

Bijlage 12 - Concept¹ Dossier Afspraken en Procedures (DAP): *Cloudplatform-dienstverlening*

KB, nationale bibliotheek

juli, 2026

X

Opdrachtnemer [NAAM]
[FUNCTIE]

X

Opdrachtnemer [NAAM]
[FUNCTIE]

KB } nationale
bibliotheek

¹Dit document wordt door Opdrachtgever verstrekt als DAP-skelet en referentiekader bij de aanbestedingsstukken. Het doel is inschrijvers inzicht te geven in de gewenste operationele werkafspraken, overlegstructuur, rollen, escalaties, mandaten, tooling, registratie, kennisoverdracht, transitie en uitvoeringsprocessen. Inschrijver hoeft de structuur van dit DAP-skelet niet één-op-één over te nemen. Inschrijver dient in de inschrijving wel expliciet aan te geven hoe zijn aanpak aansluit op dit referentiekader en waar hij afwijkt of een alternatief voorstelt.

Afwijkingen of alternatieven worden expliciet, gemotiveerd en toetsbaar opgenomen in de inschrijving en compliancematrix, inclusief de impact voor Opdrachtgever. Afwijkingen of alternatieven mogen niet afdoen aan de minimale randvoorwaarden zoals opgenomen in het Programma van Eisen.

De DAP wordt tijdens de transitie gezamenlijk ingevuld door Opdrachtgever en Opdrachtnemer. De definitieve DAP wordt uiterlijk vóór overgang naar steady-state dienstverlening door Opdrachtgever goedgekeurd.

De DAP is een operationele uitwerking van de Overeenkomst, het Programma van Eisen, de SLA en het Exit-plan. De DAP kan deze documenten niet wijzigen, beperken of buiten werking stellen.

1	Algemeen	4
1.1	Doel	4
1.2	Begrippen	4
1.3	Uitgangspunten	4
1.4	Juridisch en normatief kader	Fout! Bladwijzer niet gedefinieerd.
2	Rollen en verantwoordelijkheden	5
2.1	Rollen Opdrachtgever	5
2.2	Rollen Opdrachtnemer	5
2.3	RACI	6
3	Overlegstructuur	7
4	Tooling en registratie	7
4.1	Tooling	7
4.2	Registratieverplichtingen	8
5	Servicevensters	8
5.1	Kantooruren	8
5.2	Buiten kantooruren	9
5.3	Activiteitenmatrix per servicevenster	10
6	Incidentmanagement	11
6.1	Proces	11
6.2	Prioritering	11
6.3	Overdracht incidenten buiten kantooruren	11
7	Major incident management	12
8	Problemmanagement	12
8.1	Problemmanagement tijdens kantooruren	12
8.2	Problemmanagement buiten kantooruren	13
8.3	Signalering en opvolging	13
9	Change enablement	14
9.1	Uitgangspunten	14

9.2	Typen changes	14
9.3	Definition of Done	15
10	Access management	15
11	Werkwijze gezamenlijk platformteam	16
11.1	Architectuur	16
11.2	Criteria voor platformcomponenten	16
11.3	Soevereiniteit en autonomie	17
11.4	Manier van werken	17
11.5	Security	17
12	Buiten-kantoor tijden ondersteuning en mandaatmatrix	18
12.1	Mandaatmatrix	18
12.2	Minimale informatiepositie buiten kantooruren	19
12.3	Kennisborging achtervang medewerkers	20
13	Monitoring en eventmanagement	20
14	Rapportage	20
15	Kennisoverdracht, documentatie en overdraagbaarheid	21
16	Security en compliance	22
16.1	Certificeringen	22
16.2	Privacy en gegevensbescherming	22
17	Implementatieperiode en acceptatie reguliere dienstverlening	23
18	Beheer van de DAP	23
19	Bijlagen	25
19.1	Contactmatrix en escalatiegegevens	25

Versie	Datum	Auteur	Status	Wijzigingen
0.1	02-07-2026	Opdrachtgever	Concept	Eerste versie bij aanbestedingsstukken
0.2	[invullen]	Opdrachtgever	Concept	Verwerking Nota van Inlichtingen
1.0	[invullen]	Opdrachtgever / Opdrachtnemer	Definitief	Definitieve versie vóór overgang naar reguliere dienstverlening

1 Algemeen

1.1 Doel

De DAP beschrijft de dagelijkse operationele samenwerking tussen Opdrachtgever en Opdrachtnemer voor de dienstverlening rond de cloudplatform-dienstverlening.

De DAP bevat afspraken over rollen, contactpersonen, tooling, processen, rapportages, overlegstructuur, escalatie, communicatie, mandaten, kennisoverdracht, informatiebeveiliging, compliance, transitie en exit.

In de aanbestedingsfase fungeert dit DAP-skelet als referentiekader en minimale structuur voor de gewenste operationele samenwerking. De definitieve DAP wordt tijdens de implementatieperiode gezamenlijk uitgewerkt en vóór overgang naar reguliere dienstverlening door Opdrachtgever goedgekeurd.

1.2 Begrippen

Op deze DAP zijn de begrippen en definities van toepassing zoals opgenomen in Bijlage 10 Begrippenlijst SLA, DAP en Exit-plan Cloudplatformdienstverlening. Voor zover in dit Exit-plan aanvullende begrippen zijn opgenomen, gelden deze uitsluitend voor de uitleg en uitvoering van dit Exit-plan. Documentspecifieke aanvullingen mogen de Begrippenlijst SLA, DAP en Exit-plan niet wijzigen, maar kunnen begrippen nader operationaliseren voor exit, overdracht en beëindiging.

1.3 Uitgangspunten

Voor de DAP gelden de volgende uitgangspunten. De uitgangspunten 1 tot en met 8 gelden als minimale randvoorwaarden voor de operationele samenwerking. Afwijkingen of alternatieven van inschrijver mogen niet afdoen aan deze minimale randvoorwaarden, tenzij Opdrachtgever dit uitdrukkelijk accepteert.

1. Opdrachtgever behoudt regie op prioritering, risicoacceptatie, architectuurkaders, governance, servicekwaliteit, stakeholdercommunicatie en acceptatie van opleveringen.
2. Opdrachtnemer werkt als onderdeel van het geïntegreerde cloudplatformteam en richt de dienstverlening niet in als ondoorzichtige black-box beheerconstructie.
3. Opdrachtnemer werkt in de door Opdrachtgever aangewezen of goedgekeurde tooling, tenzij Opdrachtgever schriftelijk anders akkoord gaat.
4. Operationele werkzaamheden, besluiten, incidenten, wijzigingen, afwijkingen, herstelacties en overdrachtsinformatie worden herleidbaar, controleerbaar en overdraagbaar geregistreerd.
5. Kennisoverdracht, documentatie, runbooks en overdrachtsinformatie zijn structurele onderdelen van de dagelijkse werkwijze.
6. Buiten-kantoortijden ondersteuning vindt plaats binnen hetzelfde operationele model als de dienstverlening tijdens kantooruren, binnen dezelfde registratie-, rapportage-, overdrachts- en escalatiekaders en binnen een door Opdrachtgever goedgekeurde mandaatmatrix.
7. De DAP, RACI, mandaatmatrix, contactmatrix en escalatiematrix worden periodiek geëvalueerd en bij relevante wijzigingen geactualiseerd.

