Bijlage E – Beschrijving dienstverlening IT-beheer 2025

Inhoud

INHOUD 1

1. INLEIDING 2
1.1. Samenvatting 2
1.2. Opbouw document 2

2. UITGANGSPUNTEN EN CONTEXT VOOR DE DIENSTVERLENING 3
2.1. Doelen van hWh 3
2.2. Cloud first / Microsoft 4
2.3. Werkplekken, gebruikers 4
2.4. Hostingplatform 4
2.5. Regierol van Opdrachtgever 4

3. IT-OMGEVING 6
3.1. Digitale werkomgeving 6
3.2. Overzicht van IT-apparatuur 6
3.3. Microsoft Dynamics 365 6
3.4. Microsoft Power Platform 6
3.5. Primaire applicaties 6
3.6. Infrastructuur 7
3.7. Hostingplatform 8

4. DIENSTVERLENING 9
4.1. Digitale werkplek 9
4.2. Critical Friend 9
4.3. SPOC 9
4.4. Informatieveiligheid 10
4.4.1. Informatieveiligheid en de relatie met derde dienstverlenende partijen 10
4.5. Transitiefase 12
4.6. De dienstverlening 12
4.6.1. Responsetijden prioriteitsbepaling incidenten 15
4.6.2. Security 16
4.6.3. Technisch beheer hostingplatform 17
4.7. Niet-standaard wijzigingen 18
4.7.1. IAM oplossing 18
4.8. Governance 19

1. Inleiding

Dit document beschrijft nadere voorwaarden waaraan de door de Opdrachtnemer te leveren Prestatie IT-beheer dient te voldoen.

Dit document maakt onderdeel uit van de aanbesteding met TenderNed-kenmerk 515769.

Andere eisen die aan de uitvoering van de Overeenkomst worden gesteld, staan vermeld in de in artikel 2.2 van de Overeenkomst IT-beheer 2025 genoemde documenten.

1.1. Samenvatting

De Opdracht omvat het IT-beheer van de gehele IT-omgeving, exclusief eerstelijns ondersteuning en eerstelijns functioneel beheer. Opdrachtnemer dient in nauwe samenwerking met Opdrachtgever (hierna ook: hWh) een solide up-to-date IT-omgeving te beheren en door te ontwikkelen.

Daarbij is het van belang dat Opdrachtgever een voorlopers rol heeft binnen de sector waar in hWh kan aantonen dat nieuwe technologieën werken en hoe deze de sector kunnen ondersteunen. De Opdrachtnemer ondersteunt hierin door bij te dragen aan de voorlopers rol van de Opdrachtgever binnen de sector. Dit houdt in dat nieuwe technologieën in samenwerking kunnen worden getest, gevalideerd en toegepast in de IT-omgeving.

De IT-omgeving van hWh bestaat globaal uit twee delen. Enerzijds is er kantoorautomatisering voor de reguliere gebruikers van hWh en anderzijds een deel dat de programma's en projecten die hWh voor de waterschappen uitvoert en faciliteert.

De gebruiker van de IT-omgeving dient te beschikken over een vlekkeloos werkende IT-omgeving waarbij deze geen belemmeringen ondervindt bij het uitvoeren van zijn werkzaamheden.

Opdrachtgever werkt hybride. Dit betekent dat gebruikers werken op de plek en het moment die het beste bij het werk past. Dit kan op kantoor, thuis of elders zijn.

De Opdrachtgever is aangesloten bij het CERT-WM en heeft een contract met een SOC-dienstverlener (Thales) en een dienstverlener voor DFIR (Secura).

1.2. Opbouw document

In hoofdstuk 2 worden de hWh context en de uitgangspunten voor de dienstverlening beschreven.

Hoofdstuk 3 gaat in op de huidige IT-omgeving van hWh en bevat een beschrijving van de hard- en software en de bijbehorende diensten.

In hoofdstuk 4 wordt nader ingegaan op de te leveren diensten.

2. Uitgangspunten en context voor de dienstverlening

2.1. Doelen van hWh

hWh streeft de volgende doelstellingen na:

Betrouwbaar

- Het realiseren van een solide IT-omgeving en professionele IT-beheerorganisatie die ervoor zorgt dat de IT-omgeving beschikbaar is en blijft, om daarmee de eigen organisatie en de programma's en projecten die hWh voor de waterschappen uitvoert, te faciliteren.
- Het borgen van kwaliteit door aan te sturen op kwalitatief optimale dienstverlening op basis van prestatie-indicatoren zoals reactietijden, oplostijden, klanttevredenheid en leverbetrouwbaarheid.

Veilig

- hWh heeft zich, samen met alle andere Nederlandse overheidsorganisaties, gecommitteerd aan de Baseline Informatiebeveiliging voor Overheden (BIO). Het borgen van de informatieveiligheid is een belangrijke randvoorwaarde bij alle activiteiten van hWh.
- De ambitie van hWh is om het volwassenheidsniveau 4 van 5 te behalen met daarbij als kader de BIO en de Algemene Verordening Gegevensbescherming (AVG). Dit vraagt om risico-gestuurd te denken en te werken en vergt nauwe samenwerking met het interne team Informatieveiligheid (IV) en Privacy (P). Het interne IV&P team stelt daarbij de kaders op waarbinnen gewerkt wordt en helpt met het implementeren van deze kaders binnen de hWh IT-omgeving.

Innovatief

- hWh streeft naar een voorlopers rol binnen de sector op IT-gebied, waarbij zij kan aantonen dat nieuwe technologieën werken en hoe deze de sector kunnen ondersteunen.
- Het vooroplopen door het adopteren van vernieuwingen en tijdige updates op Microsoft-applicaties als *early adopter*.

Flexibiliteit

- Naar verwachting nemen de IT-diensten die hWh levert aan de waterschappen de komende jaren in aantal en omvang toe. De IT-beheerorganisatie dient snel en adequaat te reageren op verzoeken tot uitbreiding van de IT-omgeving vanuit de eigen organisatie en de project en beheer-activiteiten van hWh. Dit vraagt om een gebruiksvriendelijk, toekomstbestendig en efficiënt ingericht hostingplatform, waarop onder regie van hWh ook diensten kunnen worden aangeboden door een derde* partij. Een toekomstige uitbreiding naar gelieerde organisaties zoals de Unie van Waterschappen of Stowa behoort tot de mogelijkheden.

**Onder derde wordt verstaan een leverancier die een tool of software voor gebruikers (waterschappen en/of hWh) heeft gemaakt (in opdracht van hWh) die op het platform van hWh wordt gehost.*

2.2. Cloud first / Microsoft

Opdrachtgever hanteert een cloud-first strategie waarbij Microsoft de standaard is, tenzij er een specifieke reden is om voor een andere oplossing te kiezen. De IT-omgeving is volledig cloud-based en bestaat uit tenants met Microsoft 365 en Microsoft Azure, voor Microsoft 365 gebaseerd op het E5 licentiemodel. In Microsoft Azure zijn er meerdere subscriptions (abonnementen) voor de instandhouding, projecten en programma's van de Opdrachtgever. Opdrachtgever heeft bij Microsoft meerjarig Unified support afgesloten voor de gehele IT-omgeving.

