHL Stenden. Directe toegang tot bronsystemen is niet toegestaan.
3.10	**ARP10 Veiligheid**: Veiligheid wordt bereikt door gebruik te maken van centrale NHL Stenden inloggegevens, ook voor data in externe omgevingen. Daartoe wordt SurfConext of EntraID toegepast. Indien er aanleiding voor is zal een DPIA-assessment uitgevoerd worden. Inschrijver geeft aan of er gebruik gemaakt wordt van toeleveranciers en derde partijen, en met welk doel.

4. Informatievoorziening	
Voor NHL Stenden is een betrouwbare en goed ingerichte informatievoorziening essentieel voor het functioneren van onze onderwijs-, onderzoeks- en ondersteunende processen. Een samenhangend IV-landschap waarborgt dat informatie veilig, toegankelijk en consistent beschikbaar is, en vormt daarmee een voorwaarde voor continuïteit, kwaliteit en doelmatige dienstverlening.	
4.1	**Aansluiting op informatiestrategie:** Inschrijver toont aan hoe de aangeboden oplossing bijdraagt aan de realisatie van een robuuste, flexibele en toekomstbestendige digitale leer- en werkomgeving, in lijn met de ambitie van NHL Stenden om het digitale fundament ("digital backbone") voor de hogeschool te vormen. De oplossing biedt ondersteuning aan strategische pijlers zoals eenduidige flexibele informatievoorziening, data gedreven werken, innovatie en ethisch en duurzaam gebruik van technologie. Hierbij wordt aangesloten op de inzet van business intelligence binnen NHL Stenden voor selfservice, analytics en dashboarding.
4.2	**Regie en sturing:** NHL Stenden wil met een stuurmodel werken waarin de hogeschool stuurt op functionaliteit, informatiemanagement en –beleid, waarbij een groot deel van het technisch beheer en onderhoud belegd wordt bij gekwalificeerde externe partners. De inschrijver maakt inzichtelijk hoe hij invulling geeft aan deze rolverdeling en hoe de samenwerking en afstemming met NHL Stenden als regievoerder verloopt. Tevens beschrijft inschrijver de aanpak voor kennisoverdracht en –borging.
4.3	**Integratie en samenhang:** De aangeboden oplossing sluit naadloos aan op de integrale informatievoorziening van NHL Stenden en vermijdt redundantie of overlap met bestaande systemen. Inschrijver volgt de NHL Stenden standaarden voor integratie en gegevensuitwisseling (API's, datalaag) en draagt hierdoor bij aan een eenduidige en centrale management-informatievoorziening.
4.4	**Governance en transparantie**: Inschrijver committeert zich aan de governance-structuur van NHL Stenden en maakt afspraken over rollen, verantwoordelijkheden en bevoegdheden transparant en controleerbaar. Wijzigingen in dienstverlening of onderaanneming worden vooraf afgestemd. Inschrijver verschaft ons de benodigde sturingsinformatie om de regierol effectief te kunnen vervullen.
4.5	**Strategisch partnership:** Als strategisch partner denkt en werkt Inschrijver proactief mee met NHL Stenden. Inschrijver zet zijn expertise en ervaring in het hoger onderwijs in om te adviseren over zaken als integratie, architectuur, informatiebeveiliging en gebruikersadoptie.
4.6	**Standaardisatie:** De aangeboden oplossing bestaat uit standaard “off-the-shelf” functionaliteit. Maatwerk wordt tot een minimum beperkt en alleen ingezet als dit aantoonbaar noodzakelijk is en is vastgesteld met NHL Stenden. Updates en upgrades van de standaardoplossing worden zonder meerkosten en verstoring van bedrijfsprocessen doorgevoerd.
4.7	**Gebruikerservaring:** Inschrijver staat garant voor een optimale gebruikerservaring die aansluit bij de behoeften van studenten, docenten en andere eindgebruikers. De oplossing beschikt over een intuïtieve, snelle, toegankelijke interface, krachtige zelfservice-functionaliteit en contextafhankelijke ondersteuning (online help, how-to guides, e-learning academie).
4.8	**Wet- en regelgeving:** Inschrijver garandeert dat de aangeboden dienstverlening voldoet aan alle Europese en Nederlandse relevante wet- en regelgeving, nu en in de toekomst. Dit omvat onder andere de Algemene Verordening Gegevensbescherming (AVG), AI-Act, de Archiefwet en Archivering volgens MDTO standaarden, de wet Digitaal toegankelijkheid overheid, de European accessibility act en de Wet op Onderwijstoezicht (WOT) met specifieke eisen aan de bescherming van leerling gegevens, de bescherming van minderjarigen, en transparantie over de verwerking van deze gegevens binnen onderwijsinstellingen. Wijzigingen in wet- en regelgeving worden proactief gesignaleerd en vertaald naar de dienstverlening.
4.9	**Inschrijversmanagement:** Inschrijver draagt waar van toepassing zorg voor Inschrijversmanagement: • Sub-leveranciers: Actuele lijst van sub-leveranciers en hun locaties. • Ketenverantwoordelijkheid: Inschrijver blijft verantwoordelijk voor sub-leveranciers. Due diligence: Bewijs van screening van personeel met toegang tot data van NHL Stenden.
4.10	**AI:** Indien de applicatie AI gebruikt, wordt de Inschrijver geacht te voldoen aan de Europese AI verordening (AI Act), waaronder: • NHL Stenden data mag niet zonder expliciete toestemming gebruikt worden voor trainingsdoeleinden in AI modellen • De Inschrijver moet kunnen uitleggen of en hoe AI wordt ingezet in de applicatie. • Indien de applicatie AI gebruikt, moet de Inschrijver uitleg kunnen geven over de algoritmes, dataverwerking en besluitvorming. De Inschrijver moet aantoonbare maatregelen nemen tegen discriminatie en ongewenste bias in AI-modellen

5. IT Servicemanagement	
Servicemanagement richt zich op de kwaliteit, continuïteit en gebruikerservaring van de diensten die aan onze eindgebruikers worden geleverd. Door procesbeheersing en heldere afspraken met de Inschrijvers van de diensten worden risico's beperkt en wordt dienstverlening voorspelbaar en conform afgesproken servicelevels geleverd.	
5.1	Inschrijver werkt middels een SLA waarin tenminste de volgende zaken worden opgenomen: • Omschrijving van de te leveren dienst(en) met duidelijke scope-afbakening • Voertaal: minimaal NL en UK • Beschikbaarheid: volgens af te spreken uptime (afhankelijk van belang van de systemen) • Performance: Transparante monitoring en rapportage • Rapportages: rapportage rondom nader af te spreken KPI's • Responsetijden: Afspraken over reactietijden bij storingen, wijzigingen en nieuwe functionaliteiten • Oplostijden: Afspraken over oplostijden bij storingen, wijzigingen en nieuwe functionaliteiten • Support beschikbaarheid: 24/7 bereikbaarheid voor kritieke (security) incidenten
5.2	Inschrijver heeft de volgende ITIL-processen geïmplementeerd en is bereid om deze processen af te stemmen op de NHL Stenden processen, bijvoorbeeld middels een Dossier Afspraken en Procedures (DAP): • Incident management • Change management • Problem management • Service Asset & Configuration management
5.3	Inschrijver is bereid om haar SMT (Service Management Tool) te koppelen aan de SMT van NHL Stenden zodat er een interne 1e lijn en externe 2e lijn bewerkstelligd kan worden. NHL Stenden gebruikt Topdesk, voorkeur koppeling met API.