BIJLAGE 10 DOSSIER AFSPRAKEN & PROCEDURES KANTOORAUTOMATISERING

INHOUDSOPGAVE

1. Inleiding

1.1. Doel van het DAP

In het Dossier Afspraken & Procedures (DAP) zijn de afspraken vastgelegd over de dienstverlening door *[Opdrachtnemer]*, hierna te noemen Opdrachtnemer, aan Vereniging IPO, hierna te noemen Opdrachtgever.

Het DAP beschrijft hoe de dienstverlening wordt geleverd, de procedures die hierbij worden gevolgd en de samenwerking en communicatie tussen Opdrachtgever en Opdrachtnemer.

De scope van de dienstverlening is beschreven in de *[Overeenkomst]* d.d. *[datum]* (hierna te noemen de Overeenkomst).

1.2. Geldigheidsduur van het DAP

Dit DAP heeft een looptijd gelijk aan de looptijd van de Overeenkomst.

1.3. Wijziging en goedkeuring van het DAP

Dit DAP wordt goedgekeurd door:

- Manager Bedrijfsvoering (Opdrachtgever namens Vereniging IPO)

En

- *[Contracteigenaar]* (Opdrachtnemer)

Het DAP kan door partijen in gezamenlijk overleg en na schriftelijke vastlegging worden gewijzigd, bijvoorbeeld als gevolg van aangepaste procedures of wijziging in de samenwerking. Opdrachtgever en Opdrachtnemer zorgen gezamenlijk voor het opnemen van (gewijzigde) afspraken in het DAP.
De Servicemanagers van Opdrachtgever en Opdrachtnemer zijn gemandateerd om wijzigingen van het DAP door te voeren.
Wijziging van het DAP zal slechts schriftelijk tot stand komen. Na ondertekening door bovenstaande personen wordt deze van kracht.

2. Producten & Diensten

2.1. Cloud Service

Opdrachtnemer is Cloud Service Provider van de Microsoft-omgeving van Opdrachtgever.

2.2. Netwerk/infrastructuur

Opdrachtnemer is verantwoordelijk voor het beheer van het netwerk en de infrastructuur van Opdrachtgever. Alle onderdelen van deze infrastructuur zijn opgenomen in "Bijlage 18 - Huidige situatie".

2.3. Applicaties

Opdrachtnemer is verantwoordelijk voor het beheer van de Microsoft365-applicaties, overige MS-applicaties (MS Projects, MS Visio) en het applicatieportfolio dat is opgenomen in Intune.

2.4. Apparaten

Opdrachtnemer is verantwoordelijk voor het beheer van apparaten van Opdrachtgever.
Apparaten die in beheer zijn en/of waar Opdrachtnemer de regie over heeft, zijn:

- Laptops (Windows en Linux)
- Mobiele telefoons
- Printers/scanners
- Audiovisuele middelen en werkplekaccessoires
- On premise apparatuur

Zie hiervoor ook "Bijlage 18 - Huidige situatie".

2.5. Servicedesk

Opdrachtnemer levert een Nederlandstalige servicedesk.

3. Afspraken & Procedures

3.1. Technisch beheer

Opdrachtnemer is verantwoordelijk voor het technisch beheer van de Microsoft-omgeving van Opdrachtgever.
Dit houdt onder andere in:

- Het uitvoeren (testen, accepteren en in productie nemen) van technische wijzigingen in en connecties met het platform;
- Beheer van het platform: beheer van accounts, wachtwoorden, toegang, installatie van clients, installatie van nieuwe releases;
- Opstellen/bijhouden van de installatie-handleiding van het platform en alle connecties;
- Opstellen/bijhouden van technische systeemdocumentatie van het platform en alle applicaties;
- Onderhouden en uitvoeren van back-up en recovery procedures.
- Beheer en installatie van beveiligingscertificaten (TLS) op servers.

Beheer wordt uitgevoerd conform de Microsoft standaarden[1].

[1] https://www.microsoft.com/licensing/docs/view/Service-Level-Agreements-SLA-for-Online-Services

3.2. Apparaatbeheer

Alle apparaten worden beheerd in Intune.

3.2.1. Laptops

De volgende werkzaamheden worden uitgevoerd door Opdrachtnemer:

- Inspoelen: Opdrachtnemer draagt zorg voor het inrichten van laptops met de juiste Microsoft (beveiligings)instellingen en up-to-date standaard applicaties, zodat deze direct klaar voor gebruik is.
- Voorraadbeheer & laptopgebruik (in CMDB + Assetmanagement).
- Wissen bij diefstal/verlies en bij uit dienst van medewerkers.

3.2.2. Mobiele telefoons

De volgende werkzaamheden worden uitgevoerd door Opdrachtnemer:

- Opzetten en beheren van een bedrijfsportaal (MAM) m.b.v. MS Intune Suite.
- Apps in het bedrijfsportaal configureren en beheren.
- Gebruiksklaar maken van telefoons d.m.v. het toevoegen van een gebruikersprofiel.
- Wissen bij diefstal/verlies en bij uit dienst van medewerkers.

Exclusief aanschaf en beheer van SIM-kaarten.

3.2.3. Printers/scanners

Op beide locaties zijn printers aanwezig. Alle medewerkers moeten op beide locaties kunnen printen. De printers zijn verbonden met het netwerk dat wordt beheerd door Opdrachtnemer. De volgende taken worden uitgevoerd door Opdrachtnemer:

- Gebruikersbeheer in de printomgeving (momenteel van Canon). Gebruikers werken via uniFLOW SmartClient.
- Installatie en versiebeheer van drivers.

3.2.4. Audiovisuele middelen & werkplekaccessoires

Opdrachtnemer voorziet in het technisch beheer van:

- Audiovisuele (AV) middelen in Den Haag: televisies, beamers, presentatie-/vergaderschermen met bijbehorende audiovisuele toepassingen. De AV-middelen zijn verbonden met het netwerk dat wordt beheerd door Opdrachtnemer.
- Alle werkplekaccessoires, zoals, maar niet beperkt tot: muizen, toetsenborden, docking stations, et cetera.

3.2.5. On premise apparatuur

Opdrachtnemer beheert de on premise hardware van Opdrachtgever. Alle onderdelen van de on premise hardware zijn opgenomen in “Bijlage 18 - Huidige situatie”.