2.3. Werkplekken, gebruikers

Onder een werkplek wordt verstaan elke gebruiker binnen de IT-omgeving van hWh met een door hWh geleverde Microsoft E5-licentie. Bij de Opdrachtgever werken momenteel circa 230 mensen. Dit aantal varieert en is onder te verdelen in drie groepen: medewerkers in vaste dienst, ingeleende medewerkers (vanuit de Watersector) en ingehuurde mensen. Medewerkers in vaste dienst krijgen een laptop en een smartphone in bruikleen van de Opdrachtgever. Voor ingeleende medewerkers en ingehuurde mensen wordt bepaald of zij een laptop of smartphone in bruikleen krijgen. Als dit niet het geval is, maken zij gebruik van hun eigen apparatuur. Op beperkte schaal wordt gebruik gemaakt van Microsoft CloudPC, waar dit vanuit veiligheidsoogpunt nodig is.

De dagelijkse, directe operationele communicatie met de interne medewerkers wordt uitgevoerd door de beheerders van de Opdrachtgever en valt in de regel buiten de activiteiten van de Opdrachtnemer. Een voorbeeld hiervan is het daadwerkelijk gereedmaken, installeren en uitreiken van apparatuur.

2.4. Hostingplatform

De IT-omgeving wordt niet alleen gebruikt voor de basisvoorzieningen en interne diensten voor hWh. Een deel van de project- en beheeractiviteiten die Opdrachtgever voor de waterschappen laat uitvoeren, maakt ook gebruik van de IT-omgeving. Het geheel wordt hierna ook aangeduid als hostingplatform. Het gaat hierbij om aparte Azure subscriptions die door Opdrachtgever beschikbaar worden gesteld aan een derde partij om daarmee producten of diensten te leveren aan de waterschappen. Opdrachtnemer is ook verantwoordelijk voor het technisch beheer van deze subscriptions. De verwachting is dat dit onderdeel van de IT-omgeving de komende jaren gaat groeien. Opdrachtnemer dient gevraagd en ongevraagd advies uit te brengen over dit soort uitbreidingen. Opdrachtnemer dient desgevraagd op basis van een nadere Opdracht de uitbreiding te realiseren. Opdrachtnemer dient een uitbreiding van het hostingplatform eveneens te beheren.

2.5. Regierol van Opdrachtgever

Een belangrijke voorwaarde binnen deze samenwerking is dat alle activiteiten worden uitgevoerd onder de regie van de Opdrachtgever. Daar ligt enerzijds aan ten grondslag dat Opdrachtgever grip wil behouden op de IT-omgeving. Anderzijds ligt daaraan ten grondslag dat Opdrachtgever zelf alle hardware en software verwerft, waardoor het "eigenaarschap" ervan bij Opdrachtgever ligt. Deze opzet creëert een onderlinge afhankelijkheid tussen Opdrachtnemer en Opdrachtgever, waarbij beide partijen verantwoordelijkheid dragen voor een optimale dienstverlening en een zo

hoog mogelijke beschikbaarheid. Opdrachtgever zorgt ook voor de aanschaf en aanleg van passieve apparatuur (fysieke bekabeling, aansluitingen). Opdrachtnemer draagt zorg dat voor de aansluiting van de passieve apparatuur op de actieve apparatuur.

3. IT-Omgeving

Het Waterschapshuis heeft een uitgebreide digitale werkomgeving die de medewerkers en andere gebruikers van de werkomgeving ondersteunt in hun dagelijkse werkzaamheden. Voor de gehele IT-omgeving geldt dat de inrichting wordt bepaald door Opdrachtgever.

3.1. Digitale werkomgeving

De digitale werkomgeving bij het Waterschapshuis is volledig gebaseerd op technologie van Microsoft en bestaat hoofdzakelijk uit Microsoft 365 (Microsoft Office, Exchange Online, SharePoint Online, Microsoft Teams, One-drive, Sentinel, Defender, XDR, Purview).

Entra ID: Microsoft Entra ID wordt gebruikt als centrale plek om gebruikersaccounts te beheren.

Device Management: Voor het beheer van de apparaten maakt het Waterschapshuis gebruik van een volledig ingerichte omgeving met de volgende componenten:

- Mobile Device Management (MDM);
- Microsoft Intune;
- Windows Autopilot.

Windows 11: de laptops van het Waterschapshuis zijn voorzien van Microsoft Windows 11 Enterprise.

3.2. Overzicht van IT-apparatuur

Soort	Aantal	Toelichting
Laptops	111	De huidige standaard is HP
SmartPhones	80	De huidige standaard is Apple iPhone
Tablets	5	De huidige standaard is Apple iPad
CloudPC	6	Virtuele werkplek
TeamsRoom PC	6	Aansturing van de Teams omgeving van de vergaderruimtes
Printers	2	Aansturing via Printix software

Tabel 3.2: overzicht IT-apparatuur.

3.3. Microsoft Dynamics 365

Microsoft Dynamics CRM wordt binnen het Waterschapshuis op kleine schaal (circa 10 gebruikers) gebruikt.

3.4. Microsoft Power Platform

Het platform wordt op dit moment voornamelijk gebruikt voor Power BI rapportages.

3.5. Primaire applicaties

Applicatie	Toelichting
AvePoint Back-up	Cloud back-up
Azure Back-up	Cloud back-up
Govroam	Wifi-roaming

