Nucleaire Energie Organisatie Nederland

MEMO

VISIE IT DIGITAL FOUNDATION

Samenvatting

NEO NL gaat een nucleaire faciliteit ontwerpen, bouwen en exploiteren met een vitale maatschappelijke functie. Onze informatievoorziening moet daarom te allen tijde betrouwbaar, veilig en traceerbaar zijn. Digitale transformatie is voor NEO NL geen technologische exercitie, maar een strategische randvoorwaarde voor onze missie.

De nucleaire context waarin NEO NL opereert, stelt verregaande eisen aan de informatievoorziening en -beveiliging. Deze ICT-visie formuleert de strategische koers om te transformeren van de huidige DICTU-omgeving naar een eigen, beheersbaar ICT-landschap.

De centrale ambitie is een digitale werkomgeving die zowel de operationele continuïteit als de strategische wendbaarheid waarborgt.

Deze transformatie is een strategische noodzaak die niet alleen de technologie raakt, maar ook onze organisatiecultuur, werkwijzen en de relatie met de markt. De transformatie naar het nieuwe landschap rust op vier dragende pijlers:

- Identity-First Benadering: Identiteit is onze primaire verdedigingslinie. NEO NL implementeert een Identity & Access Management platform. Elke toegangspoging van gebruikers of apparaten wordt hiermee continu en expliciet geverifieerd en gelogd.
- Beveiliging en data-soevereiniteit en -autonomie vormen het fundament van elke architectuurbeslissing. Via strikte policy's wordt voldaan aan de strengste nationale en internationale nucleaire normen.
- De digitale werkomgeving wordt uniform ingericht. Dit verlaagt de beheerkosten en verbetert de securitypositie, waarbij open standaarden, overdraagbaarheid en een exitstrategie de strategische autonomie bewaken.
- Verbeteringen aan het ICT-landschap worden iteratief en beheerst doorgevoerd. Een passende governancestructuur bewaakt hierbij de samenhang en de risico's.

Binnen de vitale infrastructuur van NEO NL is continuïteit en veiligheid niet onderhandelbaar, wij maken afspraken met leveranciers voor het leveren van een gegarandeerd resultaat.

Uitgangspunten digitale werkomgeving

Architectuurprincipes

De architectuurprincipes van NEO NL zijn vastgelegd in een document: *NEO NL Enterprise Architecture*. Zij gelden voor het volledige ICT-landschap en voor alle initiatieven, percelen en onderliggende solution-architecturen. Zeven architectuurprincipes bepalen het targetlandschap en vallen uiteen in twee thema's:

1. Functionele samenhang en efficiency
    - *EA01 Value-Driven Architecture*: keuzes volgen uit bedrijfswaarde en risico, niet uit technologievoorkeur.

- *EA06 Common Foundations*: gedeelde (infra) platformen en digital building blocks worden hergebruikt in plaats van per dienst opnieuw ingericht.
- *EA07 Cloud-Enabled Architecture*: cloud is het voorkeursdeploymentmodel, mits volledig wordt voldaan aan de eisen op het gebied van regelgeving, soevereiniteit en security. Waar dat niet aantoonbaar is, geldt de voorkeur niet.
- *EA10 Proven and Reliable Technology*: gebruik van in de markt bewezen technologie, in het bijzonder voor kritieke omgevingen.

2. Onafhankelijkheid en control
   - *EA08 Security and Compliance by Design*: zero trust, least privilege en toetsbaarheid zijn onderdeel van het ontwerp en niet van de oplevering.
   - *EA09 Sovereignty and Control by Design*: NEO NL behoudt zeggenschap over gevoelige data en kritieke systemen, ook wanneer de uitvoering bij de markt ligt.
   - *EA05 Modular and Interoperable by Design*: open standaarden en losse koppeling, zodat diensten vervangbaar blijven en een exit uitvoerbaar is.

De twee thema's wijzen niet dezelfde kant op. Het eerste vraagt om bundeling, het tweede om scheiding. De ontwerpregel is daarom: scheiden waar onafhankelijke controle vereist is, bundelen waar functionele samenhang dit rechtvaardigt.