3.3. Bring your own device

Het is toegestaan voor externe medewerkers om gebruik te maken van een eigen laptop of mobiele telefoon (BYOD). Opdrachtnemer ondersteunt hierbij op volgende wijze:

- Externe medewerkers moeten hun mobiele apparaat registreren in het, door Opdrachtnemer beheerde, bedrijfsportaal (MAM). Medewerkers kunnen op de mobiele telefoons alleen maar goedgekeurde applicaties gebruiken.
- Externe medewerkers krijgen op hun eigen laptop een virtuele werkplek.

3.4. Applicatiebeheer

Opdrachtnemer is verantwoordelijk voor het applicatiebeheer van alle Microsoft 365-producten, de overige Microsoft-producten (MS Projects, MS Visio, etc.) en alle overige producten die in Intune zijn opgenomen (ongeveer 70 applicaties). Dit houdt onder andere in:

- In beheer nemen van applicaties en eventuele door derden uitgevoerde wijzigingen of uitbreidingen op de applicaties;
- Herstellen van fouten;
- Realiseren van functionele wijzigingen;
- Opstellen/bijhouden van applicatiedocumentatie, indien uitgevoerd en geïmplementeerd door Opdrachtnemer (technische ontwerpen, installatie-instructies);
- Uitvoeren van onderhoud, technische verbeteringen, updates/upgrades;
- Versiebeheer voor alle componenten van de applicaties en datadiensten;
- Inschatten/monitoren/rapporteren over gebruik van applicatielicenties;
- Bestellen van applicatielicenties;
- Installeren van applicatielicenties.

3.4.1. Actieve gebruikers

Opdrachtgever maakt voor Microsoft365 standaard gebruik van E5-licenties. Medewerkers die in Intune gekoppeld zijn aan een E5-licentie óf als exchange only user geregistreerd staan, worden gezien als een actieve gebruiker. Elke maand levert Opdrachtnemer uiterlijk op de laatste werkdag van de maand een overzicht aan bij Opdrachtgever met alle actieve gebruikers. Deze wordt in ieder eerstvolgend tactisch overleg geagendeerd en goedgekeurd door Opdrachtgever. Met dit akkoord mag Opdrachtnemer op basis van dit aantal actieve gebruikers factureren voor de kalendermaand.

3.5. Meldingenbeheer

Er zijn zes types meldingen te onderscheiden:
1. Incidenten
2. Problemen
3. Serviceverzoeken (requests for service (RFS))
4. Informatieverzoeken (requests for information (RFI))
5. Voorstel-/Offerteverzoeken (requests for proposal/quotation (RFP/RFQ))
6. Wijzigingsverzoeken (requests for change (RFC))

Ieder type melding wordt door Opdrachtgever bij Opdrachtnemer aangemeld. Dit kan via telefoon, e-mail, of rechtstreeks in het door Opdrachtnemer geleverde service management systeem. De servicedesk van Opdrachtnemer (zie paragraaf 3.8) draagt zorg voor het afhandelen van alle binnengekomen tickets conform KPI's. Hierbij wordt de aanmelder van Opdrachtgever altijd direct zo concreet en volledig mogelijk geïnformeerd bij statusupdates.

Opdrachtnemer rapporteert maandelijks over alle aangemelde, afgesloten en eventueel langdurig openstaande tickets van elk hierboven benoemd type, met afhandeltijden en SLA-statistieken, in de servicemanagement-rapportage.
Langdurig openstaande tickets worden ook besproken tijdens het wekelijkse operationeel overleg (zie paragraaf 4.2).

3.5.1. Incidenten

Incidentbeheer is gericht op het zo snel mogelijk verhelpen van verstoringen, gebreken of fouten in de juiste werking van de door Opdrachtnemer geboden producten en diensten die binnen de scope van de Overeenkomst vallen, met als doel de continuïteit van de dienstverlening zo snel mogelijk te herstellen.

Incidenten kunnen worden gemeld door medewerkers van Opdrachtgever en door Opdrachtnemer zelf. P1-incidenten dienen altijd telefonisch te worden aangemeld.
Zodra de status van het incident verandert, en na het verhelpen van het incident, informeert Opdrachtnemer Opdrachtgever direct hierover. Een incident is pas afgesloten als Opdrachtgever de oplossing accepteert.

Prioriteitstelling

De gevolgen van een incident voor de bedrijfsvoering van Opdrachtgever zijn leidend voor de volgorde en wijze van afhandeling. Hiertoe wordt bij aanmelding van het incident op basis van de omschrijving en de afgesproken prioriteitsstelling in de SLA de prioriteit bepaald door de servicedesk (P1, P2 of P3).
Bij discussie over prioritering geldt de escalatieladder (zie paragraaf 4.6).

Beveiligingsincidenten
Een beveiligingsincident is een inbreuk op de beveiliging waarbij de beschikbaarheid, integriteit of vertrouwelijkheid van gegevens in het geding komt.
Bij beveiligingsincidenten wordt door Opdrachtnemer altijd de information security officer (ISO) of de Chief Information Security Officer (CISO) van Opdrachtgever geïnformeerd.
Bij incidenten die betrekking hebben op de privacy van de organisatie van Opdrachtgever, wordt door Opdrachtnemer altijd de privacy officer van Opdrachtgever geïnformeerd.

3.5.2. Problemen

Probleembeheer heeft tot doel het structureel oplossen van ernstig verstorende incidenten alsmede terugkerende/samenhangende incidenten.
Om de dieperliggende oorzaak van deze incidenten te elimineren, wordt er een Probleem-ticket aangemaakt door Opdrachtnemer.

Opdrachtnemer draagt zorg voor het opstellen van een RCA (root cause analysis). In deze RCA wordt beschreven wat de dieperliggende oorzaak is geweest van de incidenten die tot het probleem hebben geleid. Ook wordt voorgesteld hoe het probleem kan worden opgelost. Als het probleem direct kan worden opgelost, wordt dit door Opdrachtnemer ook direct uitgevoerd. Als de oplossing een wijziging vereist, wordt dit kenbaar gemaakt aan Opdrachtgever. Vervolgens wordt (indien Opdrachtgever dit nodig acht) een wijzigingsverzoek (change request) aangemaakt om de oplossing te implementeren.