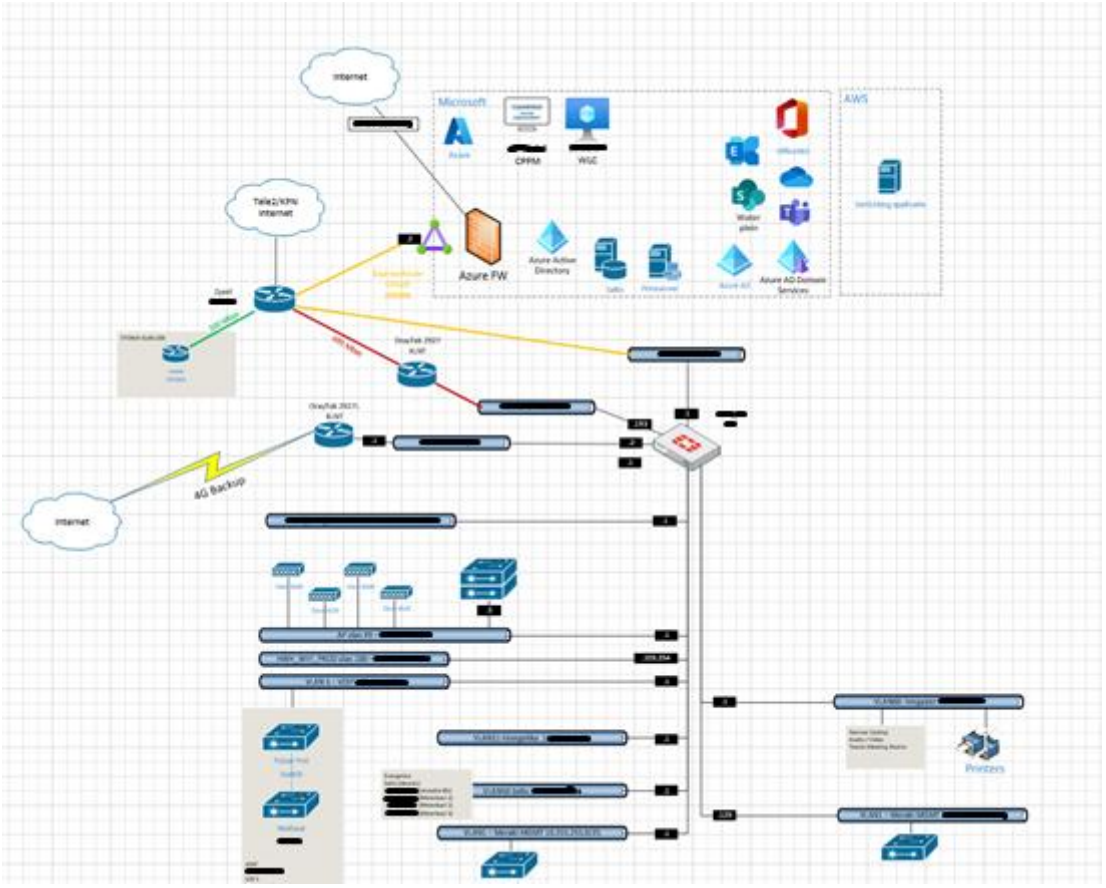
JOIN	Document management
Prosa	ERP
TOPdesk	Service management
Printix	Print software
Smartlockr	Veilig mailen
Roommanager	Ruimte reservering systeem
Salto KS	Gebouw toegangsbeveiliging
Tracco	Controle normeringen en richtlijnen

Tabel 3.5: Primaire applicaties

3.6. Infrastructuur

De kantoorlocatie (Amersfoort) is ingericht volgens het concept van activiteit-gebaseerd werken en biedt plaats aan 70 flexibele werkplekken, 4 vergaderruimtes, 3 belcellen en 4 focusruimtes. Daarnaast is er een ontmoetingscentrum met 15 vergaderzalen voor de watersector. Alle vergaderzalen zijn voorzien van een roomdisplay. Het netwerk op de locatie in Amersfoort is gebaseerd op WLAN-technologie en biedt een koppeling naar zowel het internet als de Microsoft Cloud.

De infrastructuur op de kantoorlocatie bestaat in essentie uit een firewall, 2 routers, 6 Cisco switches, 32 WiFi Access Points een GovRoam koppeling met een ClearPass Server.



Figuur 3.6: Indicatie van de netwerkarchitectuur

3.7. Hostingplatform

Zoals in paragraaf 2.4 aangegeven streeft hWh naar het realiseren en beheren van een gebruiksvriendelijk, toekomstbestendig en efficiënt ingericht hostingplatform. Op dit hostingplatform kunnen tevens onder regie van hWh diensten aan de waterschappen en gelieerde organisaties worden aangeboden door een derde[1]. Hierbij wordt ook rekening gehouden met de organisatie en rollen van hWh in relatie tot het platform en de diensten van Opdrachtnemer: dit is een groeipad.

De diensten die onder regie van hWh op het hostingplatform door derden kunnen worden aangeboden worden beheerd door:

1. hWh of de derde die diensten aanbiedt: in dat geval dient Opdrachtnemer het beheer door de derde partij te faciliteren;

2. Opdrachtnemer in alle andere gevallen.

De diensten zijn ondergebracht in één Azure tenant met daarin de volgende subscriptions:

Basisvoorzieningen:
- **hWh Connectivity:** netwerkomgeving met firewalls;
- **hWh Security:** omgeving met Defender, Sentinel, etc.;

Diensten voor de interne hWh Organisatie:
- **hWh KA:** subscriptie met toepassingen voor de interne hWh organisatie, zoals SALTO, printserver, etc.;

Diensten in het kader van project- en beheeractiviteiten voor waterschappen:
- **hWh NL Veranderdetectie:** subscriptie waarin een aantal waterschappen de tool veranderdetectie ontwikkelen en draaien;
- **hWh Musktrap:** dataplatform ingericht onder regie van HDSR (door C-motion) met data uit ESRI ten behoeve van PowerBI rapportages;
- **hWh Datastromen:** subscriptie voor het programma Datastromen om een website met kwaliteit van aanleveringen;
- **hWh Beeldmateriaal:** subscriptie voor het programma AHN & Beeldmateriaal voor dataopslag;
- **hWh NHI:** subscriptie voor het 'Nederlands Hydrologisch Instrumentarium' met storagecontainer voor downloads;
- **hWh Softwarecatalogus:** subscriptie waarbinnen de softwarecatalogus wordt gerealiseerd met behulp van Powerapps;
- **hWh Riool Vreemd Water:** subscriptie voor dashboarding over waterzuiveringen.

[1] Onder derde wordt verstaan een leverancier die een tool of software voor gebruikers (waterschappen en/of hWh) heeft gemaakt (in opdracht van hWh) die op het platform van hWh wordt gehost.

De maandelijkse Microsoft kosten voor het gebruik van Azure bedragen momenteel ongeveer €10.000 Euro. Deze kosten omvatten verschillende diensten zoals virtuele machines, opslag, databases en netwerkverkeer.

4. Dienstverlening

4.1. Digitale werkplek

De digitale moderne werkplek voor de medewerkers en overige gebruikers van hWh dient te voldoen aan de volgende eisen:

- De digitale moderne werkplek moet intuïtief en gebruiksvriendelijk zijn, zodat medewerkers en overige gebruikers gemakkelijk toegang hebben tot de benodigde applicaties, tools en informatie;
- De digitale moderne werkplek faciliteert en stimuleert medewerkers en overige gebruikers om op een veilige manier samen te creëren en te communiceren;
- Gebruikerservaring: De digitale moderne werkplek stelt de gebruiker en de omgeving centraal en zorgt ervoor dat het werk goed wordt ondersteund onder andere doordat de gebruiker geen merkbare vertraging ervaart;
- Beheer en inrichting: De digitale werkplek wordt beheerd door de Opdrachtnemer;
- Opdrachtnemer zorgt voor testscenario's en dat de werkplek technisch en functioneel is getest voordat deze in productie gaat;
- Het voorbereidings- en uitrol proces is zo efficiënt mogelijk en voorziet in een werkplek die gebruiksklaar kan worden uitgegeven door 1e lijns IT Beheer van Opdrachtgever.

