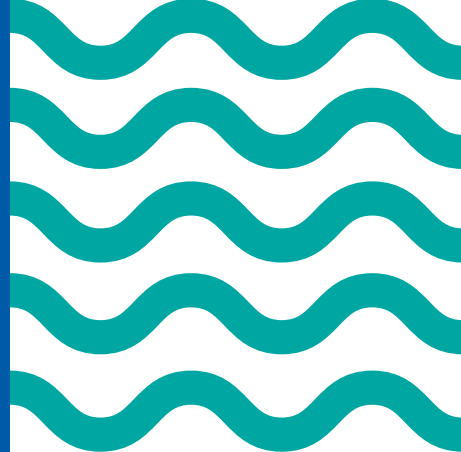


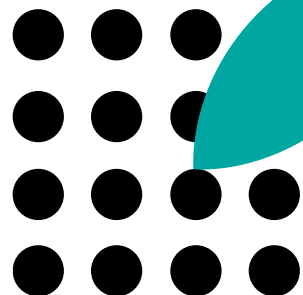
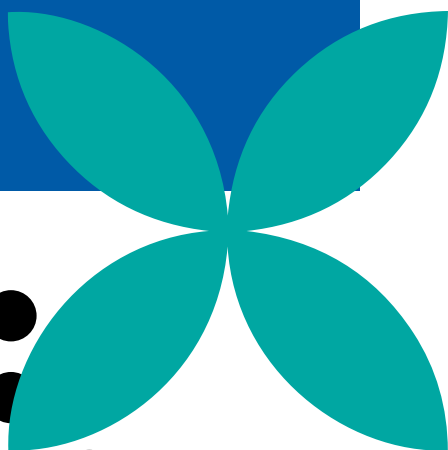


university of
applied sciences



NHL Stenden

Architectuurprincipes



De 10 architectuurprincipes

ARP01	Eigenaarschap
ARP02	Bewezen oplossingen
ARP03	Altijd up-to-date
ARP04	Regievoering
ARP05	Cloud first
ARP06	Open standaarden
ARP07	Archivering
ARP08	Veilige dataopslag
ARP09	Centrale datalaag
ARP10	Single Sign-on





ARP01 Eigenaarschap

Toelichting	Alle data, elke applicatie en elke technologie heeft een eigenaar en daarmee verantwoordelijke voor de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV).
Motivatie	Een eigenaar kent de inhoud van de materie, weet wat er mee bedoeld wordt en wat de risico's zijn bij ontbreken of onvolledig zijn. Voor data-element, applicatie, techniek die van elkaar afhankelijk zijn is het noodzakelijk om te weten wie voor dat alles verantwoordelijk is (=eigenaar), om te kunnen bespreken wat de impact is bij wijzigingen en nieuwe koppelingen.
Implicatie	Het is niet toegestaan om data, applicatie, techniek te gebruiken of te introduceren bij NHL Stenden, zonder dat bekend is wie de eigenaar is. • Van ieder data-element, applicatie en techniek is de eigenaar bekend. De eigenaar is de persoon die de relevante materiedeskundige is, of de leidinggevende van de afdeling/dienst/academie waarin zich het data-element, applicatie, techniek zich bevindt. De eigenaar kan een (functioneel/technisch) beheerder zijn, een teamleider, directeur of CvB. • De eigenaar is als materiedeskundige in staat om risico's, consequenties, toekomstige ontwikkelingen te duiden, en is verantwoordelijk voor de besluitvorming hieromtrent.

