

[dubbelklik hier om een foto in te voegen]



Technisch Programma van Eisen Deel 2 (Physical Identity Access Management)

uitgave 18-02-2026

Technisch Programma van Eisen Deel 2 (Physical Identity Access Management)

Dit document is een bijlage van de Uitnodiging tot Inschrijving
van Eindhoven Airport N.V. inzake Aanbesteding
Toegangscontrolesysteem

Colofon

Technisch Programma van Eisen Deel 2 (Physical Identity Access
Management)

Uitgave 18-02-2026

Eindhoven Airport N.V.

Office Luchthavenweg 13

Telefoon +31 (0) 40 2919 9829

Terminal Luchthavenweg 25,
5657 EA Eindhoven

1 Inleiding	5
1.1 Doelstelling	5
1.2 Scope van Perceel 2	5
1.3 Relatie met Perceel 1 (USP)	5
2 Functionele eisen PIAM	6
2.1 Identity lifecycle management	6
2.2 Autorisatiematrix en rollen (RBAC)	6
2.3 Workflow management	6
3 Badge center processen	7
3.1 Aanvraagproces luchthavenidentiteitskaart (LHIK)	7
3.2 Bezoekersmanagement en vouchers	7
3.3 Contractor management & werkvergunningen	7
3.4 Badge center hardware	8
4 Self-service portaal	8
4.1 Functionaliteit voor eindgebruikers	8
4.2 Functionaliteit voor autoriseerders/managers	8
5 Rapportage en audit	9
5.1 Compliance rapportages	9
5.2 Audit trails	9
6 Interfaces en integraties	10
6.1 Bronbestanden (Active Directory)	10
6.2 Provisioning naar USP (Perceel 1)	10
7 Performance en schaalbaarheid	10
7.1 Capaciteitseisen	10
7.2 Responstijden	10
7.3 Beschikbaarheid	10
8 Kwaliteitseisen	11
8.1 Gebruiksvriendelijkheid	11
8.2 Workflow-automatisering	11
8.3 Toekomstbestendigheid	11
9 Service level requirements	12
9.1 Beschikbaarheid	12
9.2 Performance	12
9.3 Support	12
10 Kritieke processen	13
10.1 Uitdiensttreding (KRITIEK)	13
10.2 Bezoeker-host binding	13
10.3 Werkvergunningen	13
11 Acceptance criteria	14
11.1 Functioneel	14

11.2	Performance	14
11.3	Veiligheid	14
11.4	Compatibiliteit	14
11.5	Wet- en regelgeving & normen	14
11.6	Security en hardening	14
12	Planning en fasering	15
12.1	Relatie met Perceel 1	15
12.2	Fasering	15

1 Inleiding

1.1 Doelstelling

Dit TPvE beschrijft de eisen voor **Perceel 2: Physical Identity & Access Management (PIAM)**. Het doel is de implementatie van een softwareplatform dat de administratieve en logistieke processen rondom toegangsverlening automatiseert, stroomlijnt en borgt conform de strenge regelgeving van de burgerluchtvaart.

1.2 Scope van Perceel 2

De scope omvat de levering, inrichting en het onderhoud van een PIAM-softwareoplossing of gelijkwaardig systeem.

Kernfuncties:

- Beheer van identiteiten (vast personeel, contractors, bezoekers)
- Beheer van toegangsmiddelen (Luchthavenidentiteitskaart - LHIK, bezoekerspassen, voertuigpassen)
- Automatisering van workflows (goedkeuringen, VOG/VGB-aanvragen, trainingen)
- Self-service portaal voor aanvragers

Belangrijke focus:

- **Contractor Management** is van kritisch belang aangezien het overgrote deel van de passen wordt uitgegeven aan medewerkers van externe leveranciers
- **Visitor Management** ondersteunt de dagelijkse bedrijfsvoering met efficiënte en veilige begeleiding van bezoekers
- Het systeem moet robuust contractor- en bezoekersprocessen ondersteunen met minimale administratieve overhead voor Eindhoven Airport

1.3 Relatie met Perceel 1 (USP)

Het PIAM-systeem is de **bron** voor autorisaties. Het USP (Perceel 1) is de **uitvoerende** laag (deurcontrollers).