3.5.3. Serviceverzoeken (requests for service (RFS))

Een serviceverzoek is een verzoek voor een specifieke, standaard en eenvoudige service of ondersteuning vanuit Opdrachtnemer. Voorbeelden van serviceverzoeken zijn:

- Toegang verlenen of intrekken (bijvoorbeeld een mailbox);
- Aanvragen van een nieuwe (gedeelde) mailbox, SharePoint-site of Teams-omgeving;
- Installatie van goedgekeurde applicaties en/of licenties;
- Vragen over het gebruik van applicaties of hardware;
- Aanmaken of verwijderen van gebruikers;
- Aan- of uitzetten van (nieuwe) Microsoft-diensten.

Voor specifieke soorten serviceverzoeken kan het nodig zijn om een specifieke werkinstructie op te stellen die gehanteerd zal worden door Opdrachtnemer.

3.5.4. Informatieverzoeken (requests for information (RFI))

Een informatieverzoek is een middel dat Opdrachtgever wil gebruiken om informatie te verzamelen van Opdrachtnemer over mogelijke producten of diensten die zij Opdrachtgever kan bieden, of een oplossing zoekt voor een complex probleem. Opdrachtgever wil dit type verzoeken inzetten aan de beginfase van een inkoopproces, wanneer nog niet precies bekend is welke oplossing zij nodig heeft, maar wel wil begrijpen welke mogelijkheden er op de markt beschikbaar zijn. De RFI kan mogelijk leiden tot een voorstel-/ of offerteverzoek (zie paragraaf 3.6.5).

3.5.5. Voorstel-/Offerteverzoeken (requests for proposal/quotation (RFP/RFQ))

Opdrachtgever kan Opdrachtnemer vragen om een voorstel te leveren middels het voorstelverzoek, wanneer zij een gedetailleerde oplossing zoekt voor een complex probleem.

Het biedt ruimte voor Opdrachtnemer om haar aanpak, oplossing, planning en prijs voor te stellen.
Een "eenvoudiger" versie hiervan is het offerteverzoek. Deze wordt ingezet wanneer Opdrachtgever vraagt om een specifiek product of dienst.

3.5.6. Wijzigingsverzoeken (requests for change (RFC))

Een wijzigingsverzoek is een verzoek voor een nieuw product of dienst, of een verzoek om een bestaand product of dienst (functioneel) aan te passen.
Voorbeelden van wijzigingsverzoeken zijn:

- Wijziging aan de inrichting van het Microsoft-platform;
- Wijzigingen aan het netwerk, de internetverbinding of de VPN;
- Het in beheer nemen van een nieuwe applicatie.

Er kan ook sprake zijn van een noodwijziging (emergency change request). Een wijziging geldt als noodwijziging als het om een wijziging gaat waarmee een P1-incident opgelost kan worden. De noodwijziging heeft voorrang op alle andere wijzigingen.

3.6. Gedeeld beheer

Opdrachtgever heeft Functioneel beheerders met Admin accounts op de Microsoft-omgeving. Opdrachtgever zal twee Global admin accounts gebruiken. De functioneel beheerders dienen volledige leesrechten te hebben. Alle uitvoerende beheertaken en verantwoordelijkheden liggen bij Opdrachtnemer. Acties worden alleen uitgevoerd met wederzijdse goedkeuring door en vastlegging met beide partijen. Dit kan ook het toekennen van adminrechten op een derde partij zijn. Hierover moet altijd worden vastgelegd om welke rol het gaat en voor welke periode. Opdrachtgever wil dit volgens Privileged Identity Management (PIM).

3.7. Servicedesk

De servicedesk van Opdrachtnemer levert medewerkers van Opdrachtgever ondersteuning op het gebruik van de producten en diensten die Opdrachtnemer levert binnen de gesloten Overeenkomst en eventueel aanvullende opdrachten. De servicedesk voldoet aan de volgende voorwaarden:

- De servicedesk is "skilled". Dat wil zeggen dat medewerkers van de servicedesk beschikken over technisch inhoudelijke kennis van de producten en diensten die Opdrachtnemer levert, en hierdoor in staat zijn om minimaal 80% van de tickets direct zelfstandig af te handelen. De overige 20% wordt in overleg met Opdrachtgever en/of, indien nodig, met een derde partij opgelost.
- De voertaal bij alle communicatie (mondeling en schriftelijk) is 100% Nederlands.

De servicedesk van Opdrachtnemer is verantwoordelijk voor het aannemen, registreren, coördineren, bewaken, afhandelen en rapporteren van alle binnenkomende tickets die betrekking hebben op de te leveren producten en diensten. Opdrachtnemer levert hierbij eerstelijns ondersteuning. Dit betekent dat ze van iedere medewerker van Opdrachtgever tickets aannemen, tenzij voor bepaalde typen tickets is afgesproken dat deze alleen mogen worden ingediend door vooraf vastgestelde geautoriseerde medewerkers.

De servicedesk draagt gedurende de looptijd van ieder ticket zorg voor communicatie over de voortgang met individuele gebruiker en operationeel aanspreekpunt Opdrachtgever.

De servicedesk draagt zorg voor tijdige afhandeling van tickets conform de in de SLA genoemde response- en oplostijden, gedurende het in de SLA genoemde Ondersteuningsvenster.

Bij de inzet van derde partijen, is Opdrachtnemer verantwoordelijk voor de aansturing van die partijen, waarvoor Opdrachtnemer het beheer heeft opgepakt conform de Overeenkomst.

De servicedesk is op de volgende manieren bereikbaar voor medewerkers van Opdrachtgever:

- Een vast telefonisch nummer, tegen lokaal binnenlands of gratis tarief (geen internationale nummers, geen betaalnummers). Gedurende het Ondersteuningsvenster kunnen telefonisch meldingen doorgegeven worden.
- Een service management systeem, waarbij medewerkers van Opdrachtgever zijn/haar eigen tickets kunnen inzien en reacties kunnen plaatsen. Daarnaast is het systeem breder toegankelijk voor geautoriseerde medewerkers van Opdrachtgever, die inzage hebben in alle geregistreerde tickets en ticketrapportages. Inloggen gaat via het Microsoft 365-account van de medewerker. Het service management systeem wordt geleverd door Opdrachtnemer.
- Een vast e-mailadres. E-mails kunnen 24*7 verzonden worden aan Opdrachtnemer. E-mails die naar dit e-mailadres worden gestuurd, leiden direct tot de aanmaak van een ticket in het service management systeem. De aanmelder krijgt direct een bevestiging van aanmaak van het ticket, inclusief ticketnummer. De afhandeling van tickets vindt plaats gedurende het Ondersteuningsvenster.