8. Wijziging van de DAP, RACI, mandaatmatrix, contactmatrix of escalatiematrix kan nooit leiden tot wijziging, beperking of buitenwerkingstelling van contractuele verplichtingen zonder formele wijzigingsprocedure.

Eisen die voortkomen uit informatiebeveiliging, privacy, kwaliteit, compliance, audit of wet- en regelgeving worden, voor zover relevant voor de operationele uitvoering, vertaald naar rollen, processen, registraties, rapportages, escalaties, mandaten en werkafspraken in de DAP.

2 Rollen en verantwoordelijkheden

2.1 Rollen Opdrachtgever

Rol	Verantwoordelijkheid
Product Owner Cloudplatform	Prioritering, roadmap, waarde en afstemming met organisatie
Servicemanager Opdrachtgever	SLA, DAP, service reviews, rapportages, operationele governance
Cloud Platform Engineers Opdrachtgever	Technische regie, laC-review, kennisborging, platformkwaliteit
Architectuur	Architectuurkaders, portabiliteit, ontwerpprincipes, technische besluitvorming
Security/CISO	Securitykaders, risicoadvies, baselines, compliance en audit
Privacy Officer/FG	Privacytoetsing indien persoonsgegevens of verwerkingen geraakt worden
Contractmanager	Contractbewaking, formele escalatie, wijzigingen en leveranciersprestaties
IT Operations/Service desk	Aansluiting operationele processen en gebruikerscommunicatie
DevOps-/Applicatieteams	Afnemers van platformdiensten, feedback en functionele impact

2.2 Rollen Opdrachtnemer

Rol	Verantwoordelijkheid
Service Delivery Manager	Servicekwaliteit, rapportage, escalaties, service review en verbeteringen. De SDM coördineert de inbreng van Opdrachtnemer zonder de regiefunctie van de Servicemanager van Opdrachtgever over te nemen.
Cloud Platform Engineer(s)	Beheer en doorontwikkeling binnen geïntegreerd team
Azure Architect/Specialist	Specialistisch advies over Azure, landing zones, governance en optimalisatie
Security Specialist	Securityadvies, findings, baselines, compliance en incidentondersteuning
17x7 achtervang/on-call	Incidentrespons, containment, herstel binnen mandaat en escalatie buiten kantooruren
Implementatiemanager	Inrichting implementatieperiode, overdracht, planning en acceptatie
Exitmanager	Coördinatie Exit-plan, overdraagbaarheid en exit readiness

2.3 RACI

De definitieve RACI wordt tijdens de implementatieperiode gezamenlijk uitgewerkt en als bijlage bij deze DAP opgenomen. De RACI wordt uiterlijk vóór overgang naar reguliere dienstverlening door Opdrachtgever goedgekeurd.

Een globale rolverdeling op hoofdniveau is onvoldoende. De RACI wordt uitgewerkt op een zodanig niveau dat per relevant proces of activiteit duidelijk is:

1. welke rol uitvoert;
2. welke rol besluit of eindverantwoordelijk is;
3. welke rollen worden geraadpleegd;
4. welke rollen worden geïnformeerd;
5. wanneer escalatie of goedkeuring door Opdrachtgever nodig is.

De RACI bevat minimaal verantwoordelijkheden voor:

1. incidentmanagement;
2. major incident management;
3. problemmanagement;
4. wijzigingen;
5. service requests;
6. monitoring, indien van toepassing;
7. rapportage;
8. service reviews;
9. kennisoverdracht;
10. documentatie;
11. buiten-kantoor tijden ondersteuning;
12. implementatieperiode;
13. exit en overdracht.

De RACI kan de Overeenkomst, het Programma van Eisen, de SLA, het Exit-plan of deze DAP niet wijzigen, beperken of buiten werking stellen.

2.3.1 Scope van de dienstverlening van het gezamenlijk platformteam

- Beheer van alle resources in de Azure platform landingzone
- Beheer van gedeelde platformdiensten zoals gedeelde application gateways, een containerplatform of API-management platform
- Borgen van security en compliance via Azure policies, netwerkisolatie, secrets, en lifecycle management
- Kosten en performance optimalisatie, inzicht en sturing op gebruik van platformdiensten
- Aanmaken, updaten en verwijderen van applicatie landingzones
- Enablen van ondersteunende workload-functionaliteit zoals back-up, monitoring, DNS, certificaten etc.

3 Overlegstructuur

De primaire operationele afstemming binnen het geïntegreerde cloudplatformteam vindt plaats via agile ceremonies, waaronder stand-ups, refinement, sprintplanning, reviews en retrospectives. Deze vormen de kern van de dagelijkse samenwerking en operationele besluitvorming. De hieronder beschreven overlegstructuur is aanvullend en is gericht op governance, rapportage, escalatie en continue verbetering. Deze overlegstructuur vervangt de dagelijkse operationele sturing via backlog en sprintcyclus niet.

Overleg	Frequentie	Deelnemers	Doel	Output
Service review	[maandelijks]	Service Manager KB, contactpersoon leverancier	SLA, rapportage, trends, verbeteringen	Serviceraapport en SIP
Tactisch overleg	[per kwartaal]	Service Manager KB, Product Owner/Product manager KB, accountmanager leverancier	Governance, risico's, escalaties, security, kosten	Besluiten en acties
Strategisch overleg	[jaarlijks]	Domeineigenaar Infra, Management leverancier	Contract, verlenging, strategie, security	Evaluatie
Exit-readiness review	[minimaal jaarlijks]	Service Manager KB, Product Owner/Productmanager KB, contactpersoon leverancier	Overdraagbaarheid toetsen	Exit-readinessrapport

De DAP bevat escalatiecriteria voor operationele, tactische en strategische escalatie. Deze escalatiecriteria gelden niet alleen voor incidenten, maar ook voor structurele prestatieafwijkingen, terugkerende knelpunten, niet-nagekomen afspraken, samenwerkingsissues, openstaande risico's en contractuele aandachtspunten.

4 Tooling en registratie

4.1 Tooling

Opdrachtnemer werkt in de door Opdrachtgever aangewezen tooling voor minimaal:

1. incidenten;
2. problems;
3. changes;
4. service requests;
5. documentatie;
6. repositories;
7. monitoring;
8. logging;
9. rapportage;
10. communicatie;
11. besluitvorming;

12. exitdocumentatie.

Afwijking van tooling is uitsluitend toegestaan na voorafgaande schriftelijke goedkeuring door Opdrachtgever.

4.2 Registratieverplichtingen

Alle werkzaamheden, besluiten, afwijkingen, wijzigingen, incidenten, herstelacties en overdrachtsinformatie worden zodanig geregistreerd dat deze herleidbaar, controleerbaar en overdraagbaar zijn.