4.2. Critical Friend

Een critical friend is een IT-expert die op een constructieve en kritische wijze feedback geeft op strategieën, architectuur, processen en projecten, en vanuit een objectief perspectief, "best for hWh", behulpzaam adviseert over de IT-omgeving van hWh en wijzigingen daarin en over tools en oplossingen die hWh voor de waterschappen beheert. Opdrachtnemer treedt actief op als critical friend. Als critical friend biedt Opdrachtnemer een onafhankelijk perspectief, stelt Opdrachtnemer kritische vragen en levert Opdrachtnemer eerlijke, goed onderbouwde inzichten. Als critical friend heeft Opdrachtnemer een actieve rol bij het evalueren en optimaliseren van de inrichting en het adviseren over de marktconforme en kostenefficiënte beheerprocessen, diensten en services.

Opdrachtgever kan zonder specifieke aanleiding gebruikmaken van de vraagbaakfunctie van de Opdrachtnemer. Dit betreft onder ander ook vraagstukken rond doorontwikkeling en inrichtingsvraagstukken waarbij snelle afstemming gewenst is, zodat medewerkers van de Opdrachtgever efficiënt verder kunnen werken en doorlooptijden worden verkort. Deze afstemmingsmomenten zijn vaak kort en praktisch van aard, met een duur van doorgaans circa een uur. In sommige gevallen kunnen ze uitmonden in grotere projecten.

4.3. SPOC

Opdrachtnemer heeft een single-point-of-contact (SPOC) rol voor het schakelen met leveranciers, bijvoorbeeld in het kader van het oplossen van incidenten en voor de beheer- en monitoringsactiviteiten. In deze gevallen acteert Opdrachtnemer als regisseur voor:

- het oplossen van de issues;

- Het uitvoeren van wijzigingen met betrekking tot gedane meldingen en
- het operationeel aansturen van derde partijen waarmee Opdrachtgever reeds contracten heeft en die raakvlakken hebben met of onderdeel zijn van de IT-omgeving, waaronder SaaS- en netwerkleveranciers, SOC-leveranciers en Microsoft.

Let op: Opdrachtgever is in de regel SPOC voor interne communicatie richting de medewerkers.

4.4. Informatieveiligheid

Het Waterschapshuis heeft zich, samen met alle andere Nederlandse overheidsorganisaties, gecommitteerd aan de BIO (Baseline Informatiebeveiliging voor Overheden).

HWh is daarom actief bezig om de BIO volledig risico gestuurd te implementeren en te borgen in een continu proces (PDCA-cyclus). Opdrachtnemer dient hWh volledig en op alle relevante aspecten van informatieveiligheid te ondersteunen en met hWh samen te werken.

Een Information Security Management System (ISMS) is een verzameling van activiteiten, processen en documenten die nodig is om informatiebeveiliging op een systematische manier te managen. Het ISMS helpt bij het managen van informatiebeveiliging doordat kaders, richtlijnen en afspraken op een structurele en effectieve manier worden vastgelegd. Het zorgt ervoor dat de eisen ten aanzien van vertrouwelijkheid, integriteit en beschikbaarheid van bedrijfsprocessen, informatie en informatiesystemen beter aansluiten op managementverwachtingen en bedrijfseisen. Het ISMS zorgt voor focus in het managen van informatiebeveiliging, wat het identificeren en beheersen van risico's makkelijker maakt. Een werkend ISMS is voor hWh verplicht met de komst van de nieuwe BIO2. Samen met de Opdrachtnemer moet hWh voortdurend kunnen aantonen dat, voor de scope van de geleverde dienstverlening, er voldaan wordt de IT-omgeving voldoet aan de BIO(2). Op het gebied van andere relevante (en toekomstige) wet- en regelgeving verwacht hWh een actieve houding van Opdrachtnemer. Samenwerking is hierin cruciaal.

Informatiebeveiliging in de breedste zin is een gezamenlijke verantwoordelijkheid, waarbij de Opdrachtnemer proactief de staat van informatiebeveiliging en risico gestuurd implementeert, monitort en blijft werken aan verbeteringen (PDCA-cyclus).

HWh streeft naar zero-trust architectuur op basis van het Need-to-Know principe.

4.4.1. Informatieveiligheid en de relatie met derde dienstverlenende partijen

In het kader van de informatieveiligheid is het Waterschapshuis cruciale samenwerkingsverbanden aangegaan met derde dienstverlenende partijen. Deze samenwerking stelt hWh in staat te profiteren van gespecialiseerde kennis en expertise, waardoor hWh de informatieveiligheid zo optimaal mogelijk kan waarborgen. Het is een vereiste dat de Opdrachtnemer hierin actief meewerkt.

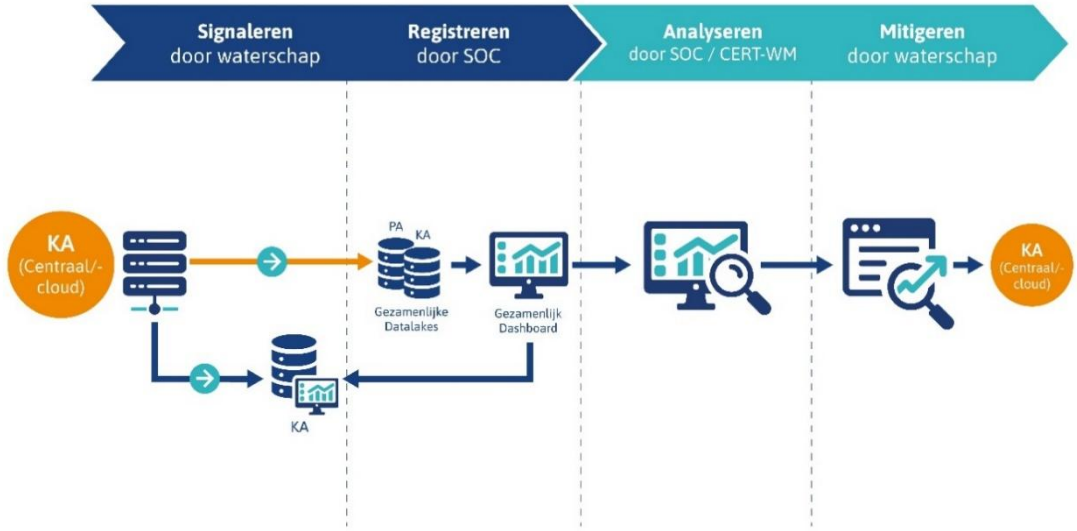
SOC

Het Waterschapshuis is een overeenkomst aangegaan met een SOC-dienstverlener en staat aan het begin van de implementatiefase. Het aansluiten hierop zal naar verwachting aan het begin van Q4 2025 zijn afgerond.

De Opdrachtgever beheert en onderhoudt de IT-omgeving conform de aansluitvoorwaarden van de afgenomen SOC-dienstverlening. Onderdelen hiervan zijn "monitoring en logging", de SIEM-

omgeving, het beschikbaar stellen van de data aan de SOC-dienstverlener en het reageren op incidenten door het nemen van mitigerende maatregelen.

