

NWO Architectuur principes en standaarden

NWO-architectuurprincipes

Architectuurprincipes zijn richtlijnen ten aanzien van het inrichten en onderhouden van de informatievoorziening en de informatiesystemen van NWO. Vanuit de verschillende externe referentiearchitecturen, zoals NORA en HORA, worden al een groot aantal architectuurprincipes aangereikt. In toevoeging daarop hanteert NWO een aantal eigen architectuurprincipes die specifiek zijn voor de omstandigheden en behoeften van NWO. Hierbij kan onderscheid worden gemaakt tussen enerzijds basisprincipes (of algemene principes), die generiek van toepassing zijn op de integrale informatievoorziening, en anderzijds domeinprincipes (of afgeleide principes), die geldig zijn voor specifieke onderdelen (domeinen) daarbinnen.

Basisprincipe

Principe	Titel	Toelichting
NWO-BP01	Architectuur is leidend	NWO kiest voor Werken met Architectuur.
NWO-BP02	afwijkingen	Het principe Comply-or-Explain is onverkort op alle afwijkingen van toepassing.
NWO-BP03	Standaarden	NWO volgt architectuur standaarden (NORA, HORA)
NWO -BP04	Wetgeving	De inrichting van processen en systemen voldoet aan relevante Europese en Nederlandse wet- en regelgeving.
NWO -BP05	Flexibiliteit en wendbaarheid	De inrichting van processen en systemen binnen NWO houdt rekening met de flexibiliteit en wendbaarheid die de strategie van NWO, alsmede de buitenwereld van NWO vraagt.
NWO -BP06	Maatschappelijke functie	De inrichting van processen en systemen binnen NWO houdt er rekening mee dat wij een maatschappelijke functie hebben die wordt uitgevoerd met gemeenschapsgeld.
NWO -BP07	complexiteit	NWO streeft naar vermindering van de complexiteit van de processen en ICT-omgeving, met behoud van betrouwbaarheid, integriteit en vertrouwelijkheid.
NWO -BP08	Generiek	Generieke diensten/systemen, die gebruikt kunnen worden voor de gehele organisatie, hebben de voorkeur
NWO -BP09	doel	Financieren en Verbinden staat centraal.

		Dit zijn de kerntaken van NWO en alle activiteiten van NWO dienen in dienst te staan van deze kerntaken.
NWO-BP10	Informatie gedreven	NWO werkt informatie gedreven. Informatie en de onderliggende data is een essentiële NWO-bedrijfsfunctie. Afgeleide principes zoals, Archiving by design, informatie is betrouwbaar en alle data principes zijn gedefinieerd omdat een goede informatiehuishouding essentieel is voor NWO.

Informatie Principes

Principe	titel	Toelichting
NWO-IP1	Open Informatie	NWO werkt vanuit de gedachte: “open tenzij”, waarbij we transparant zijn over onze resultaten, processen en data. We werken daarbij samen met ketenpartners en delen onze data proactief, uiteraard binnen geldende kaders.([15], Pagina 62, proces en ketengericht samenwerken).
NWO-IP2	Informatie is Betrouwbaar en FAIR	Informatie dient betrouwbaar, vindbaar, toegankelijk, interoperabel en hergebruikt kunnen worden. Informatie is cruciaal voor NWO en dit is in lijn met “NWO werkt informatiegedreven” principe.
NWO-IP3	Archiving by Design	Archivering is door wetgeving een verplicht onderdeel. Dit wordt verder uitgewerkt in §5.10.
NWO-IP4	Privacy by Design	Privacy by Design is een proactieve benadering van de bescherming van persoonsgegevens via technische, organisatorische en juridische maatregelen. Het betekent dat de organisaties de privacycriteria meewegen en, waar mogelijk, meenemen in het ontwikkelen van verwerkingen, producten en systemen. Privacy by Design bepaalt dat gegevensbescherming geïntegreerd moet worden in het creëren en beheren van nieuwe verwerkingen, producten, diensten, IT-systemen, IT-architectuur, apparatuur, beleid en protocollen. [17]
NWO-IP5	Security by Design en default	Onveilige technologie en kwetsbaarheden in kritieke systemen kunnen kwaadaardige cyberinbraken uitnodigen, wat leidt tot ernstige potentiële risico's voor NWO. Het is nu meer dan ooit

		cruciaal om Secure-by-Design en Secure-by-Default tot speerpunten te maken van alle productontwerp- en ontwikkelingsprocessen. [12]
--	--	---