De gezamenlijke backlog wordt beheerd in de door Opdrachtgever aangewezen tooling en vormt de centrale bron voor planning, voortgang, prioritering en rapportage binnen het geïntegreerde cloudplatformteam.

Alle relevante werkzaamheden, waaronder incidenten, changes, problems en service requests, zijn herleidbaar tot backlog-items of gerelateerde registraties in de overeengekomen tooling.

Registratie ondersteunt de agile werkwijze en mag geen onnodige belemmering vormen voor de flow van het team. Registratieverplichtingen laten onverlet dat werkzaamheden, besluiten, afwijkingen, herstelacties en overdrachtsinformatie voldoende herleidbaar, controleerbaar en overdraagbaar moeten blijven.

Registratie in de overeengekomen tooling is randvoorwaardelijk voor regie, rapportage, kennisborging, auditbaarheid en exit. Werkzaamheden of besluiten die niet zijn geregistreerd, worden niet beschouwd als volledig overdraagbaar of controleerbaar, tenzij Opdrachtgever schriftelijk anders akkoord gaat.

5 Servicevensters

5.1 Kantooruren

Onder kantooruren wordt verstaan: maandag tot en met vrijdag van 09:00 tot 17:00 uur Nederlandse tijd.

Tijdens kantooruren vindt de geïntegreerde teamdienstverlening plaats, waaronder beheer, doorontwikkeling, changes, service requests, overleg, kennisoverdracht, structurele analyse en verbetering.

Medewerkers van Opdrachtnemer zijn minimaal twee vaste werkdagen per week aanwezig op de locatie van Opdrachtgever te Den Haag. De exacte aanwezigheidsdagen worden bij aanvang van de implementatieperiode in onderling overleg vastgesteld en schriftelijk vastgelegd.

5.2 Buiten kantooruren

Voor deze DAP gelden de volgende servicevensters buiten kantooruren:

1. maandag tot en met vrijdag van 06:00 tot 09:00 uur en van 17:00 tot 23:00 uur Nederlandse tijd;
2. zaterdag, zondag en feestdagen van 06:00 tot 23:00 uur Nederlandse tijd.

Opdrachtnemer is verantwoordelijk voor het organiseren van de benodigde bezetting, achtervang en bereikbaarheid binnen deze buiten-kantoortijden. De wijze waarop Opdrachtnemer dit intern organiseert, waaronder de inzet van teamleden, achtervang of stand-by capaciteit, laat de overeengekomen service levels, mandaten, escalatieafspraken en overdrachtsverplichtingen onverlet.

Buiten kantooruren is de dienstverlening primair gericht op monitoring, incidentrespons, containment, herstel binnen mandaat, escalatie en overdracht.

Buiten-kantoortijden ondersteuning is geen zelfstandige beheerlaag, geen parallelle besluitvormingsstructuur en geen vervanging van het geïntegreerde cloudplatformteam.

5.3 Activiteitenmatrix per servicevenster

Activiteit	Kantooruren	Buiten kantooruren
Reguliere platformdoorontwikkeling	Ja	Nee
IaC-wijzigingen via pull request	Ja	Alleen emergency change of vooraf goedgekeurd
Standaard changes	Ja	Nee, tenzij vooraf ingepland
Emergency changes	Ja	Ja, conform emergency changeproces
Incidentrespons P1	Ja	Ja
Incidentrespons P2	Ja	Ja, indien binnen scope
Incidentrespons P3/P4	Ja	Nee, tenzij Opdrachtgever expliciet escaleert
Problemmanagement	Ja	Nee, alleen signalering/vastlegging
Root cause analysis	Ja	Nee, voorbereiding mogelijk
Service requests	Ja	Nee
Access requests	Ja	Alleen noodtoegang conform mandaat
Security containment	Ja	Ja, binnen mandaat
Structurele securityverbeteringen	Ja	Nee, tenzij emergency
Monitoring alerts beoordelen	Ja	Ja, voor overeengekomen alerts
Stakeholdercommunicatie	Ja, regie Opdrachtgever	Alleen conform major incidentproces
Documentatie bijwerken	Ja	Alleen minimale overdracht; structurele update tijdens kantooruren
Kennisoverdracht	Ja	Nee
Exitactiviteiten	Ja	Alleen bij urgente continuïteits- of overdrachtsrisico's

6 Incidentmanagement

Incidentmanagement wordt uitgevoerd binnen het geïntegreerde cloudplatformteam en, buiten kantooruren, door de achtervang van Opdrachtnemer binnen de kaders van deze DAP, de SLA en de mandaatmatrix.

Tijdens kantooruren ligt incidentafhandeling bij het geïntegreerde cloudplatformteam onder regie van Opdrachtgever. Incidenten worden waar passend opgenomen in de backlog of sprintcyclus. Het door Opdrachtnemer geleverde teamlid draagt hieraan bij als onderdeel van het geïntegreerde cloudplatformteam, binnen de overeengekomen inzet, expertise en werkwijze.

Buiten kantooruren is de rol van Opdrachtnemer gericht op beoordeling van meldingen of alerts, incidentrespons, containment, herstel binnen mandaat, escalatie en overdracht aan het geïntegreerde cloudplatformteam. Structurele analyse, duurzame oplossing en eventuele verbetermaatregelen vinden plaats tijdens kantooruren binnen het geïntegreerde cloudplatformteam, tenzij onmiddellijke opvolging noodzakelijk is voor continuïteit, beveiliging of beperking van directe schade.

6.1 Proces

Het incidentproces omvat minimaal:

1. melding of alert;
2. registratie;
3. classificatie op impact en urgentie;
4. toewijzing;
5. analyse;
6. herstel of workaround;
7. communicatie;
8. escalatie indien nodig;
9. afsluiting;
10. evaluatie en eventuele problemregistratie.

6.2 Prioritering

De prioritering volgt de prioriteitenmatrix uit de SLA. De DAP bevat voorbeelden en toepassingsregels voor P1 tot en met P5.

6.3 Overdracht incidenten buiten kantooruren

Elke inzet buiten kantooruren wordt uiterlijk bij aanvang van de eerstvolgende kantooruren overgedragen aan het geïntegreerde cloudplatformteam.

De overdracht bevat minimaal:

1. incidentnummer;
2. prioriteit;
3. start- en eindtijd;

4. tijdlijn;
5. geraakte componenten;
6. uitgevoerde acties;
7. betrokken personen;
8. gebruikte toegangen;
9. afwijkingen of noodmaatregelen;
10. resterende risico's;
11. benodigde vervolgacties;
12. voorstel voor problem-, change- of security follow-up.

7 Major incident management

Bij P1-incidenten en andere door Opdrachtgever aangewezen kritieke verstoringen wordt het major incidentproces gevolgd.