Onderstaande figuur geeft de routing van een beveiligingsincident weer. Opdrachtnemer dient de onderdelen "Signaleren" en "Mitigeren" te beheren en uit te voeren.



Figuur 4.4.1.1: routing beveiligingsincidenten: waar waterschap staat dient u Opdrachtnemer te lezen.

CERT-WM
Het CERT-WM (Computer Emergency Response Team voor WaterManagement) biedt operationele informatiebeveiligingsdiensten aan organisaties in de watersector. Ze verstrekken advisories, monitoren het gebruik van open standaarden, behandelen kwetsbaarheidsmeldingen, en ondersteunen bij cyberincidenten. Daarnaast voeren ze vulnerability scans, penetratietests en forensisch onderzoek uit, en voorzien ze de achterban van relevante informatie en adviezen.

Opdrachtnemer dient samen te werken met CERT-WM en neemt deel in CERT-WM, bijvoorbeeld door het opvolgen en verwerken van adviezen van het CERT-WM, conform de ITIL-processen van Opdrachtgever, en door ondersteuning te bieden bij een penetratietest.

Digital Forensic and Response (DFIR)
Het Waterschapshuis heeft een overeenkomst met Secura voor DFIR (Digital Forensics and Incident Response). De Opdrachtnemer is voorbereid op en ondersteunt bij een cyberincident of een beveiligingsinbreuk, opdat Secura onderstaande zaken kan uitvoeren binnen de gestelde kaders:

- **Digital Forensics:** Secura verzamelt, analyseert en bewaart digitale bewijsmaterialen om cyberincidenten te onderzoeken en te reconstrueren. Het doel is om de oorzaak van een aanval te achterhalen, de daders te identificeren en bewijsmateriaal te verzamelen dat kan worden gebruikt in juridische procedures.

- **Incident Response:** Secura richt zich op het snel detecteren, reageren op en mitigeren van cyberaanvallen die gaande zijn. Het doel is om de impact van een incident te minimaliseren door snel te handelen, de aanval te stoppen en het systeem te herstellen.

De diensten van Secura omvatten onder andere:

1. **Detectie van een incident:** zodra een cyberaanval wordt gedetecteerd, wordt Secura ingeschakeld om de aard en omvang van het incident te onderzoeken.
2. **Beperking van schade:** tijdens een lopende aanval helpt Secura bij het beperken van de schade door de aanval in te dammen en verdere verspreiding te voorkomen.
3. **Forensisch onderzoek:** na een incident voert Secura een forensisch onderzoek uit om te begrijpen hoe de aanval heeft plaatsgevonden, welke systemen zijn getroffen en welke gegevens mogelijk zijn gestolen.
4. **Herstel en herstelmaatregelen:** Secura helpt bij het herstellen van systemen en het implementeren van maatregelen om toekomstige aanvallen te voorkomen.

4.5. Transitiefase

Na de totstandkoming van de Overeenkomst bespreken Opdrachtgever en Opdrachtnemer het bij inschrijving ingediende Concept transitieplan ter nadere afstemming en invulling ervan. Binnen twee weken na de totstandkoming van de Overeenkomst wordt het afgestemde en nader ingevulde definitief transitieplan ter Acceptatie aan Opdrachtgever aangeboden.

Voor Acceptatie is vereist dat het transitieplan overtuigt dat de transitie binnen drie maanden na ingangsdatum van de "Overeenkomst IT-beheer 2025" adequaat is afgerond en Opdrachtnemer de IT-omgeving van hWh adequaat overeenkomstig de eisen die voortvloeien uit de Overeenkomst in beheer kan nemen.

Op te leveren producten aan einde transitie: o.a. Dossier Afspraken en Procedures (DAP) en SLA van Opdrachtnemer.

Tijdens de transitiefase is Opdrachtnemer minimaal 2 dagen per week fysiek aanwezig op locatie van Opdrachtgever.

Opdrachtnemer stelt een projectmanager aan die gedurende de gehele transitie als eenduidig aanspreekpunt fungeert voor Opdrachtgever. De projectmanager dient de coördinatie uit te voeren over alle werkzaamheden die worden uitgevoerd in het kader van dit project. Als zodanig is hij/zij eindverantwoordelijk voor het tijdig en adequaat uitvoeren van alle werkzaamheden die door de Opdrachtnemer worden uitgevoerd.

4.6. De dienstverlening

Opdrachtnemer is verantwoordelijk voor het reguliere beheer en de juiste werking van de IT-omgeving van Opdrachtgever, waaronder de Azure-omgeving, de netwerkomgeving en de Microsoft 365-applicaties. De Opdrachtnemer is binnen deze activiteiten verantwoordelijk voor het continue proces van beheren, onderhouden en updaten. Het reguliere beheer volgt het ITIL-framework.

De eerstelijnsondersteuning en het functioneel beheer wordt uitgevoerd door Opdrachtgever. De beheermedewerkers van Opdrachtgever vangen de eerste vragen vanuit de organisatie op en proberen de vragen eerst zelf te beantwoorden, waarbij de Opdrachtnemer geldt als achtervang

De ondersteuning, ofwel het support van Opdrachtnemer, start bij doorverwijzingen en/of eventuele escalaties die voortkomen uit de eerstelijnsondersteuning. Het is aan de Opdrachtnemer om deze problemen adequaat en snel op te lossen.

Opdrachtnemer verleent de dienstverlening:

i. enerzijds proactief en zelfstandig het deel waarbinnen op basis van vooraf vastgestelde kaders de Opdrachtnemer de IT-omgeving zelfstandig kan monitoren en beheren om de IT-omgeving en diensten optimaal te laten functioneren. De dienstverlening bestaat op hoofdlijnen uit de volgende onder
    a. Vraagbaak eerstelijns ondersteuning: Het bieden van diepgaande technische expertise over verschillende IT-domeinen om zodoende hWh kundig te kunnen ondersteunen en adviseren; en het hebben van kennis over het IT-omgeving van hWh, waaronder de koppelingen met betrekking tot kantoor- en bedrijfsapplicaties (niet Microsoft-applicaties), SAAS-oplossingen, netwerken (LAN/WAN/WLAN/Firewall), Microsoft oplossingen zoals Azure, Microsoft 365 en Micrsosoft Power Platform;
    b. Escalaties uit eerstelijns ondersteuning: Het diagnosticeren en oplossen van complexe problemen en (beveiligings-)incidenten die worden geëscaleerd vanuit eerstelijns support over de IT-omgeving, dan wel voortkomen vanuit incidentbeheer. Hieronder vallen ook acties die voortvloeien uit het Security Operations Center (SOC), zoals het meewerken aan onderzoeken, aanleveren van logfiles, meedenken over bronnen die gecontroleerd moeten worden, blokkeren van accounts en meelezen van de analyse. Als hierbij derden betrokken moeten worden (bijvoorbeeld applicatie- of WAN-leveranciers waarmee Opdrachtgever een contract heeft), dan dient Opdrachtnemer deze partijen ook operationeel aan te sturen. Als een incident leidt tot uitval van bepaalde functionaliteit dan dient Opdrachtnemer nader te bepalen functionarissen van Opdrachtgever hiervan op de hoogte te stellen en, waar relevant, fallback scenario's te activeren;
    c. Kantooromgeving (Devices): Het doorvoeren en bijhouden van updates en het aanleveren van informatie ten behoeve van het CMDB. Daarnaast ook het maken en beheren van images en policies, en waarborgen van connectiviteit van apparatuur met het netwerk;
    d. Update-/patch management: Het doorlopend actueel houden van de IT-omgeving op gebied van updates en patches (update management);
    e. Netwerkomgeving: Het uitvoeren van beheer en (routine)onderhoud op de netwerkomgeving en eventuele nieuwe netwerkdiensten en op de software van netwerkapparatuur. Hieronder wordt mede begrepen het werkend houden en up-to-date zijn van de netwerkomgeving om beveiligingsrisico's te minimaliseren en de prestaties te optimaliseren. Opdrachtnemer zorgt tevens voor monitoring en beveiliging (conform de gebruikelijke standaarden) van de netwerkomgeving. Alle gevraagde beheerprocessen zijn ook van toepassing op de WAN-verbindingen en internetverbindingen;
    f. Het uitvoeren van integraties en koppelen van andere IT-omgevingen (zoals SaaS-applicatie en clouddiensten) met de IT-omgeving van Opdrachtgever;
    g. Beheer inclusief monitoring van de Microsoft Azure-omgeving en Azure afgenomen diensten (inclusief Microsoft Azure cost management), Microsoft 365 en Microsoft

Power Platform. Opdrachtnemer informeert actief en tijdig de Opdrachtgever over de status door continu inzicht te bieden in de operationele status van meldingen, bijvoorbeeld door middel van ketenmonitoring en dashboards;

h. Azure landingzone(s) en Azure beheer wordt uitgevoerd conform de best practices van Microsoft (Microsoft Azure Well-Architected Framework/Cloud Adoption Framework) en volgt de referentie blauwdrukken van Opdrachtgever's Microsoft Kenniscentrum op basis van Infrastructure as Code en Terraform;
i. Security en compliance: Signaleren en mitigeren van beveiligingsincidenten, het borgen van BIO/ISO 27001:2015 compliance, het verlenen van ondersteuning aan het SOC en het groeien naar volwassenheidsniveau 4 conform het informatieveiligheidsmodel;
j. Opdrachtnemer werkt samen met de in het kader van informatieveiligheid derde dienstverlenende partijen;
k. De dienstverlening van Opdrachtnemer omvat tevens het adviseren en meedenken als "critical friend". Dat betekent dat Opdrachtnemer een eerlijke en objectieve kijk heeft en zaken probeert vanuit een extern perspectief te benaderen. De Opdrachtnemer geeft als critical friend behulpzame feedback, ondersteuning en suggesties voor verbetering binnen alle bovengenoemde beheerwerkzaamheden. Opdrachtgever kan op verzoek gebruik maken van de expertise van Opdrachtnemer, bijvoorbeeld met betrekking tot ontwerpen (architectuur), implementeren, beheren en het leveren van support op het Microsoft 365, Azure-platform en netwerkinfrastructuur. Deze verzoeken worden beschouwd als kleine en kortstondige afstemmingen en advisering, tenzij er sprake is van de situatie als bedoeld in onder ii sub n.;
l. Voor hardware van inhuur- en inleenmedewerkers dient Opdrachtnemer ondersteuning te leveren op basis van redelijke inspanning door Opdrachtnemer, d.w.z. actief meewerken en denken aan een oplossing wanneer de eindgebruiker dit meldt bij de IT-afdeling van de organisatie waar de inhuur of inleenmedewerker in dienst is;

De Vergoeding voor deze diensten bestaat uit vaste maandelijkse kosten en variabele maandelijkse kosten als genoemd in onderdeel 2a. en 2b. van het Prijzenblad;

ii. anderzijds al dan niet op verzoek: het deel waar nadrukkelijke afstemming met Opdrachtgever noodzakelijk is, bijvoorbeeld voor het doorvoeren van niet-standaard wijzigingen, en het leveren van advies en expertise voor zover dat verder gaat dan in de rol van critical friend:

m. Upgrade/life cycle management: Het doorlopend actueel houden van de IT-omgeving door de implementatie van nieuwe versies (upgrades) en nieuwe producten (lifecycle management);
n. Indien de ureninzet in verband met een verzoek als bedoeld onder i. sub k. naar het oordeel van Opdrachtgever zodanig hoog is dat het niet meer valt onder de noemer van kleine, kortstondige afstemming en advisering, kan dit als een project worden beschouwd. In dat geval worden de kosten verrekend op basis van een door Opdrachtgever goedgekeurd projectplan, goedgekeurde ureninschatting en de van toepassing zijnde uurtarieven;
o. In geval van (behoefte aan) uitbreiding, vernieuwing of vervanging van hardware of software:

i. adviseert Opdrachtnemer desgevraagd aan Opdrachtgever hierover;
ii. koopt Opdrachtgever zelf de betreffende hardware en software, en zorgt Opdrachtnemer desgevraagd voor on site configuratie en testen;

p. Trainingen: Het voorzien in trainingen en ondersteuningen aan het IT-beheerteam van Opdrachtnemer, bijvoorbeeld bij ingebruikname van nieuwe systemen (dit betreft expliciet niet de trainingen die gegeven worden aan eindgebruikers).

De Vergoeding voor deze diensten wordt bepaald aan de hand van een nadere Opdracht op basis van de uurtarieven als genoemd in onderdeel 3. van het Prijzenblad.

4.6.1. Responsetijden prioriteitsbepaling incidenten

Bij gebreken of verstoringen zijn de volgende reactietijden van toepassing:

Naam	Omschrijving	Reactietijd*	Status update	Geplande functie hersteltijd
Kritiek (P1)	Bij gebreken of verstoringen waardoor de beoogde werking van de IT-omgeving wordt verstoord; de dienstverlening kan niet meer plaatsvinden	30 minuten	Elk uur	80%<2u, 90%<8u, 99%<16u
Hoog (P2)	Bij gebreken of verstoringen die potentieel de beoogde werking van de IT-omgeving kunnen verstoren en waardoor een of meer IT-diensten van de IT-omgeving niet meer kunnen plaatsvinden, maar waarvoor een acceptabele work-around is gevonden om de werking van de IT-omgeving te continueren	1 uur	Elk 4 uur	80%<8u, 99%<48u
Medium (P3)	Bij gebreken of verstoringen die niet direct de beoogde werking van de IT-omgeving verstoren maar wel van belang zijn voor een volledige en correcte werking van de IT-omgeving	4 uur	Na oplossing storing	80%<16u, 99%<60u
Laag (P4)	Bij alle overige gebreken of verstoringen, waarvoor wel een oplossing gewenst is	16 uur	Na oplossing storing	Maximaal 10 werkdagen

Tabel 4.6.1: Reactietijden gebreken en verstoringen

*Onder reactietijd wordt verstaan: de maximale tijd, gerekend in kantooruren, tussen het (automatisch) genereren van een alarm (ongeacht de oorsprong), en het melden van een (mogelijk) incident bij de Opdrachtgever.