Applicatie Principles

principe	titel	Toelichting
NWO-AP01	kanaal onafhankelijk resultaat	Dit betekent dat op elke type device of via de in gebruik zijnde browsers dezelfde informatie wordt getoond. Dit betekent niet dat via het ene kanaal meer of minder informatie getoond of aangepast kan worden, maar wel dat wat er beschikbaar wordt gesteld dezelfde informatie is als dat je verkrijgt via andere kanalen. We maken onderscheid in het device waarmee de NWO-persona zichzelf toegang verschaft afhankelijk van de classificatie van de applicatie en de data.
NWO-AP02	Voorkom onnodige complexiteit	Vele hier gedefinieerde principes hebben tot doel om het IT landschap te vereenvoudigen. IT Architectuur is de strijd tegen complexiteit. Niet alleen voorkomen dat het ontstaat, maar ook rationaliseren als het toch is ontstaan, bijvoorbeeld door nieuwe overlappende functionaliteit geboden in (evergreen) SaaS applicaties. Het vereenvoudigen van het applicatielandschap leidt tot minder kosten en ook een uniformere werkwijze. Dit principe is ook gedefinieerd door de NORA onder NAP16
NWO-AP03	Bewaak de Levenscyclus-	Er dient regelmatig proactief geëvalueerd te worden of de applicaties hun doel voldoende dienen, door het uitvoeren van een Deming-cirkel (Plan-Do-Check-Act). Ook informatie en data verouderen en dienen op een gegeven moment te worden gearhiveerd of te worden vernietigd. Deze levenscyclussen zullen voor de verschillende use cases moeten worden gedefinieerd en opgevolgd. Dit principe is benodigd om te kunnen voldoen aan wetgeving en het applicatielandschap up to date te houden. Dit principe is ook gedefinieerd door de NORA onder NAP17.
NWO-AP04	Microsoft tenzij:	NWO heeft gekozen voor een Microsoft tenzij beleid. Dit betekent dat voor ieder te selecteren functionaliteit er gekeken dient te worden of Microsoft een geschikte applicatie/ oplossing (fit for purpose) heeft die deze functionaliteit biedt. Als een alternatieve applicatie/oplossing wordt geprefereerd boven de Microsoftoplossing dient er, in het High Level Design, te worden onderbouwd waarom deze oplossing wordt geadviseerd en hoe de business case voor deze keuze uitvalt. In de toekomst, wanneer de rationale voor deze keuze wegvalt (bijv. door een nieuwe functionaliteit in een Microsoft product), kan deze keuze heroverwogen worden (met een nieuwe business case) en alsnog een