Opdrachtgever behoudt regie op stakeholdercommunicatie. Opdrachtnemer ondersteunt technische coördinatie, analyse, herstel en rapportage. Bij incidenten waarbij een handeling van Opdrachtnemer heeft bijgedragen aan het ontstaan of de verergering, levert Opdrachtnemer tevens een technische analyse conform de SLA.

De DAP bevat:

1. major incident criteria;
2. rollen;
3. communicatiekanalen;
4. overlegfrequentie;
5. escalatiematrix;
6. technische herstelwerkwijze;
7. RCA-termijnen;
8. evaluatieproces.

8 Problemmanagement

Problems worden geregistreerd voor terugkerende incidenten, bekende fouten, technische schuld, kwetsbaarheden, beheerbaarheidsknelpunten en structurele verbeterpunten die relevant zijn voor de dienstverlening rond het Azure-cloudplatform.

Problems en daaruit voortkomende verbetermaatregelen worden opgenomen in de gezamenlijke verbeterbacklog. De Product Owner van Opdrachtgever bepaalt de prioritering op basis van waarde, risico, urgentie, afhankelijkheden en beschikbare capaciteit.

8.1 Problemmanagement tijdens kantooruren

Problemmanagement tijdens kantooruren vindt plaats binnen het geïntegreerde cloudplatformteam onder regie van Opdrachtgever.

Het door Opdrachtnemer geleverde teamlid draagt als onderdeel van het geïntegreerde cloudplatformteam bij aan analyse, oplossingsrichting, uitvoering, documentatie en kennisoverdracht.

Deze bijdrage vindt plaats binnen de overeengekomen inzet, expertise, teamafspraken en sprint- of backlogplanning.

De opname, prioritering, planning of afronding van problems of verbetermaatregelen in de backlog geldt niet als individuele resultaatsverplichting van Opdrachtnemer of het door Opdrachtnemer geleverde teamlid, tenzij een specifieke deliverable uitdrukkelijk als resultaatsverplichting aan Opdrachtnemer is opgedragen.

8.2 Problemmanagement buiten kantooruren

Buiten kantooruren is de rol van Opdrachtnemer beperkt tot beoordeling van meldingen of alerts, signalering, registratie, escalatie, tijdelijke beheersmaatregelen binnen mandaat en overdracht aan het geïntegreerde cloudplatformteam.

Structurele analyse, root cause analysis, architectuurafwegingen, structurele verbetermaatregelen en duurzame oplossingen vinden plaats tijdens kantooruren binnen het geïntegreerde cloudplatformteam, tenzij onmiddellijke opvolging noodzakelijk is voor continuïteit, beveiliging of beperking van directe schade.

8.3 Signalering en opvolging

Opdrachtnemer signaleert proactief terugkerende verstoringen, kwetsbaarheden, technische schuld, ontbrekende of verouderde runbooks, documentatiegebreken en andere knelpunten die de beheerbaarheid, supportbaarheid buiten kantooruren, security, compliance of overdraagbaarheid van het platform raken.

Bevindingen worden geregistreerd in de overeengekomen tooling en besproken in de service review of, indien urgent, geëscaleerd conform de DAP.

9 Change enablement

9.1 Uitgangspunten

Wijzigingen aan het cloudplatform worden uitgevoerd volgens een DevOps-gebaseerd changeproces. Wijzigingen worden gecontroleerd, aantoonbaar, auditeerbaar en overdraagbaar uitgevoerd.

Alle wijzigingen worden waar mogelijk uitgevoerd via:

1. Infrastructure as Code;
2. versiebeheer;
3. pull requests;
4. peer reviews;
5. geautomatiseerde CI/CD-pipelines.

Een wijziging wordt als gecontroleerd en geautoriseerd beschouwd wanneer:

1. deze is gekoppeld aan een backlog-item, incident of change request;
2. deze via een pull request is beoordeeld en goedgekeurd;
3. deze succesvol is gevalideerd via geautomatiseerde pipeline-controles;
4. de uitvoering, uitkomst en eventuele afwijkingen zijn geregistreerd in de overeengekomen tooling.

De combinatie van peer review en pipeline-validatie vormt het primaire controlemechanisme voor wijzigingen.

Traditionele voorafgaande change-goedkeuring, bijvoorbeeld via CAB, is uitsluitend vereist bij:

1. wijzigingen met hoog risico voor beschikbaarheid, security, compliance of continuïteit;
2. wijzigingen met significante architectuurimpact;
3. wijzigingen waarbij expliciet goedkeuring door Opdrachtgever is vereist.

Wijzigingen worden zoveel mogelijk gebundeld en uitgevoerd binnen sprint- of releasecycli.

9.2 Typen changes

Type change	Beschrijving	Goedkeuring
Standaard change	Vooraf goedgekeurde laag-risico wijziging	Conform DAP
Normale change	Wijziging met impact/risico	Goedkeuring volgens proces
Emergency change	Spoedeisende wijziging ter voorkoming of oplossing van incident/securityrisico	Achteraf review verplicht

Buiten kantooruren voert Opdrachtnemer uitsluitend emergency changes uit voor zover deze passen binnen de mandaatmatrix en noodzakelijk zijn voor continuïteit, beveiliging of beperking van directe schade.

Standaard changes, normale changes, reguliere doorontwikkeling en niet-spoedeisende optimalisaties worden tijdens kantooruren voorbereid, beoordeeld en uitgevoerd door het geïntegreerde cloudplatformteam, tenzij Opdrachtgever vooraf schriftelijk anders goedkeurt.

9.3 Definition of Done

Een change is pas afgerond wanneer minimaal:

1. uitvoering is geregistreerd;
2. resultaat is gevalideerd;
3. relevante documentatie is bijgewerkt;
4. runbooks zijn bijgewerkt indien van toepassing;
5. monitoring/alerting is aangepast indien nodig;
6. overdrachtsinformatie beschikbaar is;
7. open risico's zijn vastgelegd.

Voor changes tijdens kantooruren geldt aanvullend dat aan de relevante uitgangspunten uit paragraaf 9.1 is voldaan, tenzij Opdrachtgever vooraf schriftelijk anders goedkeurt.

Opdrachtnemer meldt een emergency change buiten kantooruren zo spoedig mogelijk aan de escalatiecontactpersoon van Opdrachtgever, uiterlijk binnen 2 uur na aanvang van de wijziging. De volledige registratie inclusief resultaat, afwijkingen en resterende risico's wordt uiterlijk bij aanvang van de eerstvolgende kantooruren overgedragen.

10 Access management

De DAP beschrijft het proces voor aanvragen, wijzigen, intrekken en controleren van toegangsrechten.

Voor beheer- en administratieve toegang geldt minimaal:

1. least privilege;
2. MFA;
3. logging;
4. periodieke review;
5. noodtoegangsprocedure;
6. functiescheiding waar passend;
7. expliciete goedkeuring bij verhoogde rechten.

Risicoacceptatie rond toegang ligt bij Opdrachtgever.