In het geval een incident driemaal of meer plaatsvindt, is Opdrachtnemer verplicht tot het uitvoeren van een root-cause-analysis om de oorzaak te zoeken, Opdrachtgever te adviseren over een passende oplossing en desgevraagd te implementeren.

4.6.2. Security

Opdrachtnemer meldt informatiebeveiligingsincidenten onverwijld conform tabel 4.6.2.1.1 bij de aangewezen contactpersoon van Opdrachtgever. De Opdrachtnemer dient alle gevraagde ondersteuning te leveren en actief samen te werken met Opdrachtgever en alle door Opdrachtgever daartoe aangewezen organisaties.

In afwijking van eis 24 van Bijlage F - Programma van Eisen IT-Beheer 2025 is Opdrachtnemer 24/7 direct telefonisch bereikbaar voor security incidenten. De werkwijze wordt nader uitgewerkt in Bijlage I – Dossier Afspraken en Procedures (DAP).

Opdrachtnemer voert wekelijks kwetsbaarheidsscans uit op de IT-omgeving van Opdrachtgever, registreert, informeert en rapporteert aan de Opdrachtgever en lost geconstateerde kwetsbaarheden op. Opdrachtnemer dient monitoring te implementeren voor dreigingsdetectie en moet in staat zijn om snel te reageren op beveiligingsincidenten in de Microsoft 365 en Azure omgeving.

Opdrachtgever moet gaan voldoen aan aankomende Cyberbeveiligingswet. Dit betekent dat Opdrachtgever binnen de keten risico's moet inventariseren. Opdrachtnemer zal binnen deze keten vallen en er wordt daarbij ook van Opdrachtnemer verwacht dat deze zal meewerken aan het inventariseren van de risico's van Opdrachtgever. Tevens zal Opdrachtnemer risico's binnen de eigen processen die invloed hebben op de processen van Opdrachtgever inventariseren en doorgeven aan de Opdrachtgever. Opdrachtnemer werkt mee aan uit te voeren risicoanalyses.

4.6.2.1. Classificatieniveau en reactietijden security incidenten

Opdrachtnemer draagt zorg voor een tijdige prioritering van en respons op security incidenten door melding aan de Opdrachtgever en het CERT-WM. Hierbij voldoet Opdrachtnemer aan de volgende richtlijn:

In onderstaande tabel staat de classificatie van gebeurtenissen voorvloeiend uit de security monitoring, leidend tot incidenten die de cyberveiligheid beïnvloeden en de snelheid waarmee de Opdrachtnemer op die incidenten reageert.

Classificatie	Omschrijving	Reactietijd**	Rapportagetijd & vorm	Mitigerende maatregelen
Succesvolle hack (Critical)	Een geslaagde, gerichte aanval is uitgevoerd op een systeem hetgeen resulteert in een ernstige inbreuk op de beveiliging, dan wel data exfiltratie wordt waargenomen. De impact hiervan moet zo snel mogelijk worden geminimaliseerd.	10 minuten	Elke 30 minuten Incident rapportage mailen aan Opdrachtgever	< 1 uur
Succesvolle inbreuk	Er is een inbreuk op de beveiliging die een hoog risico vormt.	10 minuten	Elke 30 minuten	< 1 uur

(Critical)	Directe aandacht is vereist.		Incident rapportage mailen aan Opdrachtgever	
High risk	Er is een poging gedaan om door de beveiliging heen te breken. Deze poging is mislukt, omdat de aanval niet succesvol was of omdat een beveiligingsvoorziening de activiteit blokkeerde. De oorzaak hiervan moet worden onderzocht.	1 uur	Elke 2 uur Incident rapportage mailen aan Opdrachtgever	< 4 uur
Benign Positive High Risk	Er wordt verdacht gedag geconstateerd (True Positive) dat niet als kwaadaardig hoeft te worden beschouwd. Bijvoorbeeld een penetratietest.	1 uur	Elke 2 uur Incident rapportage mailen aan Opdrachtgever	< 4 uur
Malicious Medium risk	Er heeft zich een aanvalspoging voorgedaan maar deze is niet geslaagd. Er is geen actie vereist, maar deze poging kan inzage geven in het dreigingslandschap of in de veiligheid van de eigen omgeving.	4 uur	4 uur Incident rapportage wordt beschikbaar gesteld	n.v.t.
False positive Low risk	Er is ten onrechte een alert afgegaan op gedetecteerd gedrag. Dit gedrag bleek tevens na analyse legitiem te zijn.	16 uur	16 uur Conclusie bijgevoegd bij case	n.v.t.
Not malicious	Detectie heeft gedrag geobserveerd dat als legitiem wordt bevonden binnen deze omgeving.	16 uur	16 uur Conclusie bijgevoegd bij case	n.v.t.

Tabel 4.6.2.1.1: Reactietijden security incidenten

**Onder reactietijd wordt verstaan: de maximale tijd (24/7), tussen het optreden van het (mogelijk) incident, en het melden van een (mogelijk) incident bij de Opdrachtgever.

4.6.3. Technisch beheer hostingplatform

Voor de beheer- en projectactiviteiten op het hostingplatform zijn diverse subscriptions ingericht (zie paragraaf 3.7). Deze subscriptions maken onderdeel uit van de IT-omgeving. De dienstverlening voor het hostingplatform omvat, naast de overige uit overeenkomst voortvloeiende diensten, onder andere:

- Aanmaken subscription in Azure portal;
- Azure Policy gebruiken om naleving van hWh regels af te dwingen;
- Rollen toewijzen met Azure RBAC (Role-Based Access Control) om toegang tot resources te beheren;
- Beheerdersrollen toevoegen of wijzigen;
- Kosten en gebruik monitoren en kostenwaarschuwingen uitsturen;
- Voorstellen doen voor kostenbesparingen;
- Beleid configureren voor subscriptions;
- Azure beveiligingsmaatregelen beheren en toepassen zoals netwerkbeveiligingsgroepen en firewallregels;
- Resources beheren;
- Tagging gebruiken voor het categoriseren en beheren van resources;
- Monitoring gebruiken voor het bewaken van de prestaties en beschikbaarheid van resources;
- Log Analytics gebruiken voor het verzamelen en analyseren van loggegevens;
- Afstemming met de derde partij die zijn diensten via een subscription aanbiedt.

Op aangeven van Opdrachtgever is het mogelijk dat (een deel van) de bovenstaande activiteiten worden uitgevoerd door een derde partij.

4.7. Niet-standaard wijzigingen

Opdrachtnemer dient:

- op verzoek te adviseren over niet-standaard wijzigingen van de IT-omgeving;
- op verzoek niet-standaard wijzigingen van de IT-omgeving te realiseren of bij te dragen aan de realisatie daarvan, zoals systeemupgrades, migraties en implementaties.