- PIAM bepaalt *WIE WAAR* mag komen en *WANNEER*
- PIAM stuurt geautoriseerde records (Kaartnummer + Autorisatiegroep) naar het USP
- USP koppelt statusinformatie (bijv. "pas gebruikt", "pas defect") terug naar PIAM

2 Functionele eisen PIAM

2.1 Identity lifecycle management

Het systeem moet de volledige levenscyclus van een identiteit ondersteunen:

1. **Onboarding:** Aanmaken identiteit, vastleggen persoonsgegevens, initiëren screening
2. **Actief:** Beheer van autorisaties, wijzigingen in functie/afdeling, her-certificering
3. **Offboarding:** Automatische intrekking van rechten bij uitdiensttreding, blokkeren pas, inname-registratie

2.2 Autorisatiematrix en rollen (RBAC)

Het systeem moet toegang verlenen op basis van een Autorisatiematrix die gekoppeld is aan de zonering van Eindhoven Airport:

- **LPA (Landside Public Area):** Geen specifieke pas nodig, tenzij voor specifieke kantoorruimtes
- **SRA (Security Restricted Area):** Vereist LHIK + Beveiligingsonderzoek + Security Training
- **SRA-CP (Critical Part):** Strikte scheiding, aanvullende eisen
- **Technische Ruimtes:** Toegang op basis van functie en werkvergunning

De oplossing moet **Role Based Access Control (RBAC)** of gelijkwaardige autorisatiemethodiek ondersteunen: een 'Elektricien SPIE' krijgt automatisch de set rechten die bij dat profiel hoort.

2.3 Workflow management

Het systeem moet configureerbare workflows bieden voor goedkeuringsprocessen.

- *Voorbeeld:* Aanvraag toegang Serverruimte → Goedkeuring Manager → Goedkeuring IT-Security → Toekenning recht → Notificatie gebruiker
- Tijdgebonden autorisaties: Rechten moeten automatisch vervallen na een instelbare datum/tijd

3 Badge center processen

3.1 Aanvraagproces luchthavenidentiteitskaart (LHIK)

Het systeem moet het Badge Center ondersteunen bij:

- Digitaliseren van het papieren aanvraagformulier
- Monitoring van de status van het Verklaring van Geen Bezwaar (VGB) / VOG proces
- Koppeling met e-learning (Security Awareness Training): Pas wordt pas geactiveerd na geslaagde training
- Printen en coderen van kaarten (ID-card printers aansturing)

3.2 Bezoekersmanagement en vouchers

Kritiek proces - Eindhoven Airport ontvangt dagelijks bezoekers van verschillende aard:

- **Vooraf aanmelden:** Via digitaal portaal of email met automatische voucher-generatie
- **Walk-in bezoekers:** Registratie bij balie met directe koppeling aan host
- **Begeleiding:** Het systeem moet borgen dat bezoekers in SRA altijd gekoppeld zijn aan een geautoriseerde begeleider (Host)
- **Vouchers:** Mogelijkheid voor bedrijven om bezoekers 'uit te nodigen' via email met een QR-code of barcode voor aanmelding bij de balie/kiosk
- **Groepsbezoeken:** Ondersteuning voor rondleidingen met meerdere bezoekers onder één host
- **VIP-bezoekers:** Mogelijkheid voor expedited processing met voorafgaande screening

3.3 Contractor management & werkvergunningen

Kritiek proces - Het overgrote deel van de toegangspassen wordt uitgegeven aan contractors:

- Het PIAM moet robuust contractor management bevatten of hierop integreren
- **Contractorbedrijven:** Mogelijkheid voor externe bedrijven om eigen personeel te beheren via delegated administration
- **Werkvergunningen:** Integratie of module voor beheer van werkvergunningen met koppeling aan specifieke autorisaties
- **Bulk-operaties:** Ondersteuning voor aanvragen van meerdere contractors tegelijk (bijvoorbeeld bij nieuwe project)
- **Automatische verlenging:** Optie voor automatische verlenging van toegang bij doorlopende contracten, met goedkeuringsworkflow
- **Expiry management:** Proactieve waarschuwingen bij verlopen van contractor-autorisaties of werkvergunningen
- Toegang tot technische ruimtes wordt enkel verleend als er een geldige, goedgekeurde werkvergunning is gekoppeld aan de identiteit/pas voor de specifieke periode

3.4 Badge center hardware

Het PIAM-systeem moet integreren met of ondersteuning bieden voor de volgende Badge Center hardware:

Badge-printers:

- Minimaal **2 badge-printers** ondersteunen (primair + failover)
- Printer-eisen of gelijkwaardig:
 - Dual-sided color printing
 - MIFARE DESFire EV2/EV3 encoding (compatibel met huidige passen)
 - Throughput: minimaal 100 kaarten/uur
- Inschrijver specificeert welke printer-merken/-modellen worden ondersteund

Zelfbedieningskiosk (optioneel):

- Touchscreen voor bezoekersregistratie
- QR/barcode scanner voor vouchers
- Badge-printer integratie voor directe uitgifte tijdelijke passen
- Multi-taal ondersteuning (minimaal Nederlands en Engels)

Verantwoordelijkheid: Inschrijver levert software-integratie en specificaties, Eindhoven Airport levert fysieke hardware conform specificaties.

4 Self-service portaal

4.1 Functionaliteit voor eindgebruikers

Een web-based portaal (en/of mobiele app) waar medewerkers:

- Hun eigen gegevens kunnen inzien
- Status van hun aanvragen kunnen volgen
- Pin-code wijzigingen kunnen initiëren (indien van toepassing)
- Verloren pas kunnen melden (blokkeren)
- Eigen trainingen en certificeringen kunnen inzien

4.2 Functionaliteit voor autoriseerders/managers

- Managers van externe bedrijven (bijv. afhandelaars, schoonmaak) moeten hun eigen personeel kunnen beheren (aanvragen, verlengen, uitdienst melden)
- “Delegated Administration”: EANV delegeert het administratieve werk naar de partners, EANV Badge Center verifieert en accordeert
- Bulk-goedkeuring: Mogelijkheid om meerdere aanvragen tegelijk goed te keuren
- Dashboard: Overzicht van alle actieve medewerkers en hun autorisaties

5 Rapportage en audit

5.1 Compliance rapportages

Het systeem moet standaardrapportages leveren voor audits door de Koninklijke Marechaussee (KMar) en interne auditors. Onderstaande tabel specificeert de verplichte rapportages:

Rapport	Frequentie	Formaat	Distributie	Auditor
Actieve SRA-passen	Wekelijks	Excel	Automatisch email Security Manager	KMar
Verlopende screenings (binnen 30 dagen)	Maandelijks	PDF + Excel	On-demand via portaal	Badge Center
Tijdelijke autorisaties >30 dagen actief	Wekelijks	Dashboard + Email alert	Automatisch Security Manager	Interne Audit
Werkvergunningen zonder goedkeuring	Dagelijks	Alarm + Dashboard	Real-time	Operations
Contractor-overzicht per bedrijf	Maandelijks	Excel	On-demand	Badge Center
Bezoekerslog SRA (laatste 90 dagen)	On-demand	Excel	Badge Center / Security	KMar
Blokkade-acties (laatste 30 dagen)	Maandelijks	PDF	Automatisch Security Manager	Interne Audit

Aanvullende eisen:

- Alle rapportages moeten binnen **30 seconden** gegenereerd kunnen worden
- Export naar minimaal Excel en PDF
- Filtering en sorteermogelijkheden per rapportage
- Automatische distributie via email voor geplande rapportages
- Ad-hoc rapportages: Het systeem moet een rapportage-builder of gelijkwaardige functionaliteit bieden waarmee geautoriseerde gebruikers zelf rapportages kunnen samenstellen op basis van beschikbare datavelden

5.2 Audit trails

Elke mutatie in het systeem (aanmaak, wijziging, verwijdering, goedkeuring) moet onuitwisbaar worden gelogd:

- *Wie* heeft de wijziging doorgevoerd?
- *Wanneer* is dit gebeurd?
- *Wat* was de oude waarde en de nieuwe waarde?
- *Waarom* (optioneel verplicht commentaarveld bij kritische wijzigingen)
- Retentie: minimaal **12 maanden** online, **7 jaar** archivering

6 Interfaces en integraties

6.1 Bronbestanden (Active Directory)

- Synchronisatie met Azure AD voor authenticatie (Single Sign-On) van portaalgebruikers
- **Nice to have:** Eindhoven Airport heeft vanwege beperkt vast personeel en lage mutaties, desondanks worden inschrijvers uitgenodigd om hun visie te omschrijven op het integreren met identity providers van verschillende partijen (EANV, Viggo, CSU, Marechaussee, etc.).
- Identiteitsbeheer voor vast personeel gebeurt handmatig via Badge Center, maar wel in het PIAM-systeem als single-source-of-truth.
- De koppeling met Active Directory is primair voor authenticatie
- Koppeling met overheid (achtergrondscreening)
- Voorbereid op digitale koppeling met systemen voor achtergrondscreening (indien beschikbaar gesteld door overheid)
- Monitoring van status VOG/VGB aanvragen met notificaties bij verlopen of benodigde acties
- Export-functionaliteit voor batch-aanvragen bij overheid (conform overheidsformaten)