11 Werkwijze gezamenlijk platformteam

11.1 Architectuur

- Het team werkt binnen de vastgestelde architectuurprincipes van de KB
- Afwijkingen van architectuurkaders worden vooraf met de betrokken architecten overlegd met duidelijke risico-impactanalyse, mogelijke alternatieven en planning voor het oplossen van eventuele technical debt.
- De cloudomgeving moet worden ingericht en beheerd volgens een landing zone-architectuur conform best practices van het Microsoft Cloud Adoption Framework.
- Cloudresources moeten worden voorzien van verplichte tags voor bijvoorbeeld omgeving, applicatie en eigenaar.
- Taggingbeleid: beschrijft verplichte tags (namen, waarden, naamconventies), handhavingsverantwoordelijkheid en controleprocedure. Op te stellen tijdens implementatieperiode en op te nemen als bijlage bij de DAP.
- Het team legt relevante architectuurkeuzes, afwijkingen van architectuurkaders en situaties waarin wordt afgeweken van de interne koers van de KB vast in Architecture Decision Records of een gelijkwaardige vastleggingsvorm, inclusief overwogen alternatieven, risico's, kostenimpact, security- en compliance-impact, beheerimpact en exit-impact.
- Architectuurkeuzes worden mede beoordeeld op:
 - o beheerbaarheid
 - o supportbaarheid buiten kantooruren
 - o benodigde runbooks

11.2 Criteria voor platformcomponenten

Voor nieuwe of gewijzigde platformcomponenten geldt dat deze moeten aansluiten op de sprintafspraken en werkwijze van het geïntegreerde cloudplatformteam.

Voor zover relevant voor de betreffende component wordt geborgd dat sprake is van:

1. technische implementatie conform de overeengekomen werkwijze;
2. validatie via CI/CD-pipelines;
3. monitoring en alerting;
4. logging en auditing;
5. operationele documentatie en, indien van toepassing, runbooks;
6. security- en compliance-eisen;
7. beoordeling van beheerbaarheid, supportbaarheid buiten kantooruren en overdraagbaarheid;
8. registratie van eventuele afwijkingen, restpunten, risico's of tijdelijke workarounds.

Er vindt geen separate acceptatiefase buiten de sprint plaats indien aan de afgesproken sprint- en kwaliteitscriteria is voldaan, tenzij expliciet anders overeengekomen of tenzij Opdrachtgever op grond van de SLA, DAP, Overeenkomst of het Programma van Eisen expliciete goedkeuring of acceptatie heeft voorgeschreven.

Deze criteria laten onverlet dat Opdrachtgever regie houdt op prioritering, architectuurkaders, risicoacceptatie, security- en compliancekaders en acceptatie van opleveringen waar expliciete acceptatie is overeengekomen.

11.3 Soevereiniteit en autonomie

- Het team houdt een actueel overzicht bij van relevante cloud-native, Azure-specifieke of leveranciersspecifieke afhankelijkheden die kunnen leiden tot vendor lock-in, inclusief motivatie, risico's, alternatieven, mitigerende maatregelen en overdraagbaarheid bij exit.
- Het team past Azure-native diensten en platformfunctionaliteit alleen toe wanneer deze aantoonbaar bijdragen aan functionaliteit, beheerbaarheid, security, schaalbaarheid, kostenoptimalisatie of continuïteit. De keuze wordt expliciet afgewogen tegen open standaarden, overdraagbaarheid en exitmogelijkheden.
- IaC-oplossingen worden waar mogelijk voorzien van abstractielagen die migratie of vervanging van onderliggende diensten vereenvoudigen. Platformkeuzes worden expliciet beoordeeld op overdraagbaarheid en migratiegereedheid

11.4 Manier van werken

- De primaire afstemming binnen het cloudplatformteam vindt plaats via agile ceremonies. Deze vormen de kern van de operationele samenwerking en besluitvorming.
- Het team werkt vanuit centrale version repositories onder eigenaarschap van de KB
- Alle intellectuele eigendomsrechten, waaronder auteursrechten, op configuraties, IaC-code, scripts, runbooks, architectuurdocumentatie en overdrachtsinformatie die in het kader van de dienstverlening zijn opgesteld of beheerd, berusten bij Opdrachtgever dan wel worden bij deze bepaling aan Opdrachtgever overgedragen. Opdrachtnemer verkrijgt op deze materialen geen zelfstandig gebruiksrecht anders dan noodzakelijk voor de uitvoering van de dienstverlening.
- Alle productiewijzigingen verlopen via pull requests en peer reviews.
- Het uitrollen van en wijzigingen aan infrastructuur wordt via Infrastructure-as-Code en geautomatiseerde CI/CD pipelines uitgevoerd en niet handmatig in de cloudomgeving. Daarbij wordt gebruik gemaakt van automatische validatie van Infrastructure-as-Code configuraties.
- Automatisering en scripts maken gebruik van Azure Managed Identity of vergelijkbare mechanismen voor veilige authenticatie, niet van wachtwoorden tenzij dit technisch niet mogelijk is
- Er wordt gebruik gemaakt van Azure Verified Modules voor Terraform indien mogelijk

11.5 Security

- Security- en governancebeleid wordt waar mogelijk geautomatiseerd toegepast.
- Het team richt een patch- en vulnerabilitymanagementproces in.
- Het team ondersteunt een volwassen IAM- en RBAC-model conform least privilege-principes, inclusief periodieke beoordeling van toegangen en beheerrechten.
- Privileged rollen binnen de Azure-omgeving worden beheerd via Privileged Identity Management met just-in-time toegang, goedkeuringsmechanismen en verplichte MFA.
- Het team configureert en onderhoudt actief de benodigde technische voorzieningen binnen het cloudplatform om compliance continu inzichtelijk te maken, waaronder minimaal:
 - o Geautomatiseerde compliance monitoring op basis van erkende standaarden, waaronder de toepasselijke CIS Benchmark en/of de configuratiebaselines van de cloudplatformleverancier
 - o Configuratiebaselines die aantoonbaar zijn afgeleid van de CIS Benchmarks (Level 1 minimaal, Level 2 waar risico's dit vereisen) of de hardeningsrichtlijnen van de betrokken platformleverancier
 - o Continue beleidscontrole via Infrastructure-as-Code (IaC) of cloudeigen policy-engines, waarmee afwijkingen van de baseline automatisch worden gedetecteerd en gerapporteerd

- Compliance dashboards en -rapportages die periodiek (minimaal maandelijks) inzicht geven in de compliance-status, openstaande bevindingen en de voortgang van herstelmaatregelen.

12 Buiten-kantoor tijden ondersteuning en mandaatmatrix

12.1 Mandaatmatrix

Binnen kantoor uren werkt het geïntegreerde cloudplatformteam met een hoge mate van autonomie. Het team is bevoegd om zelfstandig werkzaamheden, wijzigingen en verbeteringen uit te voeren voor zover deze binnen de gezamenlijke backlog of sprintdoelen vallen, passen binnen de overeengekomen architectuurkaders en voldoen aan de Definition of Done uit paragraaf 9.3 en, voor zover relevant, de criteria voor platformcomponenten uit paragraaf 11.2.