Bij een niet-standaardwijziging moet het gehele wijzigingsproces (zie Bijlage G – Beleid Change Management) worden doorlopen. De wijziging moet worden gepland, het risico moet worden beoordeeld en de wijziging moet worden goedgekeurd. Nadere afspraken over het wijzigingenproces worden vastgelegd in een Dossier Afspraken en Procedures (DAP).

Opdrachtgever kan nadere Opdrachten voor adviezen en niet-standaardwijzigingen ook opdragen aan derden en is derhalve niet verplicht adviezen bij Opdrachtnemer te vragen en al evenmin verplicht niet-standaard wijzigingen door Opdrachtnemer te laten uitvoeren.

4.7.1. IAM oplossing

De Opdrachtgever heeft de behoefte om het Identity & Access Management (IAM) proces verder te automatiseren en te verbeteren. Dit moet leiden tot een efficiënter beheer van identiteiten en toegangsrechten, waarbij de beveiliging wordt versterkt, operationele efficiëntie wordt verhoogd en naleving van regelgeving wordt gewaarborgd.

De Opdrachtnemer dient een onafhankelijk en gedegen advies op te stellen. Dit advies moet zijn gebaseerd op een grondige analyse van alternatieven, waarbij het bedrijfsprofiel van de Opdrachtgever worden meegenomen. Het advies kan worden opgevolgd door de implementatie van een passende IAM-oplossing.

De Opdrachtnemer wordt verantwoordelijk voor de volgende activiteiten:

- **Advisering en Analyse**
  - Binnen één maand na ingang van de overeenkomst opleveren van een onafhankelijk advies over een passende IAM-oplossing.
  - Analyse van beschikbare alternatieven, inclusief een vergelijking van functionaliteiten en mogelijkheden.
  - In kaart brengen van de functionele eisen en kaders op basis van het bedrijfsprofiel en de behoeften van de Opdrachtgever.
  - Definiëren van een onderbouwde implementatieaanpak.
  - Advisering over de mate van detail en afbakening van toegangsrechten, bijvoorbeeld op programmaniveau of per project.

- **Implementatie (op verzoek)**
  Op verzoek van Opdrachtgever dient Opdrachtnemer binnen zes maanden na ingang van de overeenkomst de door Opdrachtgever gekozen IAM-oplossing te realiseren en operationeel te maken, inclusief:
  - het opstellen en implementeren van functieprofielen voor verschillende rollen, zoals Projectleider, Technisch Manager, PMO, Inkoper, Contractmanager en HR medewerker;
  - het inrichten van governance en beheerprocessen rondom IAM.

  Opdrachtgever is niet verplicht de implementatie door Opdrachtnemer te laten uitvoeren en kan dit ook door een derde laten uitvoeren.

- **Beheer**
  - De Opdrachtnemer is verantwoordelijk voor het beheer van de geïmplementeerde tool.
  - Automatisering van IAM-processen, inclusief het beheren en toekennen van rollen en rechten.
  - Integratie met relevante applicaties en systemen binnen de organisatie.

Vanuit de regierol van Opdrachtgever selecteert Opdrachtgever de IAM-oplossing en koopt deze zelf in.

4.8. Governance

Opdrachtnemer rapporteert en overlegt periodiek strategisch, tactisch en operationeel met Opdrachtgever over de uitvoering van de Overeenkomst.

Strategisch overleg

Doel van dit overleg is het bespreken van de kwaliteit van de IT-omgeving en de dienstverlening in de afgelopen periode, het bespreken van nieuwe marktontwikkelingen en het bepalen van eventuele aanpassingen in de dienstverlening. Eenmaal per jaar kan hierbij ook de meting van de gebruikerstevredenheid worden betrokken. Opdrachtnemer geeft gevraagd en ongevraagd advies over optimalisatie en kostenverlaging door inzet van alternatieve producten en/of oplossingen. De frequentie van het strategisch overleg is tweemaal per jaar.

Tactisch overleg

Doel van dit overleg is het bespreken van de kwaliteit van de IT-omgeving en de dienstverlening. Input voor het overleg zijn onder andere de servicelevel rapportages en voortgangsrapportages

van de wijzigingen. Het overleg dient te resulteren in voorstellen tot verbetering van de kwaliteit van de dienstverlening, vermindering van het aantal service desk meldingen, of kostenoptimalisatie.

De frequentie van dit overleg is 2-maandelijks en vindt plaats op de tweede dinsdag van de even maand. Het eerste halfjaar vindt dit overleg 2-wekelijks plaats mede om een goede onderlinge relatie op te kunnen bouwen.

De Opdrachtnemer geeft minimaal tweemaal per jaar gevraagd en ongevraagd aanbevelingen/adviezen over de Microsoft 365 en Azure omgeving, zoals compliancy, monitoring, resourcegebruik, security, beveiligingsmaatregelen en de manier waarop oplossingen ingezet worden.

Change Advisory Board (CAB)

Het CAB is een overlegorgaan van de Opdrachtgever dat zo vaak als nodig overlegt. Doel van CAB is het beoordelen van niet-standaard wijzigingen, eventuele wijzigingen in de SLA en eventuele additionele diensten. Indien relevant sluit Opdrachtnemer zich, met de benodigde expertise, aan bij het CAB zoals door Opdrachtgever is georganiseerd. Dit laat onverlet hoe Opdrachtnemer het wijzigingsbeheer intern heeft georganiseerd.

Securityoverleg

Doel van dit overleg is het bespreken van het actuele dreigingslandschap en risicobereidheid van Opdrachtgever. Opdrachtnemer geeft proactief advies en legt diverse scenario’s voor aan Opdrachtgever hoe om te gaan met deze bedreigingen en risico’s. De frequentie van dit overleg is elk kwartaal.
Opdrachtgever en Opdrachtnemer stellen allebei vaste contactpersonen aan voor communicatie over de dienstverlening en leggen deze vast in de DAP.

Alle overleggen vinden plaats op een locatie van Opdrachtgever, tenzij door Opdrachtgever anders wordt bepaald. Uiterlijk een week vóór een overleg, levert Opdrachtnemer een voortgangsrapportage met betrekking tot het betreffende overleg aan Opdrachtgever aan. Van alle overleggen wordt door Opdrachtnemer een schriftelijk verslag gemaakt. Het verslag wordt binnen een week na het overleg voorgelegd als concept aan Opdrachtgever. Opdrachtnemer en Opdrachtgever stellen het verslag binnen een week na voorlegging van het concept aan Opdrachtgever vast.

De gedetailleerde invulling van de rapportages en overlegstructuur wordt vastgelegd in de DAP.

De rollen en organisatie bij Opdrachtgever zijn nog in ontwikkeling. In samenwerking met de Opdrachtnemer wordt periodiek gekeken hoe de overleggen op de beste manier kunnen worden ingericht.