6.2 Provisioning naar USP (Perceel 1)

- Real-time of near-real-time provisioning van kaarthouders en toegangsrechten naar het Security Management Systeem van Perceel 1
- Beveiliging: Alle data-uitwisseling tussen PIAM en USP dient versleuteld plaats te vinden (TLS 1.2 of hoger)
- Authenticatie: Wederzijdse authenticatie tussen systemen (certificaat-gebaseerd of OAuth 2.0 / API keys)
- Zie TPvE Deel 3 voor gedetailleerde interface-specificaties

7 Performance en schaalbaarheid

7.1 Capaciteitseisen

- Het systeem moet minimaal **4.000 actieve identiteiten** kunnen beheren
- Het systeem moet schaalbaar zijn tot **6.000 identiteiten** zonder (VM) hardware-upgrade
- Gelijktijdige gebruikers self-service portaal: minimaal **100 simultane sessies**

7.2 Responstijden

- Self-service portaal: maximaal **3 seconden** laadtijd per pagina (95th percentile)
- Provisioning naar USP (aangepast):
 - **Individuele wijziging:** Maximaal **60 seconden** (real-time provisioning)
 - **Batch-operaties (>10 identiteiten):** Maximaal **5 minuten** (async processing)
 - **Kritieke blokkering (uitdiensttreding):** Maximaal **15 minuten** (conform sectie 10.1)
- Rapportage generatie: maximaal **30 seconden** voor standaard compliance rapporten

7.3 Beschikbaarheid

- PIAM platform: minimaal **99%** uptime gedurende kantooruren (07:00-19:00, ma-vr)
- Self-service portaal: minimaal **98%** uptime (24/7)
- Geplande onderhoudsmomenten: maximaal **4 uur per maand**, na akkoord opdrachtgever, met minimaal 1 week vooraankondiging

8 Kwaliteitseisen

Dit hoofdstuk beschrijft de kwaliteitseisen die Eindhoven Airport stelt aan het PIAM-systeem. Deze eisen vormen de basis voor de beoordeling van inschrijvingen op het gunningscriterium 'Kwaliteit oplossing' en worden tijdens de contractperiode geborgd via de in dit TPvE beschreven acceptance criteria en service level requirements.

8.1 Gebruiksvriendelijkheid

Het systeem moet aantoonbaar gebruiksvriendelijk zijn voor alle doelgroepen:

- **Badge Center medewerkers:** Intuïtieve workflows zonder uitgebreide training
- **Eindgebruikers:** Self-service zonder helpdesk-ondersteuning voor standaard aanvragen
- **Managers/Autoriseerders:** Goedkeuringsprocessen binnen 3 klikken
- **Contractors:** Eenvoudige aanvraagprocedures via gedelegeerde portalen

Inschrijver moet in de offerte aantonen hoe gebruiksvriendelijkheid wordt geborgd (bijv. usability testing, reference cases, UI/UX design principes).

8.2 Workflow-automatisering

Het systeem moet workflows maximaal automatiseren. Inschrijver wordt gevraagd hun visie over de haalbaarheid, strategie en randvoorwaarden voor in ieder geval het volgende te omschrijven:

- LHIK-aanvragen automatiseren (zonder handmatige tussenkomst Badge Center)
- **Contractor-processen:** Minimaal **90%** geautomatiseerd via delegated administration
- Automatische escalatie bij overschrijding van interne SLA's
- Herinnering-notificaties voor verlopen rechten/screening (14 dagen vooraf)
- Automatische blokkering bij expiry van screening of training

Inschrijver moet in de offerte beschrijven welke workflows worden geautomatiseerd en hoe dit wordt gemeten.

8.3 Toekomstbestendigheid

- **Open standaarden:** Gebruik van REST API's of gelijkwaardig met volledige documentatie voor toekomstige integraties
- **Modulaire architectuur:** Onderdelen moeten vervangbaar zijn zonder core-systeem te raken
- **Vendor-agnostic:** Geen vendor lock-in op database of infrastructuur niveau
- **Biometrie-ready:** Voorbereid op integratie met biometrische systemen in de toekomst (geen implementatie vereist nu)

Inschrijver moet technology roadmap (5 jaar) overleggen en uitleggen hoe het systeem meegaat met toekomstige ontwikkelingen.