De mandaatmatrix in deze paragraaf heeft betrekking op buiten-kantoor tijden ondersteuning. De mandaatmatrix bepaalt welke handelingen Opdrachtnemer buiten kantoor uren zelfstandig mag uitvoeren, welke handelingen voorafgaande goedkeuring vereisen, welke handelingen niet zijn toegestaan en wanneer escalatie naar Opdrachtgever verplicht is.

De mandaatmatrix wordt tijdens de implementatieperiode gezamenlijk uitgewerkt en uiterlijk vóór overgang naar reguliere dienstverlening door Opdrachtgever goedgekeurd.

De mandaatmatrix bevat minimaal:

1. welke acties Opdrachtnemer zelfstandig mag uitvoeren;
2. welke acties voorafgaande goedkeuring vereisen;
3. welke acties nooit zelfstandig worden uitgevoerd;
4. wanneer escalatie verplicht is;
5. welke acties achteraf moeten worden gemeld;
6. welke informatie uiterlijk bij de eerstvolgende kantoor uren wordt overgedragen;
7. welke kosten- en impactgrenzen gelden voor zelfstandig handelen door Opdrachtnemer buiten kantoor uren, waaronder indien van toepassing een maximumbedrag per actie, een cumulatief maximum per maand en situaties waarin voorafgaande schriftelijke goedkeuring van Opdrachtgever vereist is;
8. welke noodscenario's gelden en hoe deze achteraf worden geëvalueerd.

Een globale mandaatmatrix op hoofd niveau is onvoldoende indien daaruit niet duidelijk blijkt welke handelingen wel, niet of alleen na goedkeuring zijn toegestaan.

Onderstaande mandaatmatrix ziet uitsluitend op buiten-kantoor tijden ondersteuning en beperkt niet de normale autonomie van het geïntegreerde cloudplatformteam tijdens kantoor uren, voor zover wordt gewerkt binnen backlog, sprintdoelen, architectuurkaders, overeengekomen werkwijze, de

Definition of Done uit paragraaf 9.3 en, voor zover relevant, de criteria voor platformcomponenten uit paragraaf 11.2.

Type actie	Zelfstandig toegestaan door Opdrachtnemer?	Voorwaarden	Escalatie nodig?
Herstart bekende component	Ja	Runbook ² actueel en getest	Alleen bij mislukking of impactvergroting
Opschalen capaciteit binnen vooraf vastgestelde grenzen	Ja	Binnen afgesproken kosten- en impactgrens	Achteraf melden
Failover uitvoeren van redundante component	Ja	Indien standaard component of runbook aanwezig	Alleen bij mislukking of impactvergroting
Tijdelijk blokkeren verdachte toegang	Ja	Bij acuut securityrisico	Direct melden aan security-escalatie
Rollback van een recente change	Ja	Indien het zeer sterke vermoeden bestaat dat deze onverwachte problemen veroorzaakt en er een correcte rollback mogelijk is	Alleen bij mislukking of impactvergroting
Uitvoeren van herstel instructies van de cloud provider	Ja	Bij storing van de onderliggende cloud infrastructuur en als hiervoor expliciete instructies worden geleverd door de cloud provider	Alleen bij mislukking of impactvergroting
Aanpassen firewall/network rules ³	Beperkt	Alleen pre-approved scenario's	Ja bij afwijking
Wijzigen IAM/RBAC	Nee, tenzij noodscenario	Alleen conform noodtoegangsprocedure	Altijd melden
Uitvoeren emergency change	Ja, indien noodzakelijk	Registratie en achteraf review verplicht	Ja conform prioriteit
Structurele architectuurwijziging	Nee	Niet toegestaan buiten kantooruren	Voorafgaande goedkeuring
Uitschakelen logging/monitoring	Nee	Niet toegestaan, tenzij noodzakelijk en goedgekeurd	Altijd vooraf escaleren
Verwijderen resources/data	Nee	Niet toegestaan buiten kantooruren, tenzij expliciet goedgekeurd	Altijd vooraf escaleren
Inschakelen ketenleverancier	Beperkt	Alleen indien contractueel toegestaan en geregistreerd	Melden aan Opdrachtgever

12.2 Minimale informatiepositie buiten kantooruren

Opdrachtnemer beschikt buiten kantooruren minimaal over:

1. actuele contact- en escalatielijst, inclusief security-escalatie en CSIRT-contacten indien van toepassing;
2. actuele prioriteitenmatrix;

² Runbook indien beschikbaar.

³ Firewall- en netwerkenpassingen zijn een interne KB-aangelegenheid. Opdrachtnemer conformeert zich aan de op dat moment geldende werkwijze.

3. actuele mandaatmatrix;
4. actuele runbooks;
5. toegang tot monitoring en logging;
6. toegang tot incidentregistratie;
7. inzicht in actuele open P1/P2-incidenten;
8. inzicht in geplande changes en freeze-periodes;
9. overzicht kritieke componenten;
10. noodtoegangsprocedure;
11. security- en compliance-instructies;
12. major incident communicatieprocedure;
13. de geldende bereikbaarheid van het serviceteam en, indien relevant voor securityincidenten, de CSIRT-bereikbaarheid.

Communicatie met de buiten-kantoor tijden achtervang van Opdrachtnemer kan in het Engels plaatsvinden. Alle documentatie, overdrachtsrapportages en formele communicatie richting Opdrachtgever worden in het Nederlands opgesteld, tenzij Opdrachtgever schriftelijk anders heeft overeengekomen.

12.3 Kennisborging achtervangmedewerkers

Achtervangmedewerkers en buiten-kantoor tijden engineers nemen minimaal maandelijks deel aan teamactiviteiten van het cloudplatformteam, zodat kennis van architectuur, werkwijzen en wijzigingen actueel blijft.

13 Monitoring en eventmanagement

Monitoring en alerting worden ingericht voor beschikbaarheid, performance, capaciteit, security, policy compliance, kosten en platformgezondheid.

Alerts zijn gekoppeld aan prioriteit, runbook, verantwoordelijke rol, opvolgingstermijn en escalatiepad. Opdrachtnemer geeft aan waar en op welke manier de alerts worden aangeleverd voor de aansluiting op de buiten-kantoor tijden ondersteuning.

14 Rapportage

De rapportage sluit aan op de indeling van KPI's en stuurindicatoren in de SLA. De DAP werkt per KPI of stuurindicator minimaal uit:

1. definitie;
2. databron;
3. meetmethode;
4. rapportagefrequentie;
5. eigenaar van de registratie;
6. wijze van duiding in de service review;
7. of sprake is van een service level target, stuurindicator of teambrede flow-indicator.

Teambrede DevOps-flow-indicatoren worden in de rapportage gebruikt als stuurinformatie voor het geïntegreerde cloudplatformteam. Zij worden niet gebruikt als individuele outputnorm voor het door Opdrachtnemer geleverde teamlid, tenzij dit uitdrukkelijk en schriftelijk anders is overeengekomen.