ARP02 Bewezen oplossingen

Toelichting	We gebruiken bewezen tools. Ons applicatieportfolio biedt inzicht in geschikte applicaties voor verschillende activiteiten, zowel gelicentieerd als gratis. De opdracht is: geen maatwerk (laten) maken. Mis je een functionaliteit? Onderzoek de markt op bestaande apps en neem contact op met het CIO Office. Ook als je echt behoefte hebt aan een nieuwe functionaliteit (innovatie).
Motivatie	We zijn een onderwijsinstelling die vergelijkbaar is met andere onderwijsinstellingen. We delen een gezamenlijke architectuur (HORA). Invulling van componenten wordt gevonden in oplossingen die breed gedragen worden in het hoger onderwijs. Als dat niet het geval is, zoeken we naar oplossingen die breed gebruikt worden in de (internationale) markt. Dat betekent dat we tevreden zijn met 80%, omdat andere organisaties hiermee ook in hun informatievoorziening kunnen voorzien. We gaan niet zelf oplossingen maken, of laten maken, als er een marktoplossing aanwezig is. Hiermee voorkomen we dat we eigen maatwerkoplossingen creëren die geen gebruik maken van breed gedragen oplossingen (toekomstvastheid, beheerbaarheid, schaalbaarheid, veiligheid, security, vervangbaarheid, etc). Uiteraard moet standaardisatie en hergebruik innovatie niet in de weg staan. Dit architectuurprincipe (ARP02) moet gelezen worden als de voorwaarden die innovatie makkelijker maakt. Bijvoorbeeld, een innovatieve oplossing moet makkelijk aangesloten kunnen worden op de bestaande infrastructuur, omdat deze infrastructuur gebruik maakt van standaardisatie en hergebruik. Vergelijk alle stopcontacten in Europa die standaard zijn, je kunt daar alles op aansluiten. Zie ook ARP06.
Implicatie	Het is niet toegestaan om maatwerk te ontwikkelen, als er geschikte oplossingen in de markt aanwezig zijn (kant en klaar). • De Collaborative Trust Framework^{*)} wordt opgevolgd (open source, broncode, maatwerk door derde partijen) • Bij aanvraag van nieuwe oplossingen wordt eerst door CIO Office gekeken of er al een oplossing voor de gevraagde functionaliteit aanwezig is. Indien dat het geval is, wordt in overleg met de aanvrager in principe deze bestaande oplossing gehanteerd. Alleen in uitzonderingsgevallen kan beargumenteerd een uitzondering worden toegestaan door het CIO Office. • Waar dezelfde functionaliteit door meerdere oplossingen wordt gerealiseerd, zal gestart worden met een harmonisatie. Initiatief hiertoe ligt bij de eigenaar/eigenaren van de huidige functionaliteit(-en). Dat wil zeggen: een keuze voor 1 van de in gebruik zijnde oplossingen, en uitfasering van de overige. • Innovatie en ontwikkeling moet altijd mogelijk zijn. Indien het principe dit tegenhoudt (of lijkt te houden), dan wordt in een open dialoog bekeken wat de mogelijkheden zijn (dat zou ook het bijwerken van het principe kunnen zijn). ^{*)} https://communities.surf.nl/publieke-waarden/artikel/collaborative-trust-framework-zelfregulatie-om-publieke-waarden-te



ARP03 Altijd up-to-date

Toelichting	Alle applicaties en systemen houden wij of onze leverancier up-to-date, zodat de data veilig blijft. De CMDB is daarin leidend en actueel.
Motivatie	Intern en extern beheerde componenten worden op het laatste patch-niveau gehouden. Dit verhoogt de veiligheid van de systemen en de data die daarmee verwerkt worden. Beargumenteerd mag het patch-niveau tijdelijk op het een-na-actueelste niveau gehouden worden. Onder componenten wordt alles verstaan waar een updateniveau te duiden is (hardware, middleware, software). In de CMDB worden de componenten geregistreerd en bijgehouden, zodat we 1 leidende administratie hebben.
Implicatie	Componenten die zich op een lager niveau bevinden, moeten zo spoedig mogelijk op het laatste niveau worden gebracht, of worden vervangen. Leveranciers van componenten hebben een patch-/updatebeleid beschikbaar en rapporteren hierover via de bestaande service-lijnen.



ARP04 Regievoering

Toelichting	NHL Stenden fungeert als regisseur richting IT-dienstverleners (intern en extern) en waarborgt zo de samenhang en kwaliteit van de IT-dienstverlening.
Motivatie	De rol van NHL Stenden verschuift van uitvoering naar het uitzetten van taken en het bewaken of die taken goed worden uitgevoerd. Elke functionaliteit en voorziening wordt als dienst afgenomen, tenzij beargumenteerd dat we het zelf (beter) kunnen doen. Hiervoor heeft NHL Stenden een Sourcing Strategie. Waar de oplossing ook ligt, er is altijd een backup, recovery, disaster handling, exit strategie aanwezig.
Implicatie	Van bestaande diensten die we nog 'intern' faciliteren, wordt actief beoordeeld of dit nog steeds de meest gewenste oplossing is. Altijd en frequent wordt beoordeeld of backup, recovery, disasterplannen, exit strategie nog actueel is, ongeacht of de dienst intern of extern belegd is. Periodiek wordt een recovery ingepland. Recovery vindt plaats in een separate (test-)omgeving. De eigenaar (ARP01) initieert de recovery en beoordeelt dat de recovery tijdig, juist en volledig is.