3.7.1. On site support

Veel support-werkzaamheden kunnen remote worden uitgevoerd. De praktijk leert echter dat het wenselijk is dat Opdrachtnemer op regelmatige basis op locatie van Opdrachtgever aanwezig is.
Opdrachtnemer is wekelijks op dinsdag fysiek tussen 08:00-13:00 aanwezig voor on site support, afwisselend op locatie Den Haag en Utrecht. Er is dan minimaal 1 (servicedesk)medewerker van Opdrachtnemer aanwezig.
De exacte aard van de werkzaamheden wordt in onderling overleg bepaald. Gedacht wordt aan:

- Ad hoc uitleg en helpen van gebruikers;
- Afhandeling van vooraf afgesproken (vaste) werkzaamheden;
- Afhandeling van werkzaamheden die konden wachten tot de on site support dag;
- Tickets bijwerken van alle uitgevoerde werkzaamheden tijdens de on site support dag.
- Uitleveren van apparaten.

Ondersteuning op locatie vindt op afgesproken dagen plaats en wordt voor het gehele jaar vooraf ingepland.

3.8. Configuratiebeheer & activabeheer (CMDB)

Opdrachtnemer houdt een CMDB bij, inzichtelijk voor Opdrachtgever.
Dit heeft als doel dat er te allen tijde actuele, nauwkeurige en betrouwbare informatie beschikbaar is over de producten die Opdrachtnemer beheert en de Configuratie Items (CI's) die deze ondersteunen. De informatie wordt direct na iedere release/update geactualiseerd.
Bij het in beheer nemen van een nieuw product of applicatie worden alle configuratie-items van dit product in de CMDB opgenomen.
Bij een uitfasering van een product of applicatie worden alle configuratie-items van dit product uit de CMDB gehaald.
Het wijzigen van de CMDB wordt altijd uitgevoerd met versiebeheer: na elke wijziging is zichtbaar wat er aangepast is.
De functioneel beheerders KA en technisch beheerder KA van Opdrachtgever krijgen leesrechten op deze CMDB.

Opdrachtnemer houdt ook alle in beheer zijnde activa (assets) bij. Dit kan in de CMDB opgenomen worden, of in een apart asset managementsysteem.
De focus ligt op alle activa van Opdrachtgever die in beheer is bij Opdrachtnemer, zoals hardware, softwarelicenties, financiële activa, infrastructuur, en andere middelen. Het beschrijft zaken zoals aanschaf, eigendom, gebruik, kosteneffectiviteit, onderhoud en afschrijving.
Het doel is om het gebruik, de waarde en de levensduur van activa te optimaliseren, evenals het beheer van kosten en investeringen.

3.9. Identity & Access Management (IAM)

Opdrachtnemer voorziet in een integrale en generiek toepasbare Identity & Access Management (IAM) dienst waarmee niet alleen op een veilige en betrouwbare manier de verschillende clouddiensten en on premise domeindiensten kunnen worden ontsloten, maar ook eventuele toekomstige nieuwe diensten kunnen worden aangesloten. De dienst dient de volgende faciliteiten te omvatten: Auto User Provisioning, Service Automation, Passwordmanagement, Single Sign On (SSO), Role Based Access Control / Access Governance en faciliteiten voor Auditing en Compliance management.

3.10. Infrastructuur (netwerk en internettoegang)

Opdrachtnemer beheert het kantoornetwerk op (alle) locaties van Opdrachtgever. Het netwerk is altijd versleuteld.
Alle toegang tot het internet gaat via een beveiligde bedrijfsverbinding (Govroam VPN).
Er wordt gebruik gemaakt van eigen DNS-servers waar dagelijks gescand wordt op het voorkomen van kwaadwillende verzoeken.

3.11. Calamiteitenbeheer

Een calamiteit is een onverwachte, ernstige gebeurtenis die leidt tot verstoring of onderbreking van de normale werking van IT-systemen, -netwerken of -diensten, waarbij het functioneren van de organisatie ernstig beïnvloed wordt. Hierbij is er sprake van downtime en dataverlies.
Voorbeelden zijn (regionale) stroomstoring, uitval van externe communicatielijnen, brand in gebouwen enzovoort. Bij een calamiteit dient Opdrachtnemer te zorgen voor continuïteit in de afgesproken dienstverlening. Indien Opdrachtnemer gebruik maakt van een uitwijk, mogen alle producten en diensten in beheer hiervan geen hinder ondervinden. Opdrachtnemer dient een adequaat calamiteitenplan voor te leggen aan Opdrachtgever bij het aangaan van het contract. Opdrachtgever beoordeelt of het calamiteitenplan adequaat is en kan indien nodig aanvullende maatregelen eisen.

3.12. Informatiebeveiligingsbeheer

Hieronder volgen de securitymanagement procedures die door de Opdrachtgever worden vastgesteld in samenwerking met Opdrachtnemer. Het doel van deze procedures is om een veiligere kantoorautomatiseringsomgeving te waarborgen, de integriteit en vertrouwelijkheid van gegevens te beschermen, en te voldoen aan relevante wet- en regelgeving.

3.12.1. Doelstellingen

- Beveiliging van Informatie: Garanderen dat alle gevoelige informatie en systemen adequaat worden beveiligd tegen ongeoorloofde toegang en datalekken.
- Risicovermindering: Identificeren en mitigeren van potentiële beveiligingsrisico's door middel van een gestructureerde aanpak.
- Compliance: Voldoen aan relevante regelgeving en standaarden, zoals GDPR/AVG, ISO 27001, en Baseline Informatiebeveiliging Overheid (BIO 1 en straks BIO 2) en de NIS2-richtlijnen.