9 Service level requirements

9.1 Beschikbaarheid

- Uptime PIAM: **99% gedurende kantooruren** (ma-vr 07:00-19:00)
- Uptime self-service portaal: **98% (24/7)**
- Provisioning interface naar USP: **99,5%** (kritiek pad)

Servicewindow provisioning interface: De provisioning interface tussen PIAM en USP kent geen gepland servicewindow. Onderhoud aan deze interface dient buiten operationele uren plaats te vinden of redundant te worden uitgevoerd zonder onderbreking van de dienstverlening. Hierover treedt opdrachtnemer proactief in gesprek met opdrachtgever.

9.2 Performance

- Provisioning latency (individueel): **max 60 seconden** tussen actie in PIAM en effect op fysiek toegangspunt
- Provisioning latency (batch >10): **max 5 minuten**
- Self-service response: **max 3 seconden** per pagina
- Rapportage: **max 30 seconden** voor standaard rapporten

9.3 Support

- P1 (Provisioning volledig faalt): **2 uur** response, **4 uur** oplossing
- P2 (Portaal niet beschikbaar): **4 uur** response, **8 uur** oplossing
- P3 (Performance degradatie): **8 uur** response, **24 uur** oplossing
- P4 (Overige issues): **16 uur** response, **48 uur** oplossing

Prioriteitsdefinities:

- P1: Het PIAM-systeem of de provisioning interface naar het USP is volledig onbereikbaar, waardoor geen nieuwe toegangsrechten kunnen worden verleend of ingetrokken. Directe impact op de veiligheid of operationele continuïteit van de luchthaven.
- P2: Een essentiële functie is niet beschikbaar (bijvoorbeeld het self-service portaal of de rapportagemodule), maar de kernfunctionaliteit voor toegangsverlening blijft operationeel. Significante hinder voor gebruikers of beheerders.
- P3: Een specifieke functie of workflow functioneert niet naar behoren, maar er is een workaround beschikbaar. Beperkte impact op de dagelijkse operatie.
- P4: Cosmetische afwijkingen, documentatievragen of verbeterverzoeken zonder directe operationele impact.

Configuration changes:

- Standaard configuratiewijzigingen (nieuwe autorisatiegroep, workflow aanpassing): 5 werkdagen
- Urgente configuratiewijzigingen: 2 werkdagen (na goedkeuring change manager)

10 Kritieke processen

10.1 Uitdiensttreding (KRITIEK)

- Bij markering “Uitdiensttreding” moet toegang **binnen 15 minuten** worden geblokkeerd
- Het systeem moet fail-safe zijn: bij interface-storing met USP moet er **automatisch alarm** naar Security Operations
- **Verificatie:** Inschrijver moet aantonen hoe dit wordt geborgd en hoe dit wordt getest tijdens commissioning
- **Monitoring:** PIAM controleert elk uur of provisioning-interface naar USP actief is, alarm bij > 2 uur downtime

10.2 Bezoeker-host binding

- Bezoekers in SRA moeten **te allen tijde** gekoppeld zijn aan een actieve, aanwezige host
- Bij vertrek host terwijl bezoeker nog aanwezig: **automatisch alarm** naar Security Operations
- Het systeem moet overdracht tussen hosts ondersteunen met volledige audit trail
- Groepsbezoeken: Eén host kan maximaal 10 bezoekers tegelijk begeleiden (configureerbaar)

10.3 Werkvergunningen

- Toegang tot technische ruimtes mag alleen worden verleend indien geldige, goedgekeurde werkvergunning actief is voor die specifieke periode
- Verificatie van werkvergunning moet plaatsvinden **voordat** autorisatie wordt geprovisioned naar USP
- Automatische blokkering bij expiry werkvergunning
- Alarm bij werkvergunningen die >30 dagen actief zijn zonder herziening

11 Acceptance criteria

11.1 Functioneel

Het PIAM-systeem wordt geaccepteerd indien:

- Alle processtappen uit sectie 3 (Badge Center) aantoonbaar functioneren
- Self-service portaal (sectie 4) toegankelijk en werkend is voor alle doelgroepen
- Alle verplichte rapportages uit sectie 5.1 kunnen worden gegenereerd binnen gestelde tijd
- Interfaces uit sectie 6 werkend zijn en gevalideerd
- **Contractor management** volledig functioneel is inclusief delegated administration
- **Visitor management** volledig functioneel is inclusief host-binding en alarmeren