Greenfield-status en groeiprognose

NEO NL is opgericht in februari 2026. Als jonge organisatie bevindt NEO NL zich in een unieke greenfield-situatie: alle ICT-voorzieningen, infrastructuren en de IT-organisatie worden vanaf de grond opgebouwd. Binnen drie tot vijf jaar groeit de organisatie naar verwachting van 150 naar ongeveer 1.000 werkplekken. Het ICT-landschap moet zo worden ontworpen dat het deze opschaling in omvang, complexiteit en data-infrastructuur naadloos en veilig kan faciliteren.

NEO NL contracteert partners die intrinsiek in staat en bereid zijn om gedurende de looptijd van de overeenkomst flexibel mee te bewegen met de organisatorische en technologische dynamiek. Dit omvat flexibiliteit over drie assen:

- Volume-flexibiliteit: het naadloos op- en afschalen van de contractomvang parallel aan de groei van het aantal medewerkers.
- Functionele flexibiliteit: het inhoudelijk aanpassen, moderniseren of volledig stopzetten van bestaande diensten wanneer onze context daarom vraagt.
- Portfolio flexibiliteit: het introduceren van nieuwe, nog onvoorziene ICT-voorzieningen binnen de bestaande contractuele kaders.

Innovatie-eisen

Binnen de vitale, nucleaire infrastructuur van NEO NL is technologische stilstand een veiligheidsrisico. Innovatie is daarom geen vrijblijvende optie, maar een harde eis. Van partners wordt verwacht dat zij proactief bijdragen aan het continu verbeteren van de weerbaarheid, wendbaarheid, digitale autonomie en compliance van de geleverde diensten.

Vier strategische ICT-pijlers

Pijler 1: Identity-First benadering (eIAM als enabler)

Identiteit is de primaire verdedigingslinie binnen ons zero-trust model. NEO NL implementeert een centraal Enterprise Identity & Access Management (eIAM) platform, welke op dit moment nog ingekocht moet worden. NEO NL positioneert eIAM bewust als een interne foundation layer en behoudt eigenaarschap, beleid en risicobesluiten. Als single source of identity voedt dit platform alle werkomgevingen en achterliggende applicaties. Dit verlaagt de complexiteit en verhoogt de traceerbaarheid. Het platform wordt ontworpen op basis van hoge beschikbaarheid en schaalbaarheid, waarbij moderne protocollen (OAuth, OpenID Connect en SAML) de standaard zijn.

Pijler 2: Security by Design in de nucleaire context

In de nucleaire context is cybersecurity geen achteraf toegevoegde schil, maar het fundament van elke beslissing. Hiervoor bouwen we onder meer op de regelgeving door ANVS en IAEA. De architectuur voldoet aan zero-trustprincipes en aan de toepasselijke wet- en regelgeving, normenkaders en richtlijnen, waaronder de Cyberbeveiligingswet, de Wet weerbaarheid kritieke entiteiten, de BIO2 en - voor zover van toepassing - ABRO/ en TBB3 en specifieke nucleaire regelgeving. Dit vereist een organisatiebrede security-aware cultuur: veiligheid is de verantwoordelijkheid van elke medewerker, architect en leverancier. Fysieke en digitale dreigingen zijn onlosmakelijk met elkaar verbonden. *Security by Design* is daarom de leidende filosofie voor zowel de toekomstige Operational Technology (OT) in de faciliteit als de IT-systemen die NEO NL vandaag al inricht.
Het ICT-landschap van NEO NL wordt aantoonbaar ontworpen en getoetst langs de strengste nationale en internationale normeringsstandaarden:

- Internationaal (Nucleair & Cybersecurity): IAEA Nuclear Security Series (NSS), de richtlijnen van de ANVS, en de IEC-standaarden 62443, 62645 en 62859.
- Kwaliteit & Informatiebeveiliging: ISO 19443 (specifiek voor de nucleaire sector), ISO 9001 en ISO/IEC 27001.
- Nationale kaders: de Cyberbeveiligingswet en de relevante wet- en regelgeving voor vitale infrastructuur.