15 Kennisoverdracht, documentatie en overdraagbaarheid

Kennisoverdracht, documentatie en overdraagbaarheid zijn structurele onderdelen van de dienstverlening. Deze activiteiten zijn geen optionele of incidentele werkzaamheden, maar onderdeel van de reguliere samenwerking binnen het geïntegreerde cloudplatformteam, transitie, wijzigingsafhandeling, incidentopvolging en exit.

Kennisborging vindt primair plaats door samenwerking binnen het geïntegreerde cloudplatformteam. Het team werkt daarbij volgens de principes van co-working, pairing, gezamenlijke verantwoordelijkheid, pull request reviews, technische walkthroughs, RCA-besprekingen, change reviews en gezamenlijke documentatie.

Documentatie wordt beheerd in de door Opdrachtgever aangewezen of goedgekeurde omgeving. Documentatie ondersteunt de dagelijkse werkwijze, beheerbaarheid, supportbaarheid buiten kantooruren, security, compliance, auditbaarheid en overdraagbaarheid. Documentatie is geen vervanging van samenwerking, maar een randvoorwaarde voor controleerbaarheid, continuïteit en exit.

Opdrachtnemer is verantwoordelijk voor het tijdig vastleggen en actueel houden van de door hem ingebrachte technische documentatie, runbooks, werkinstructies, configuratieonderbouwing, overdrachtsinformatie en relevante afhankelijkheden, voor zover deze voortkomen uit de door Opdrachtnemer uitgevoerde werkzaamheden of buiten-kantoor tijden ondersteuning.

Overdrachtsmomenten worden gericht ingezet bij onboarding van nieuwe teamleden, wisseling van personeel van Opdrachtnemer, overdracht naar andere teams of leveranciers, voorbereiding op exit en andere situaties waarin continuïteit, beheerbaarheid of overdraagbaarheid dit vereisen.

Voor overdrachtsobjecten die niet al voldoende herleidbaar, controleerbaar en overdraagbaar zijn vastgelegd in de door Opdrachtgever aangewezen tooling, repositories of documentatieomgeving, wordt een Exit-inventaris bijgehouden.

Opdrachtnemer zorgt ervoor dat overdrachtsobjecten, afhankelijkheden, risico's, tijdelijke workarounds en overige relevante overdrachtsinformatie die voortkomen uit de door hem uitgevoerde werkzaamheden of buiten-kantoor tijden ondersteuning tijdig worden vastgelegd, aangevuld of aangewezen.

De Exit-inventaris wordt minimaal jaarlijks besproken in de service review en waar nodig geactualiseerd. Opdrachtgever beoordeelt of de beschikbare informatie voldoende bruikbaar is voor overdracht, continuïteit en exit.

16 Security en compliance

De DAP operationaliseert de voor de dienstverlening relevante eisen en afspraken die voortkomen uit informatiebeveiliging, privacy, compliance, audit of wet- en regelgeving. De inhoudelijke eisen worden vastgesteld door de daarvoor verantwoordelijke disciplines, waaronder Security, Privacy, Risk en Compliance. De DAP vertaalt de relevante gevolgen daarvan naar rollen, processen, escalaties, rapportages, registraties en operationele werkafspraken.

De DAP bevat minimaal afspraken over:

1. beveiligingsbevindingen;
2. patching;
3. logging;
4. audit bewijs;
5. naleving van beleid/policies;
6. uitzonderingsproces;
7. risicoacceptatie;
8. ketenleveranciers;
9. meldingen van securityincidenten;
10. security-incidentprocedure van Opdrachtgever.

Voor securityincidenten wordt aangesloten op de door Opdrachtgever vastgestelde security-incidentprocedure en escalatieroute. Indien CSIRT-betrokkenheid vereist is, wordt geëscaleerd conform de CSIRT-afspraken van Opdrachtgever. De CSIRT-bereikbaarheid vormt geen zelfstandig servicevenster voor de cloudplatformdienstverlening, tenzij dit uitdrukkelijk is overeengekomen.

16.1 Certificeringen

Opdrachtnemer beschikt over en behoudt gedurende de looptijd van de Overeenkomst actuele en geldige certificeringen op het gebied van informatiebeveiliging en cloudplatformdienstverlening, waaronder ten minste ISO 27001 en ISO 27017. Opdrachtnemer levert jaarlijks, uiterlijk binnen 30 kalenderdagen na aanvang van elk contractjaar, een bewijs van geldigheid aan Opdrachtgever in de vorm van een geldig certificaat of een gelijkwaardig auditrapport.

Op eerste verzoek van Opdrachtgever overlegt Opdrachtnemer het meest recente bewijs binnen 10 werkdagen.

Personeel van Opdrachtnemer dat toegang heeft tot kritieke omgevingen van Opdrachtgever valt onder de Nederlandse rechtsmacht en is onderworpen aan Nederlands recht. Opdrachtnemer legt bij aanvang van de dienstverlening een overzicht voor van medewerkers met toegang tot kritieke omgevingen, inclusief werklocatie. Wijzigingen worden uiterlijk vijf werkdagen vooraf gemeld. Opdrachtgever behoudt het recht toegang te weigeren of in te trekken voor medewerkers die niet aan deze eis voldoen.

16.2 Privacy en gegevensbescherming

- Definitie van een datalek zoals in de Verwerkersovereenkomst beschreven.

- Procedure (en werkwijze) datalekken en meldplicht zoals in de Verwerkersovereenkomst is vastgesteld worden toegevoegd aan de DAP.

17 Implementatieperiode en acceptatie reguliere dienstverlening

De overgang naar reguliere dienstverlening vindt pas plaats nadat Opdrachtgever heeft vastgesteld dat de dienstverlening operationeel beheersbaar en overdraagbaar is ingericht.

Daarvan is minimaal sprake indien:

1. de definitieve DAP is ingevuld en door Opdrachtgever is goedgekeurd;
2. de SLA operationeel toepasbaar is;
3. de vastlegging van de scope van de dienstverlening beschikbaar is, indien van toepassing;
4. de RACI op activiteitsniveau is uitgewerkt en door Opdrachtgever is goedgekeurd;
5. de mandaatmatrix is vastgesteld;
6. escalatiepaden zijn ingericht en waar relevant getest;
7. minimale werkinstructies en/of runbooks beschikbaar zijn;
8. de rapportagestructuur is ingericht;
9. relevante kennisoverdracht heeft plaatsgevonden of aantoonbaar is gestart;
10. de voor exit en overdracht relevante informatie is vastgelegd of aangewezen in de overeengekomen tooling, repositories of documentatieomgeving, en een eventuele aanvullende Exit-inventaris is door Opdrachtgever beoordeeld op bruikbaarheid;
11. de planning voor het eerste ingevulde Exit-plan is akkoord;
12. open risico's, afhankelijkheden, tijdelijke workarounds en restpunten zijn vastgelegd, toegewezen en voorzien van opvolging.