3.12.2. Beveiligingsaspecten

Toegangsbeheer

- Authenticatie: Implementatie van een sterk wachtwoordbeleid, inclusief Multi-Factor Authentication (MFA) voor alle systemen. Voor kritieke systemen zal in de toekomst zwaardere eisen worden gesteld.
- Autorisatie: Toegang tot systemen en informatie wordt verleend op basis van het principe van de minste privilege (least privilege), waarbij gebruikers alleen toegang krijgen tot informatie die noodzakelijk is voor hun rol.

- Periodieke herzieningen: Regelmatige herziening van toegangsrechten om ervoor te zorgen dat ze up-to-date blijven en corresponderen met de huidige functies en verantwoordelijkheden van gebruikers.

Databeveiliging

- Versleuteling: Gegevens in rust en in transit worden versleuteld met eigen sleutels om onbevoegde toegang te voorkomen.
- Verwisselbare opslagmedia: is altijd met Bitlocker versleuteld.
- Wachtwoordkluis: voor alle wachtwoorden, wachtzinnen, secrets en versleutelingsleutels wordt een wachtwoordkluis gebruikt waar de eisen van *Toegangsbeheer* van toepassing op is.
- Back-up: Regelmatige back-upprocedures moeten worden ingesteld en getest (zie paragraaf 3.15).
- Dataclassificatie: Gegevens worden geclassificeerd op basis van hun gevoeligheid, en beveiligingsmaatregelen worden afgestemd op het risiconiveau van elk gegevenstype.

Beveiliging van Netwerken

- Firewall en Intrusion Detection Systems (IDS): Beveiliging van netwerken door het implementeren van firewalls en IDS om ongeoorloofde toegang en aanvallen te detecteren.
- VPN voor interne toegang: Gebruik van Virtual Private Networks (VPN) voor veilige toegang tot interne systemen vanuit externe locaties.
- VPN voor Externe Toegang: Gebruik van Virtual Private Networks (VPN) voor veilige toegang tot externe systemen vanuit interne en externe locaties.
- DNS-server: Gebruik van een eigen DNS-server is om alle DNS-verzoeken binnen de organisatie inzichtelijk te hebben en om te voorkomen dat partijen zoals Google profielen van medewerkers kunnen opbouwen.
- Timeserver: Gebruik van een timeserver is om ervoor te zorgen dat alle systemen dezelfde tijd hanteren. Dit is belangrijk voor de juiste werking van encryptie en het afhandelen van incidenten. Systemen waarvan de tijd niet met die van de timeserver overeenkomen, worden actief gesignaleerd en binnen maximaal één werkdag aangepast.

Beveiliging van Apparatuur

- Fysieke Beveiliging: Zorg voor fysieke beveiligingsmaatregelen bij bedrijfsfaciliteiten om onbevoegde toegang tot servers en netwerkapparatuur te voorkomen.
- Apparaatmanagement: Implementatie van Mobile Device Management (MDM) voor beheer en beveiliging van mobiele apparaten.

3.12.3. Incidentbeheer

Incident Response Plan

- Identificatie en Rapportage: Procedures voor het snel identificeren en rapporteren van beveiligingsincidenten.
- Responsteams: Toewijzing van verantwoordelijkheden aan specifieke medewerkers of teams voor de afhandeling van incidenten, inclusief IT, juridische, en Public Relations (PR)-teams.
- Opdrachtnemer: Pakt pro- en reactief security gerelateerde signalen op. Indien nodig wordt dit met de Information Security Officer van de Opdrachtgever besproken. De zaken die zich hebben voorgedaan komen maandelijks in de incidentrapportage terug.
- Documentatie en Analyse: Documentatie van alle incidenten, inclusief het verloop van de gebeurtenis, de respons en de lessen die zijn geleerd.

3.12.4. Opleiding en Bewustwording

- Training: Regelmatige beveiligingstrainingen voor personeel over best practices, phishing-detectie, en andere relevante onderwerpen.

- Bewustwordingscampagnes: Initiatieven om het beveiligingsbewustzijn binnen de organisatie te vergroten.
- Opdrachtnemer rapport hier jaarlijks over: een jaarkalender (vooraf) en een rapportage over wat er daadwerkelijk is gedaan en wat de score is (achteraf).

3.12.5. Beheer en Evaluatie

- Regelmatige audits: Uitvoeren van periodieke beveiligingsaudits zoals de Microsoft Secure Score (minimaal: ISO 27001, Baseline Informatiebeveiliging Overheid) om de effectiviteit van de procedures te evalueren en verbeterpunten te identificeren.
- Herziening van procedures: Jaarlijkse herziening van beveiligingsprocedures en -beleid om te voldoen aan veranderende bedreigingen en technologische ontwikkelingen.

3.13. IDU (In Dienst / Uit Dienst)

3.13.1. Instroom (Onboarding)

Opdrachtgever heeft een onboarding proces. Opdrachtnemer maakt uiteindelijk op basis van specificaties vanuit Opdrachtgever een nieuw account aan. Deze worden gekoppeld aan licenties en applicaties. Dit gebeurt via het service request proces.

3.13.2. Doorstroom

Opdrachtnemer maakt op basis van specificaties vanuit Opdrachtgever de gevraagde wijzigingen aan in het account. Dit gebeurt via het service request proces.

3.13.3. Uitstroom (Offboarding)

Opdrachtgever heeft een offboarding proces. Opdrachtnemer zet uiteindelijk op basis van de specificaties vanuit Opdrachtgever het account op inactief.
Gedurende de drie maanden na de inactief-datum blijft het account en de gegevens bewaard.
Na drie maanden wordt het account en de gegevens definitief gewist door Opdrachtnemer.
In de servicemanagement-rapportage wordt door de Opdrachtnemer een overzicht van verwijderde accounts aangeleverd.

3.14. Back-up oplossing

Opdrachtnemer maakt gebruik van een back-up oplossing waarbij voor Opdrachtgever van belang is dat te allen tijde gewaarborgd is:

- De integriteit en beschikbaarheid van gegevens.
- Een effectieve en snelle hersteltijd na een gegevensverliesincident.
- Voldoen aan wettelijke en compliance-eisen met betrekking tot gegevensbeheer.

Deze back-up oplossing wordt toegepast op alle systemen, applicaties en gegevens die in beheer zijn bij Opdrachtnemer.