Pijler 3: Gestandaardiseerde digitale werkplek

Er wordt gekozen voor een uniforme digitale werkplek. De functionele en technische inrichting wordt per risico- en gebruikssituatie bepaald en blijft technologieneutraal. Standaardisatie verkleint de attack surface (aanvalsvector) en vereenvoudigt het patch- en lifecyclemanagement. Dit verlaagt de Total Cost of Ownership (TCO) en minimaliseert de belasting op de servicedesk. Voor de medewerker resulteert dit in een consistente, veilige en hoogpresterende gebruikerservaring. De architectuur is zodanig ingericht dat een overstap naar een andere werkplekoplossing operationeel en contractueel mogelijk blijft. Open standaarden, overdraagbaarheid van data en configuraties en waar passend open source waarborgen de strategische autonomie die past bij een vitale maatschappelijke organisatie.

Pijler 4: Governance

De dynamiek van de transformatie vraagt om een iteratief en beheerst deliverymodel, gecombineerd met strikte architectuurbewaking. Portfoliomanagement prioriteert projecten op basis van strategische waarde en risico. De te ontwerpen governancestructuur functioneert niet als bureaucratische drempel, maar als een vliegwiel voor snelle, transparante en reproduceerbare besluitvorming en risicobeheersing. NEO NL richt deze governance in de komende periode verder in. De precieze organisatievorm, bemensing en consequenties voor bijvoorbeeld af te sluiten SLA's zijn nog niet vastgesteld. Door de organisatie actief te betrekken bij de transformatie, verankeren we securitybewustzijn en creëren we het noodzakelijke draagvlak voor de nieuwe manier van werken.

IT Service Management en Service Integration

NEO NL richt IT Service Management en Service Integration in op basis van internationaal erkende normen en best practices. ISO/IEC 20000-1 en ITIL v4 vormen daarbij een belangrijk referentiekader voor de inrichting, beheersing en continue verbetering van het servicemanagementsysteem. SIAM wordt gehanteerd als best-practice framework voor de inrichting en uitvoering van service-integratie.

Eén geïntegreerde dienstverlening

NEO NL kiest voor een ICT-landschap waarin gespecialiseerde marktpartijen verantwoordelijk zijn voor verschillende onderdelen van de dienstverlening. Voor medewerkers, stakeholders en de organisatie moet dit landschap echter functioneren als één samenhangende ICT-dienstverlening. De grenzen tussen leveranciers en contracten mogen niet zichtbaar worden in de kwaliteit en continuïteit van de dienstverlening. Het uitgangspunt hierbij is end-to-end servicemanagement: niet de afzonderlijke technische component of leverancier staat centraal, maar de volledige dienstverlening zoals deze door NEO NL en haar medewerkers wordt ervaren.

Gebruikersgerichte dienstverlening

NEO NL streeft daarom naar een herkenbare en laagdrempelige toegang tot ICT-ondersteuning, waarbij gebruikers niet zelf hoeven te bepalen welke leverancier verantwoordelijk is voor een incident, verzoek of probleem. De lead supplier as service integrator zorgt voor de juiste routering, coördinatie en opvolging binnen de achterliggende ICT-keten en bewaakt de voortgang tot de dienstverlening voor de gebruiker is hersteld of het verzoek is afgehandeld.

Service-integratie in het multi-vendor landschap (SIAM)

In het multi-vendor landschap van NEO NL is samenhang tussen de verschillende ICT-diensten essentieel. NEO NL kiest er daarom voor om de operationele service-integratie bij aanvang te beleggen bij een gespecialiseerde marktpartij. Deze partij (lead supplier as service integrator) vormt de verbindende schakel tussen de verschillende ICT-leveranciers en ondersteunt NEO NL bij het realiseren van één samenhangende end-to-end dienstverlening. Iedere leverancier blijft verantwoordelijk voor de kwaliteit en uitvoering van de eigen dienstverlening. De service-integratiepartner neemt deze verantwoordelijkheid niet over, maar draagt eraan bij dat de afzonderlijke diensten als één geïntegreerde ICT-keten functioneren.