Opdrachtgever kan overgang naar reguliere dienstverlening weigeren of uitstellen indien bovenstaande onderdelen onvoldoende concreet, onvolledig, niet bruikbaar of niet toetsbaar zijn uitgewerkt.

18 Beheer van de DAP

De DAP, RACI, mandaatmatrix, contactmatrix en escalatiematrix worden minimaal jaarlijks en bij relevante wijzigingen geëvalueerd en waar nodig geactualiseerd.

Relevante wijzigingen zijn onder meer wijzigingen in scope, rollen, tooling, servicevensters, escalatielijnen, ketenleveranciers, security- of compliancekaders, buiten-kantoor tijden ondersteuning, exitafspraken, overdrachtsubjecten of afhankelijkheden.

Bij de periodieke evaluatie van de DAP wordt ook beoordeeld of de voor exit en overdracht relevante informatie voldoende actueel, vindbaar en bruikbaar is vastgelegd of aangewezen in de overeengekomen tooling, repositories of documentatieomgeving. Voor zover een aanvullende Exit-inventaris wordt bijgehouden, wordt beoordeeld of deze nog actueel en bruikbaar is.

Wijzigingen worden vastgelegd inclusief datum, aanleiding, wijziging, eigenaar, impact en goedkeuring.

Wijzigingen in de DAP, RACI, mandaatmatrix, contactmatrix, escalatiematrix of aanvullende Exit-inventaris mogen niet leiden tot wijziging van contractuele verplichtingen, SLA-afspraken, scope of prijs zonder formele wijzigingsprocedure.

De actuele contactgegevens, bereikbaarheidsgegevens, vervangingsafspraken en escalatiecontacten worden opgenomen in Bijlage 19.1 Contactmatrix en escalatiegegevens. Wijzigingen in deze bijlage worden schriftelijk vastgelegd en door de Servicemanager van Opdrachtgever goedgekeurd. Actualisatie van deze bijlage geldt niet als wijziging van de DAP, tenzij de wijziging gevolgen heeft voor rollen, verantwoordelijkheden, servicevensters, mandaten, escalatiecriteria of contractuele verplichtingen.

19 Bijlagen

19.1 Contactmatrix en escalatiegegevens

De contactmatrix bevat de actuele contactgegevens, bereikbaarheidsgegevens, vervangingsafspraken en escalatiecontacten voor de uitvoering van de dienstverlening.

De contactmatrix wordt gebruikt voor operationele afstemming, incidentmanagement, major incident management, buiten-kantoor tijden ondersteuning, security-escalatie, tactische escalatie, strategische escalatie en exit.

De contactmatrix wordt actueel gehouden gedurende de looptijd van de Overeenkomst. Opdrachtnemer meldt wijzigingen in zijn contactpersonen, bereikbaarheidsgegevens, vervangers of escalatielijnen tijdig aan Opdrachtgever. Opdrachtgever verwerkt of laat verwerken welke contactgegevens voor de samenwerking noodzakelijk zijn.

Wijzigingen in contactgegevens, bereikbaarheidsgegevens of vervangers gelden niet als wijziging van de DAP, tenzij zij gevolgen hebben voor rollen, verantwoordelijkheden, servicevensters, mandaten, escalatiecriteria of contractuele verplichtingen.

Rol / functie	Partij	Naam	E-mailadres / kanaal	Telefoonnummer	Bereikbaarheid	Vervanger / back-up	Escalativeniveau	Opmerkingen
Servicemanager Opdrachtgever	Opdrachtgever	[invullen]	[invullen]	[invullen]	Kantooruren	[invullen]	Tactisch	SLA, DAP, service review, operationele governance
Product Owner Cloudplatform	Opdrachtgever	[invullen]	[invullen]	[invullen]	Kantooruren	[invullen]	Operationeel / tactisch	Prioritering, backlog, sprintplanning en acceptatie
Cloud Platform Engineer Opdrachtgever	Opdrachtgever	[invullen]	[invullen]	[invullen]	Kantooruren	[invullen]	Operationeel	Technische afstemming, review, kennisborging
Security-escalatie Opdrachtgever	Opdrachtgever	[invullen]	[invullen]	[invullen]	Conform securityprocedure	[invullen]	Security	Securityincidenten, securityrisico's en escalaties
CSIRT-contact, indien van toepassing	Opdrachtgever	[invullen]	[invullen]	[invullen]	Conform CSIRT-afspraken	[invullen]	Security	Alleen bij securityincidenten waarvoor CSIRT-betrokkenheid vereist is
Contractmanager Opdrachtgever	Opdrachtgever	[invullen]	[invullen]	[invullen]	Kantooruren	[invullen]	Strategisch / contractueel	Contractuele escalaties, wijzigingen en leveranciersprestaties
IT Operations / Servicedesk Opdrachtgever	Opdrachtgever	[invullen]	[invullen]	[invullen]	Conform interne afspraken	[invullen]	Operationeel	Aansluiting operationele processen en

Rol / functie	Partij	Naam	E-mailadres / kanaal	Telefoonnummer	Bereikbaarheid	Vervanger / back-up	Escalatieniveau	Opmerkingen
								gebruikerscommunicatie
Service Delivery Manager Opdrachtnemer	Opdrachtnemer	[invullen]	[invullen]	[invullen]	Kantooruren	[invullen]	Tactisch	Servicekwaliteit, rapportage, escalaties en service review
Teamlid / Cloud Platform Engineer Opdrachtnemer	Opdrachtnemer	[invullen]	[invullen]	[invullen]	Kantooruren	[invullen]	Operationeel	Inzet binnen het geïntegreerde cloudplatformteam
Buiten-kantoor tijden achternavigatie	Opdrachtnemer	[invullen]	[invullen]	[invullen]	Conform DAP 5.2	[invullen]	Operationeel / escalatie	Incidentrespons, containment, herstel binnen mandaat en overdracht
Security Specialist Opdrachtnemer	Opdrachtnemer	[invullen]	[invullen]	[invullen]	Conform securityprocedure	[invullen]	Security	Securityadvies, findings, baselines, compliance en incidentondersteuning
Azure Architect / Specialist Opdrachtnemer	Opdrachtnemer	[invullen]	[invullen]	[invullen]	Op afroep / conform afspraak	[invullen]	Tactisch / specialistisch	Specialistisch advies over Azure, landing zones, governance en optimalisatie
Implementatiemanager Opdrachtnemer	Opdrachtnemer	[invullen]	[invullen]	[invullen]	Tijdens implementatieperiode	[invullen]	Implementatie	Inrichting implementatieperiode, planning, overdracht en acceptatie
Exitmanager Opdrachtnemer	Opdrachtnemer	[invullen]	[invullen]	[invullen]	Bij exit / op verzoek	[invullen]	Exit	Coördinatie Exit-plan, overdraagbaarheid en exit-readiness
Ketenleverancier, indien van toepassing	Derde partij	[invullen]	[invullen]	[invullen]	Conform ketenafspraken	[invullen]	Operationeel / specialistisch	Alleen voor zover betrokken bij dienstverlening, continuïteit, security of exit