De back-up oplossing kan er als volgt uit zien:

Dagelijkse werkdag back-ups
Frequentie: Elke werkdag (maandag t/m vrijdag).
Type: Volledige back-up op maandag en de andere dagen een incrementele back-up.
Doel: Back-up van alle gewijzigde bestanden en databases sinds de laatste volledige back-up.
Bewaarperiode: 7 werkdagen (de meest recente back-ups van de afgelopen week zijn 7 werkdagen beschikbaar). Voorbeeld: De back-up van maandag 1/1 wordt op woensdag 10/1 overschreven.
Opslaglocatie: Cloud en/of lokaal.
Opslagwijze: de back-ups worden versleuteld en niet-wijzigbaar (“immutable”) voor 7 werkdagen opgeslagen.

Wekelijkse back-ups
Frequentie: Elke vrijdagnacht (of een andere overeengekomen dag van de week).
Type: Volledige back-up.
Doel: Volledige back-up van alle gegevens.
Bewaarperiode: 4 weken (1 back-up per week).
Opslaglocatie: Cloud en/of lokaal.
Opslagwijze: de back-ups worden versleuteld en niet-wijzigbaar ("immutable") voor 4 weken opgeslagen.

Maandelijkse back-ups
Frequentie: Elke laatste dag van de maand.
Type: Volledige back-up.
Doel: Een volledige back-up van alle gegevens en systemen.
Bewaarperiode: 12 maanden (1 back-up per maand).
Opslaglocatie: Lokaal, in de cloud en op offline opslagmedia.
Opslagwijze: de back-ups worden versleuteld en niet-wijzigbaar ("immutable") voor 12 maanden opgeslagen.

Kwartaal back-ups
Frequentie: Elke laatste dag van elk kwartaal (31 maart, 30 juni, 30 september, 31 december).
Type: Volledige back-up.
Doel: Een volledige back-up van alle gegevens.
Bewaarperiode: 2 jaar (1 back-up per kwartaal).
Opslaglocatie: Cloud en/of lokaal.
Opslagwijze: de back-ups worden versleuteld en niet-wijzigbaar ("immutable") voor 2 jaar opgeslagen.

Jaarlijkse back-ups
Frequentie: Elke laatste dag van het jaar (31 december).
Type: Volledige back-up.
Doel: Volledige back-up van alle gegevens voor archivering en compliance.
Bewaarperiode: 7 jaar (1 back-up per jaar, afhankelijk van wettelijke vereisten).
Opslaglocatie: Lokaal, in de cloud, op externe opslagmedia en in een beveiligde archiefruimte.
Bewaarperiode: Afhankelijk van het beleid (bijv. 30 dagen tot 1 jaar).
Opslaglocatie: Cloudopslag met immutability-functionaliteit of gespecialiseerde back-up-systemen.
Opslagwijze: de back-ups worden versleuteld en niet-wijzigbaar ("immutable") voor 7 jaar opgeslagen.

Back-up beveiliging
- Back-ups dienen dagelijks te worden gecontroleerd.
- Alle back-upbestanden worden met de sleutel van de Opdrachtgever versleuteld, zowel in transit als in rust om gegevensintegriteit en privacy te waarborgen.
- Er wordt rolgebaseerd toegangsbeheer toegepast.
- De back-ups worden buiten het domein van Opdrachtgever bewaard.
- Gebruik Azure Active Directory (AAD) voor geavanceerd toegangsbeheer en multi-factor authenticatie (MFA) om de toegang tot de databases te beveiligen.
- De maximaal toegestane dataverlies (RPO) is conform SLA.

Recovery & restore procedures
- Alle recovery & restore procedures zijn door Opdrachtnemer gedocumenteerd, inclusief stap-voor-stap instructies voor elk type herstelscenario.
- Recovery procedures worden minimaal op jaarbasis getest.
- De restore procedure wordt minimaal jaarlijks of na een grote wijziging getest.

- De maximale tijd die een restore in beslag mag nemen (RTO), is conform SLA.

Monitoren back-ups en restore

- Van back-up en recovery activiteiten en de verblijfplaats van de media wordt een logboek bijgehouden.
- Toegang tot de back-ups wordt in een auditlog bijgehouden;
- Mislukte back-ups worden binnen 4 uur gesignaleerd, de oorzaak geanalyseerd en corrigerende acties uitgevoerd.
- Een uitgevoerde restore wordt getest op:
    - Toegankelijkheid, kunnen de juiste mensen er daadwerkelijk bij;
    - Werking, kunnen de juiste mensen hun werkzaamheden uitvoeren.

3.15. Onderhoud

Onderhoud vindt doorgaans plaats tijdens het Onderhoudsvenster zoals gedefinieerd in de SLA. Opdrachtgever wordt niet vooraf of achteraf geïnformeerd welk onderhoud wordt/is uitgevoerd. Het is mogelijk dat de producten en diensten tijdens het onderhoud geheel of gedeeltelijk niet beschikbaar zijn voor Opdrachtgever. Na afloop van het onderhoudsvenster zijn de producten en diensten altijd weer beschikbaar conform KPI's en afspraken.

Wanneer Opdrachtnemer het noodzakelijk acht, kan Opdrachtnemer ad hoc onderhoud inplannen buiten het Onderhoudsvenster. Opdrachtgever wordt hier conform SLA over geïnformeerd. Een bericht van ad hoc onderhoud zal de volgende informatie bevatten:
1. een onderbouwing voor het inplannen van ad hoc onderhoud en waarom dit niet tijdens het Onderhoudsvenster uitgevoerd kan worden;
2. het tijdskader waarin het ad hoc onderhoud zal plaatsvinden;
3. de verwachte feitelijke duur van het ad hoc onderhoud;
4. de producten en/of diensten waarop het ad hoc onderhoud van invloed zal zijn.

Onderhoud op projectbasis wordt gezamenlijk door beide partijen ingepland.

3.16. Exitstrategie

De exitstrategie is essentieel voor het soepel beëindigen van een contract en het overdragen van verantwoordelijkheden, producten, diensten en data.
Opdrachtnemer heeft een exitplan opgeleverd aan Opdrachtgever. Deze bevat de volgende onderdelen:

Beëindigingscriteria en -voorwaarden

- De redenen voor beëindiging: Een duidelijke beschrijving van de omstandigheden waaronder de overeenkomst kan worden beëindigd, zoals de afloop van de contractperiode of niet-naleving van contractuele afspraken.
- Opzegtermijn: Conform Raamovereenkomst.
- Datum van beëindiging: De datum waarop Opdrachtnemer formeel stopt met de levering van haar diensten aan Opdrachtgever.