ARP05 Cloud first

Toelichting	We gebruiken openbare cloudtechnologieën voor schaalbaarheid en flexibiliteit met aandacht voor duurzaamheid en energie. Systemen in eigen beheer zijn alleen mogelijk na goedkeuring van het CIO Office.
Motivatie	Snel en flexibel kunnen reageren is niet mogelijk met langlopende contracten waarin hardware is opgenomen. Met publieke cloud-technologie wordt gebruik gemaakt van platformen die snel op- en afgeschaald kunnen worden, vandaar dat private en hybride cloud-technologie minder voorkeur geniet. Pay per use is de norm. We blijven wel altijd kijken naar de kostefficiëntie, zoals wat er nodig is om snel op- en af te schalen; we kunnen dit niet zelf 7x24 doen (ARP04 Regievoering).
Implicatie	• On premise componenten zijn niet toegestaan, tenzij beargumenteerd dat er geen andere keuze is. • Bestaande on premise voorzieningen worden beoordeeld of er een cloud-variant mogelijk is. On premise componenten zijn niet toegestaan, tenzij beargumenteerd dat er geen andere keuze is. • Bestaande on premise voorzieningen worden beoordeeld of er een cloud-variant mogelijk is.



ARP06 Open standaarden

Toelichting	Het koppelen van systemen en het transporteren van data realiseren we via open standaarden. Zo zijn we transparant over het distribueren van data op een veilige manier. Gebruik van niet-open standaarden is alleen toegestaan als er geen open alternatief is met adequate beveiligingsmaatregelen.
Motivatie	NHL Stenden is een open organisatie, die samenwerking stimuleert. Samenwerking wordt mogelijk door gebruik te maken van open standaarden, zowel aan de kant van NHL Stenden als aan de kant van de samenwerkende partner/leverancier. Hiermee wordt samenwerking bevorderd en is er inzicht in de mate van toegepaste security. Gesloten standaarden zijn niet toegestaan, tenzij er geen vergelijkbare open standaard beschikbaar is en die gesloten standaard adequate en afgestemde securitymaatregelen beschrijft. Standaarden zullen actief op het laatste beveiligingsniveau gebracht worden, of beargumenteerd 1 niveau daaronder.
Implicatie	• Nationale en internationale samenwerkingsstandaarden (bv HORA, NIST) worden actief gehanteerd. • Gesloten standaarden zijn niet toegestaan. • Een lijst met gebruikte open standaarden wordt bijgehouden door CIO Office. • Toegestane open standaarden op • https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/open-standaarden/ • https://openonderwijsapi.nl/#/

ARP07 Archivering

Toelichting	Archiefwaardige informatie wordt volgens wet- en regelgeving bewaard. Afwijkende bewaar- en vernietigingstermijnen en –locaties worden afgestemd met de archivaris.
Motivatie	In principe geldt ‘Archive by design’, waarbij de volgende ‘first’ criteria gelden zodat informatie duurzaam toegankelijk is en blijft: digitaal first, centraal first, cloud first, eenmalig opslaan first. De informatiehuishouding is op orde en data wordt bewaard volgens de afgesproken bewaartermijnen, zodat de verantwoording van de kwaliteit het onderwijs- en de niet-onderwijsprocessen is geborgd.
Implicatie	• Van de relevante systemen wordt in kaart gebracht welke data zich daarin bevinden en data wordt voorzien van de minimaal benodigde set van metadata, die nodig is voor het uitvoeren van de processen en het beheer daarvan. • De archivaris geeft aan welke data bewaard moet worden, inclusief termijnen, voorwaarden en eventuele uitzonderingen. • Digitale data wordt in principe digitaal verwerkt en gearchiveerd. Dit gebeurt voornamelijk in centrale systemen in de Cloud, waarbij een onderscheid wordt gemaakt tussen werkarchieven en het wettelijk archief. Via semi-automatische processen wordt deze data gecontroleerd bewaard en indien nodig vernietigd na het verstrijken van de geldende bewaartermijnen. Archiefwet 1995 - https://wetten.overheid.nl/BWBR0007376/2022-05-01 WHW 1992 - https://wetten.overheid.nl/BWBR0005682/2024-01-01 Selectielijst_Hogescholen_Versie_mei_2022 – https://www.vereniginghogescholen.nl/kennisbank/vereniging-hogescholen/artikelen/selectielijst-hogescholen-versie-2022 AVG 2016 - https://autoriteitpersoonsgegevens.nl/uploads/imported/verordening_2016_-_679_definitief.pdf Beoordelingskader_accreditatiestelsel_hoger_onderwijs_Nederland_2018 - https://www.nvao.net/files/attachments/.89/Beoordelingskader_accreditatiestelsel_hoger_onderwijs_Nederland_2018.pdf