		migratie naar een Microsoftproduct worden ingezet, wat past in de best of suite strategie van NWO. De rationale achter het Microsoft tenzij principe is een vereenvoudiging van het Applicatielandschap en beperktere kennisopbouw nodig van de IT organisatie.
NWO-AP05	Bouw Diensten Modulair op	Maak bij de ontwikkeling van diensten gebruik van een modulaire indeling met een maximale interne samenhang en minimale externe koppelingen. Door diensten modulair op te bouwen en te ontkoppelen wordt de flexibiliteit vergroot, wat leidt tot meer wendbaarheid, meer hergebruik en duurzaamheid. Dit principe is ook gedefinieerd door de NORA onder NAP07.
NWO-AP06	Bundel Diensten	De integratie van deze services wordt continu verbeterd (leider in de markt) en er worden applicaties aan de service suite toegevoegd. Door het evergreen principe worden de applicaties in de suite continu verbeterd en worden functionaliteiten toegevoegd. Een nadeel kan zijn dat ook functionaliteiten worden uitgefaseerd, waarvoor dan een alternatief gezocht dient te worden. De IT organisatie dient zichzelf op de hoogte te houden van deze veranderingen en daarop te anticiperen. Daarnaast ontslaat dit principe de organisatie er niet van om de geleverde services en de bijbehorende kosten goed te overwegen, aangezien alternatieve services beter fit-for-purpose kunnen zijn en dus een lagere TCO kunnen hebben. Dit is verder uitgewerkt in het Microsoft tenzij en Surf tenzij constraint. Bundel diensten betekent ook dat als er een vraag is vanuit de business voor een bepaalde functionaliteit er ook eerst gekeken wordt of deze functionaliteit kan worden geleverd vanuit een bestaande diensten bundel, i.p.v. het zoeken naar een nieuwe punt oplossing/applicatie. Een goed voorbeeld van een gebundelde dienst is Microsoft 365. Maak zoveel mogelijk gebruik van de services in het M365 platform. (Best of Suite in plaats van best of Breed). De reden voor dit principe zijn dat het gebruik van gebundelde diensten het beheer vereenvoudigd en er minder kennis nodig is. Daarnaast is integratie beter op orde, wat het aantal benodigde (zelf beheerde of maatwerk) integraties verlaagd.
NWO-AP07	Hergebruik , vóór kopen, voor maken	Microsoftapplicaties, en door NWO geselecteerde pakketten van andere leveranciers, hebben veel standaard functionaliteiten die kunnen worden toegepast en hergebruikt om vele primaire en secundaire processen te faciliteren. Deze SaaS applicaties kunnen worden aangepast door configuratie. Daarnaast bieden vele SaaS applicaties add-ons vanuit een app-store die ingezet kunnen worden. Er wordt pas over gegaan op maatwerk (via SDKs en APIs) als er een duidelijke business case gemaakt kan worden en er dus significante

		tijd/geld winst te behalen is. Maatwerk kan bestaan uit low code (bijvoorbeeld power platform) of pro code (zoals C#/Python code of Python/Powershell scripts), afhankelijk van de benodigde toepassing. Het standaard tenzij principe wordt vooral gevolgt om de kosten en complexiteit van het IT landschap laag te houden. Vooral het beheer van maatwerk is duur en vaak is het lastig de kennis van een maatwerk applicatie vast te houden als er weinig doorontwikkeling is aan de applicatie. Het gevolg is dat kleine aanpassingen en het veilig houden (regulier beheer) in een late fase van de life cycle van de applicatie erg duur worden. Het is dus essentieel om in de business case de beheer kosten over de gehele levens cyclus van de applicatie mee te nemen. §5.8 gaat verder in op maatwerk.
--	--	---

Data Principles

Principe	titel	Toelichting
NWO-DP01	Data bij de Bron	Binnen NWO wordt er zo min mogelijk informatie gesynchroniseerd tussen systemen, om het applicatielandschap eenvoudig te houden. Als deze informatie in andere systemen benodigd is dan kan deze via een (bij voorkeur REST of SOAP) API opgehaald worden. Van elk systeem dient helder beschreven te zijn voor welke bron data dit systeem verantwoordelijk is en van welke data uit andere systemen het afhankelijk is.
NWO-DP02	Data is uniform geclassificeerd	Daar tegenover staat dat dat vertrouwelijk geclassificeerde data moet worden beschermd, aangezien we inconsistentie en lekken van vertrouwelijke informatie willen voorkomen. Hiervoor gebruiken we conditional access (zie § 7.5).
NWO-DP03	Data heeft altijd één eigenaar	Het dient helder te zijn wie er eigenaar is van gegevens en daarmee verantwoordelijk voor de kwaliteit en de bijbehorende informatie principes.
NWO-DP04	Data wordt indien nodig, zo lang als nodig bewaard	Dit principe sluit aan bij het informatie principe “Archiving by design”
NWO-DP05	Data terminologie en modellen zijn gestandaardiseerd	Door heldere modellering en terminologie wordt er onduidelijkheid en dubbelzinnigheid voorkomen, waardoor de complexiteit van de data afneemt.
NWO-DP06	NWO data is overzichtelijk, inzichtelijk en correct	Dit principe sluit aan bij het informatie principe “Informatie is Betrouwbaar en FAIR”.