Mogelijke beëindigingskosten

- Financieel overzicht: Geeft alle kosten weer die optreden tijdens het beëindigen van de overeenkomst, zoals administratieve kosten en/of kosten voor het overdragen van de producten, diensten en data.

Overdrachtsplan

- Overdracht van producten en diensten: Bevat een overzicht van alle producten en diensten die overgedragen gaan worden, en bevat ook procedures voor het overdragen van deze producten en diensten.

- Overdracht van data: Bevat een overzicht van alle data die overgedragen gaan worden, en bevat ook procedures voor het overdragen van alle data, inclusief het formaat en de beveiliging van de gegevens.
- Planning: Geeft de tijdslijnen weer waarop de overdracht van producten, diensten en data plaatsvindt.
- Eigendom van de gegevens: Beschrijving van eigenaarschap van alle gegevens tijdens en na overdracht.
- Opdrachtnemer geeft aan hoe vertrouwelijke informatie wordt behandeld tijdens en na de overdrachtsperiode.
- Opdrachtnemer zorgt voor de veilige vernietiging of overdracht van vertrouwelijke informatie.

Servicecontinuïteit en ondersteuning tijdens de overdrachtsperiode

- Beschrijft hoe Opdrachtnemer zorgdraagt voor continuering van de dienstverlening tijdens de overdrachtsperiode, tot aan de formele beëindiging van het contract.
- Beschrijft de extra ondersteuning tijdens de overdrachtsperiode: Opdrachtnemer maakt duidelijk welke extra ondersteuning wordt geboden tijdens de overgangsperiode.
- Beschrijft de tijdelijke diensten (indien nodig): De noodzakelijke tijdelijke diensten die ervoor zorgen dat Opdrachtgever geen onderbreking van service ervaart tijdens de overgangsperiode.

Risico's/Herstelscenario's

- Risico's: Opdrachtnemer brengt in beeld welke risico's er zijn bij de overdracht en welke mitigerende maatregelen genomen kunnen worden.
- Herstelscenario's: Opdrachtnemer heeft herstelscenario's opgesteld, voor het geval er zich problemen voordoen tijdens de overdracht (bijvoorbeeld verlies van data of dienstonderbrekingen).
- Herstelwerkzaamheden: In het geval van een mislukte overgang waarbij dit aantoonbaar aan Opdrachtnemer heeft gelegen, voert Opdrachtnemer kosteloos herstelwerkzaamheden uit.

Nazorg

- Opdrachtnemer beschrijft de nazorg en de duur van de nazorgperiode: Een periode ná de beëindiging van het contract waarin Opdrachtnemer nog nazorgdiensten levert, zoals het beantwoorden van vragen of het verhelpen van problemen die zich na overdracht kunnen voordoen.

Verantwoordelijkheden van Opdrachtgever

- Hoe Opdrachtgever kan bijdragen aan een zo soepel mogelijk lopende beëindiging.

Opdrachtgever kan dit plan goedkeuren of afwijzen. Wanneer Opdrachtgever het plan afwijst, moet hij dit doen met een duidelijke en concrete onderbouwing. Daarnaast dient Opdrachtnemer een verbeterplan in te dienen binnen 14 werkdagen.

4. Samenwerking

4.1. Team & rollen

Opdrachtnemer werkt met een vast team van professionals voor Opdrachtgever die volledig bekend zijn met de technische omgeving van Opdrachtgever.

Opdrachtnemer wijst op operationeel, tactisch en strategisch niveau rollen aan die fungeren als vast aanspreekpunt voor Opdrachtgever.

Er wordt gezorgd voor adequate en tijdige vervanging bij afwezigheid.

Het vaste team inclusief rollen en contactpersonen is beschreven in Bijlage 1 Communicatiematrix van dit DAP. Personele wijzigingen worden in Bijlage 1 aangepast en in het tactisch overleg door beide partijen ondertekend.

4.2. Overlegstructuur

Nadere invulling van de overlegstructuur (agendering en deelnemers) wordt in overleg tussen Opdrachtgever en Opdrachtnemer bepaald.

Operationeel overleg
Er zal minimaal 1x per week een overleg op operationeel niveau plaatsvinden. In dit overleg worden alle (langdurig) openstaande tickets besproken, en worden acties hierover afgesproken.

Tactisch overleg
Er zal 1x per maand een overleg op tactisch niveau plaatsvinden, om de samenwerking te evalueren en de kwaliteit van de dienstverlening te bespreken.
De te agenderen punten zijn bijvoorbeeld:

- Aantal actieve gebruikers geldend voor de kalendermaand.
- Bijzonderheden uit de servicemanagement-rapportages van het afgelopen kwartaal.
- Uitvoeren/evalueren van lopende SIP (zie paragraaf 4.3).
- Uitvoeren/evalueren van het klanttevredenheidsonderzoek (zie paragraaf 4.4).
- Uitvoeren/evalueren van audits (zie paragraaf 4.5).
- Eventuele bijzonderheden rondom opdrachtverlening en facturatie.
- Voorgestelde aanvullingen en/of wijzigingen aan het DAP.
- Actualisatie van het exit-plan (eens per half jaar).
- Andere optimalisatie-mogelijkheden van de dienstverlening.
- Een vooruitblik naar het volgende kwartaal.

Strategisch overleg
Er zal minimaal 1x per jaar een overleg op strategisch niveau plaatsvinden.
De te agenderen punten zijn bijvoorbeeld:

- Monitoring van de uitnutting van het contract.
- Monitoring van de samenwerking.
- Strategische ontwikkelingen die invloed hebben op de organisatie en/of het contract.
- Marktontwikkelingen en innovaties.