Uniforme processen en centrale informatiepositie

Effectieve regie vereist een betrouwbare en gedeelde informatiepositie. NEO NL streeft daarom naar één centrale of aantoonbaar geïntegreerde IT-servicemanagementinformatiepositie waarin relevante operationele informatie over de verschillende ICT-diensten en leveranciers samenkomt. Federatieve leveranciersplatformen zijn toegestaan mits de informatiepositie aantoonbaar is geïntegreerd. Incidenten, dienst verzoeken (service requests), problemen, wijzigingen, configuraties, kennis en andere relevante service-informatie worden volgens uniforme uitgangspunten geregistreerd en beheerd. Leveranciers worden verplicht om hun dienstverlening hierop aan te sluiten en de voor ketenregie noodzakelijke informatie tijdig beschikbaar te stellen.

Integratie van nieuwe diensten en leveranciers

Nieuwe diensten worden volgens een uniforme service-introductieaanpak opgenomen in de bestaande dienstverlening. Daarbij worden onder andere de aansluiting op servicemanagementprocessen, ITSM-tooling, support- en escalatiemodellen, monitoring, configuratieregistratie, kennisoverdracht en operationele verantwoordelijkheden ingericht voordat een dienst volledig in beheer wordt genomen. De service-integratiepartner ondersteunt en coördineert deze onboarding en zorgt dat nieuwe leveranciers vanaf de start aansluiten op de geldende processen en samenwerkingsafspraken van NEO NL.

Regieorganisatie

Orkestratie in plaats van uitvoering

NEO NL heeft op dit moment een regie-organisatie die zich wil ontwikkelen richting de juiste vorm om de doelstellingen van NEO NL te realiseren. De precieze toekomstige omvang en taakverdeling van de interne IT-organisatie zijn nog niet vastgesteld. Voor nu is de kern van onze sturing helder: NEO NL bepaalt het wat en het waarom: wij stellen de strategische doelen, architectuurprincipes, securitykaders, compliancenormen en interoperabiliteitseisen. De leverancier bepaalt het hoe: binnen onze kaders is de leverancier verantwoordelijk voor de technische invulling, detailarchitectuur en operationele realisatie. De operationele en uitvoerende SIAM-, regie- en servicemanagementtaken worden bij aanvang bij de leverancier belegd. NEO NL kan geselecteerde taken tijdens de looptijd gefaseerd overnemen via vooraf geprijsde opties, overdrachtsafspraken en acceptatiecriteria. Deze filosofie vormt de basis voor onze aanbestedingen en contracten. We selecteren partners die deze professionele verantwoordelijkheid dragen en proactief acteren binnen ons sturingskader.

Verplichte interoperabiliteit en samenwerking

NEO NL accepteert geen silo-gedrag of het afschuiven van verantwoordelijkheden tussen marktpartijen (‘pointing fingers’). Om een geïntegreerde, veilige en beheerbare dienstverlening te garanderen, is naadloze ketensamenwerking een harde contractuele randvoorwaarde. Dit betekent concreet:

- Gezamenlijke procesintegratie: incidenten, wijzigingen (changes) en problemen worden partner- en scope-overstijgend afgehandeld volgens uniforme ITIL-processen.
- Gezamenlijke verbetering: partners dragen bij aan gezamenlijke analyses en verbeterinitiatieven wanneer vraagstukken meerdere diensten of leveranciers raken.

- Open technische interfaces: leveranciers zijn verplicht om interfaces (API's) en monitoringdata open te stellen om end-to-end traceerbaarheid en cybersecurity-monitoring mogelijk te maken.
- Gedeelde operationele verantwoordelijkheid: bij ketenbrede verstoringen acteren leveranciers als één team onder regie van de SIAM-organisatie van NEO NL, waarbij het herstel van de vitale functie altijd prioriteit heeft boven contractuele discussies.
- Voorkomen van vendor lock-in: leverancierssspecifieke technologie mag de overdraagbaarheid van data, integraties en dienstverlening niet onnodig beperken