NWO-DP07	Gestructureer de data prevaleert boven ongestructureerd	NWO gebruikt momenteel veel ongestructureerde data waardoor de informatie in deze data lastig is te extraheren. Het bij de bron gestructureerd opslaan zal de vertalingsslag naar informatie vereenvoudigen
NWO-DP08	Data wordt gedurende zijn hele levenscyclus beheerd en beschermd	Datagebruik op basis van role based access (RBAC) met per rol bijbehorende rechten op basis van CRUD (create-read-update-delete) • Data, proces en parameter onafhankelijk opslaan • Indien van toepassing: mutaties op data worden op attribuutniveau vastgelegd met bijbehorende time/user-stamp / historie • Er wordt gebruik gemaakt van conditional access (zie § 7.5).

Technologie Principles

Principe	titel	Toelichting
NWO-TP01	SSO	Alle applicaties van NWO zullen worden voorzien van Single Sign On via het IAM-platform, tenzij dit technisch niet mogelijk is. De rationale achter dit principe is dat NWO controle wil houden over de Identiteiten en authenticatie centraal wil laten afhandelen. Daarnaast zorgt SSO voor een betere gebruikersbeleving en minder kans op lekken van wachtwoorden. Daarnaast kan er zo gebruik gemaakt worden van de conditional access mogelijkheden van IAM.
NWO-TP02	Cloud tenzij	Dit betekent dat NWO primair zoekt naar cloud oplossingen om hun interne processen te ondersteunen. Als er applicaties zijn die nog niet "end-of-life" zijn en on-premise worden gehost, dan zullen deze applicaties meegenomen worden in het op te starten cloud migratieproject. End-of-life applicaties zullen worden decommissioned. De belangrijkste reden voor het cloud tenzij principe is dat de security beter gewaarborgt kan worden in de cloud.
NWO-TP03	SaaS voor Paas voor IaaS:	Bij SaaS oplossingen kan NWO de verantwoordelijkheden van het beheer van applicaties overdragen aan een derde partij. . Deze SaaS applicaties kunnen worden aangepast door configuratie. Daarnaast bieden vele SaaS applicaties add-ons vanuit een app-store die ingezet kunnen worden. Als SaaS niet voldoet dan kan gekozen worden voor PaaS en dat impliceert maatwerk, met de benodigde kennis. IaaS kan alleen gekozen worden voor Legacy Oplossingen die niet eenvoudig gemigreerd kunnen worden naar Cloud Native oplossingen. De rationale achter dit principe is dat NWO zich richt op regie voering en niet op het opbouwen van technische (security) kennis. Ook vereisen de requirements van NWO geen complex IT applicatielandschap.
NWO-TP04	Standaard Tenzij	Oplossing moeten voldoen aan de open standaarden zoals gedefinieerd in [E11], de 'Pas toe of leg uit'-standaarden. Het is nuttig om ook de Aanbevolen standaarden te volgen.

		Ook wordt vaak Open Source genoemd als standaard. Vaak is de maturity van open source oplossingen bij standaard software zoals bijvoorbeeld office software inferieur aan de closed source oplossingen zoals Microsoft Office 365. Het opbouwen van een IT landschap op open source oplossingen is momenteel nog onvoldoende en dient uitgebreid te worden met closed source producten van leveranciers. Ook zie je vaak dat er maar een deel van een oplossing als open source wordt aangeboden en dat de grootste “Added Value” komt van een closed source leverancier, waardoor er toch Vendor Lock-in ontstaat. Vendor-Lockin is niet te voorkomen, maar er dient wel goed onderzocht/overwogen te worden of het aantal vendors geminimaliseerd kan worden en wat de betrouwbaarheid/reputatie is van deze Vendor.
--	--	---