4.3. Service Improvement Plan (SIP)

Informatie over wel of niet behaalde KPI's is inzichtelijk in de servicemanagement-rapportages en in een portaal (bijvoorbeeld het service management systeem). Opdrachtnemer signaleert proactief richting Opdrachtgever wanneer KPI's niet worden gehaald. Op dat moment initieert Opdrachtnemer een gesprek met Opdrachtgever. Er kan dan besloten worden om het SIP in te zetten. Het SIP is een hulpmiddel om de kwaliteit van de dienstverlening te verbeteren. Het SIP wordt door Opdrachtnemer opgesteld en door Opdrachtgever geaccordeerd. Vervolgens voert Opdrachtnemer het plan uit zoals beschreven, en rapporteert hierover aan de servicemanager van Opdrachtgever en in het tactisch overleg.
Het SIP bevat minimaal:

- **Huidige situatie**: Een analyse van de huidige prestaties en de geïdentificeerde problemen of zwakke punten.
- **Doelen**: Een beschrijving van de benodigde verbeteringen, zo specifiek en concreet mogelijk.

- **Acties**: Concrete stappen en maatregelen die genomen moeten worden om de doelen te realiseren.
- **Verantwoordelijkheden**: Een beschrijving van de verantwoordelijkheden voor de uitvoering van (onderdelen van) het plan. Dit zorgt voor eigenaarschap over de te nemen acties.
- **Planning**: Weergave van de tijdslijnen en deadlines van alle acties. Dit zorgt voor een realistische planning en houdt het plan op koers.
- **Metingen en beoordeling**: Een beschrijving van hoe succes wordt gemeten. Bijvoorbeeld door het (opnieuw) meten van de KPI's. Als het resultaat door Opdrachtgever als voldoende en consistent wordt beschouwd, wordt het SIP afgerond.

Indien het gewenste succes niet behaald is en Opdrachtgever hierover negatief beoordeelt, krijgt Opdrachtnemer de mogelijkheid om een nieuw of aangepast SIP op te stellen en uit te voeren. Mocht na driemaal schriftelijk beoordelen door Opdrachtgever nog steeds niet voldoende en consistente verbetering zichtbaar zijn, dan heeft Opdrachtgever de mogelijkheid om de procedure voor ontbinding van de Overeenkomst te starten.

4.4. Klanttevredenheidsonderzoek

De survey voor het klanttevredenheidsonderzoek wordt opgesteld door Opdrachtgever. Opdrachtgever bepaalt hoeveel en welke medewerkers gevraagd worden om het onderzoek in te vullen.
Mocht Opdrachtnemer te laag scoren, dan wordt het SIP ingezet (zie paragraaf 4.3).

4.5. Audits

Opdrachtnemer verleent medewerking bij de uitvoering van mogelijke periodieke interne en externe audits.

4.6. Escalatieladder

Het uitgangspunt is dat Opdrachtgever en Opdrachtnemer met de communicatiematrix (Bijlage 1 van dit DAP) werken, waarbij elke rol binnen elk niveau aan beide kanten een aanspreekpunt heeft, en waarbij regelmatig overleg plaatsvindt om mogelijke problemen vroegtijdig op te pakken en zonder escalatie in goede banen te leiden.

Echter kan het voorkomen dat een probleem niet binnen het eigen niveau opgelost kan worden, bijvoorbeeld door beperkingen in bevoegdheden, kennis/ervaring of doorlooptijd. Een duidelijke escalatieladder, met korte en directe communicatielijnen, zorgt ervoor dat er een constructieve samenwerking blijft tussen Opdrachtgever en Opdrachtnemer, wanneer een probleem op een hoger niveau moet worden opgelost.
In de tabel hieronder zijn verschillende escalatieniveaus zichtbaar. De direct betrokkenen informeren elkaar schriftelijk over de keuze voor escalatie.

Niveau	Type probleem	Acties	Betrokkenen Opdrachtgever	Betrokkenen Opdrachtnemer
1	Kleine routinematige problemen die binnen de bevoegdheid en kennis van de medewerker vallen.	Zelf oplossen. Escaleren naar niveau 2 als doorlooptijd overschreden wordt of als andere afspraken niet worden nageleefd.	Functioneel beheerder KA	
2	Problemen die kennis/bevoegdheden van de eerste lijn overschrijden, maar nog beheersbaar zijn.	Er wordt eventueel meer specialistische kennis of ervaring ingeschakeld. Escaleren naar niveau 3 als de doorlooptijd overschreden wordt of als het probleem met	Servicemanager	

		extra hulp niet kan worden opgelost.		
3	Complexe problemen die de normale dienstverlening verstoren.	Het probleem wordt diepgaand onderzocht en er wordt gezocht naar een oplossing. Mogelijk is er samenwerking met andere afdelingen nodig. Escaleren naar niveau 4 als het probleem een te brede impact krijgt op de bedrijfsvoering of als er geen oplossing binnen dit niveau beschikbaar is.	Coördinator KA (in samenspraak met de Servicemanager)	
4	Kritieke problemen die de bedrijfscontinuïteit bedreigen of aanzienlijke impact hebben op de reputatie of financiën van Opdrachtgever.	Er wordt direct actie ondernemen door het management. Eventueel wordt crisismanagement opgestart. Het probleem blijft op dit niveau tot er een oplossing is voor het probleem.	Manager bedrijfsvoering	

Bijlage 1: Communicatiematrix

Rollen Opdrachtgever

Functie (A-Z)	Naam	Contactgegevens
Adviseur facilitaire zaken		
Chief Information Security Officer		
Contractmanager		
Coördinator KA		
Functioneel beheerder KA		
Information Security Officer		
Inkoop		
Manager Bedrijfsvoering		
Servicemanager		
Systeembeheerder ICT		
Technisch beheerder KA		

Rollen Opdrachtnemer

Nog in te vullen.

Functie	Naam	Gegevens

Communicatiematrix

Onderwerp	Opdrachtgever	Opdrachtnemer
Ondersteuning bij meldingen/tickets	Functioneel beheerder KA	
Infrastructuur, netwerk, werkomgeving	Technisch beheerder KA	
Informatiebeveiliging	Information Security Officer (ISO) Chief Information Security Officer (CISO)	
Privacy	Privacy officer	
SLA, DAP en servicemanagementrapportage	Servicemanager	
Scope van de dienstverlening (toename of afname van producten en/of diensten)	Manager Bedrijfsvoering Coördinator KA	
Uitnutting van het contract	Contractmanager	
Opdrachtverlening en facturatie	Inkoop	
Opdrachtverlening/Budget/Financiën	Coördinator KA	
Facilitair (fysieke werkvloer)	Adviseur facilitaire zaken	