11.2 Performance

- Alle eisen uit sectie 7 zijn aangetoond tijdens commissioning
- Load-test met 100 simultane gebruikers doorstaan zonder performance degradatie
- Provisioning-test individueel én batch conform SLA's uit sectie 9.2

11.3 Veiligheid

- Uitdiensttreding proces (sectie 10.1) gevalideerd: pas werkt niet meer binnen 15 minuten na markering
- Bezoeker-host binding (sectie 10.2) gevalideerd: alarm wordt correct gegenereerd binnen 5 minuten
- Werkvergunning-proces (sectie 10.3) gevalideerd: toegang wordt geblokkeerd bij expiry
- Audit trail compleet: alle wijzigingen traceerbaar met wie, wat, wanneer

11.4 Compatibiliteit

- Systeem werkt met bestaande MIFARE DESFire toegangspassen zonder heruitgifte
- Badge-printers kunnen bestaande passen hercoderen zonder physical replacement

Note: Gedetailleerd commissioningplan met testscenario's wordt door winnende inschrijver opgeleverd conform eis in TPvE Deel 1.

11.5 Wet- en regelgeving & normen

Opdrachtnemer dient te voldoen aan in ieder geval onderstaande (of gelijkwaardig):

- **IEC 62443 of gelijkwaardig:** Cybersecurity voor industriële automatiseringssystemen (minimaal SL2-niveau)
- **ISO 27001 of gelijkwaardig:** Informatiebeveiliging.
- **ISO/IEC 27701 of gelijkwaardig:** Bescherming van persoonsgegevens conform AVG, met o.a. borging van Privacy by design & default.
- **EANV specifiek:** Bijlage P.7 - Handboek Safety en Security.
- **EANV specifiek:** Bijlage J - Security Annex IT en Informatiebeveiliging.

11.6 Security en hardening

Alle servers moeten worden gehardend conform CIS Level 1 benchmark met een minimale score van 90%. Inschrijver is verantwoordelijk voor het uitvoeren van de hardening; EANV ondersteunt op verzoek. Inschrijver neemt een Proof of Concept voor hardening op in het commissioningplan en toont aan dat de applicatie correct functioneert na hardening. Voor aanvullende eisen wordt verwezen naar Bijlage J – Security Annex IT en Informatiebeveiliging.

12 Planning en fasering

12.1 Relatie met Perceel 1

Het PIAM-systeem (Perceel 2) dient te integreren met het Unified Security Platform (Perceel 1). De implementatie van Perceel 2 moet worden afgestemd op de faseringsmomenten van Perceel 1, maar hoeft niet gelijktijdig operationeel te zijn. Het PIAM-systeem zit niet op het kritieke pad richting de go-live datum van 14 juni 2027.

12.2 Fasering

De implementatie van het PIAM-systeem verloopt parallel aan Perceel 1, met de volgende indicatieve fasering:

- **Fase 1 - Configuratie en integratie (Q3-Q4 2026):** Installatie en configuratie van het PIAM-systeem. Aansluiting op testomgeving Perceel 1. Inrichting workflows, autorisatieprofielen en rapportages.
- **Fase 2 - Acceptatietesten (Q4 2026 - Q1 2027):** Uitvoering FAT en SAT. Validatie van integratie met Perceel 1 (provisioning, event feedback). Training Badge Center medewerkers.
- **Fase 3 - Go-live (Q2 2027):** Operationele ingebruikname PIAM-systeem. Overdracht naar beheerorganisatie. Start SLA-verplichtingen.

De exacte planning wordt na gunning in overleg met Opdrachtnemer Perceel 1 en Opdrachtgever vastgesteld. Inschrijver dient in de offerte aan te geven welke doorlooptijd benodigd is voor de implementatie en welke afhankelijkheden er zijn met Perceel 1.

13 Training en kennisoverdracht

Opdrachtnemer verzorgt de volgende trainingen als onderdeel van de implementatie:

- **Training beheerders:** minimaal 2 dagen — configuratie, beheer en troubleshooting van het PIAM-systeem.
- **Training eindgebruikers:** minimaal 1 dag — gebruik van het self-service portaal, aanvraagprocessen en rapportages.