ARP08 Veilige dataopslag

Toelichting	Data is altijd betrouwbaar, veilig opgeslagen en raadpleegbaar, onafhankelijk van locatie en tijd. Medewerkers en studenten beheren zoveel mogelijk hun eigen gegevens in systemen. Omdat data gevoelig is en waarde heeft, hanteren we deze beleidsregels hoe hiermee om te gaan.
Motivatie	Data is altijd integer en zal altijd veilig opgeslagen en geraadpleegd kunnen worden, locatie en tijdonafhankelijk. Medewerkers en studenten beheren zoveel mogelijk hun eigen gegevens in systemen.
Implicatie	• Doelbinding bepaalt of gegevens uitgewisseld mogen worden; zonder doelbinding wordt het gegeven niet uitgewisseld. • Indien noodzakelijk en voorgeschreven, zal data voorzien zijn van een BIV-classificatie *) • Data wordt afdoende versleuteld opgeslagen en afdoende versleuteld uitgewisseld (zowel tussen interne als externe systemen) • Verplichtingen die in de AVG zijn opgenomen, en de aanwijzingen in de 'selectielijst hogescholen' **), worden opgevolgd (bewaren, verwijderen) *) https://www.surf.nl/files/2019-03/201512-leidraad-classificatie-scipr-2.0.pdf **) https://www.verenighogescholen.nl/kennisbank/vereniging-hogescholen/artikelen/selectielijst-hogescholen-versie-2022



ARP09 Centrale datalaag

Toelichting	Data is toegankelijk via een (1) centraal systeem. Toegang en rollen worden geregistreerd.
Motivatie	Data wordt eenmalig opgeslagen en meervoudig opgevraagd. Daarmee wordt voorkomen dat dezelfde data op vele plaatsen opgeslagen en aangepast wordt, met als gevolg dat een veelheid aan data-interpretatie ontstaat: de integriteit, vertrouwelijkheid en beschikbaarheid van de keten komt in gevaar. Indien data opvraagbaar moet zijn, dan zal dat opvragen plaatsvinden bij één centrale bron (centrale datalaag), waar de voorwaarden zijn vastgelegd wanneer opgevraagd en bewerkt mag worden. Dit zogenaamde register wordt beheerd en bewaakt door het CIO Office.
Implicatie	• Er worden geen systemen direct gekoppeld met bronsystemen; ontsluiting van data zal plaatsvinden via de centrale datalaag. • Gegevens worden altijd geregistreerd bij de bron en geschikt gemaakt voor meervoudig gebruik • Gegevens worden geleverd door de bron aan de centrale datalaag (push) • Alle data die uitgewisseld worden, moet voorzien zijn van een BIV-classificatie



ARP10 Single Sign-on

Toelichting	Toegang tot alle NHL Stenden-systemen en –data, zowel intern als in de cloud, gaat met een (1) set inloggegevens. Inloggen gebeurt via SurfConext of EntraID. Twee Factor Authenticatie passen we toe wanneer het risico op misbruik groot is.
Motivatie	Er is binnen NHL Stenden een centrale plaats waarin de inloggegevens zijn opgeslagen. Alle systemen waarop ingelogd moet worden, maken gebruik van deze centraal opgeslagen inloggegevens. Het is niet toegestaan om duplicaten van deze inloggegevens op te slaan in andere systemen. Door zowel Entra ID naast Surf Conext als IDP te ondersteunen, verbeteren we de toegankelijkheid, veiligheid en interoperabiliteit van onze systemen voor zowel nationale als internationale gebruikers. Aangezien Entra ID al wordt ondersteund door NHL Stenden en samen met Surf Conext de enige twee SSO-tools zijn die NHL Stenden ondersteunt, kunnen we een naadloze integratie en consistente gebruikerservaring garanderen met een minimale toename van beheer.
Implicatie	• Systemen waarop ingelogd wordt met een NHL Stenden-account, maken slechts gebruik van de centrale plaats bij NHL Stenden waar de inloggegevens zijn opgeslagen. • Het is niet toegestaan om duplicaten van NHL Stenden-accounts en/of -wachtwoorden aan te maken, te gebruiken of op te slaan. Ook is het niet toegestaan om deze inloggegevens op te slaan in andere omgevingen en systemen, of deze zich nu binnen of buiten de NHL Stenden-omgeving bevinden.