Programma van Eisen (PvE)

Europese Aanbesteding IT Managed Services Stichting Halt

Halt.

Inhoud

1. Doel en context van het PvE

Het PvE heeft als doel om transparant en objectief de verwachtingen van Stichting Halt ten aanzien van IT-dienstverlening te formuleren. De aanbesteding is noodzakelijk vanwege het aflopen van het huidige contract en de wens om de IT-dienstverlening strategisch te herijken. Halt streeft naar een toekomstbestendige, schaalbare en veilige IT-omgeving die hybride werken ondersteunt en aansluit op de cloud-first strategie.

1.1 Aanbestedende organisatie (stichting Halt)

Stichting Halt is een landelijk opererende organisatie met een maatschappelijke opdracht die zich uitstrekt over scholen, wijken, gemeenten, sportverenigingen, ketenpartners en gezinnen. Halt richt zich op het herstellen en voorkomen van grensoverschrijdend gedrag door jongeren en werkt volgens de principes uit het Internationaal Verdrag inzake de Rechten van het Kind (IVRK).
Halt heeft twee kernactiviteiten: interventie en preventie. Interventie is de wettelijke taak waarbij jongeren die strafbaar gedrag hebben gepleegd een Halt-interventie krijgen, zonder dat zij een strafblad ontvangen. Jaarlijks worden ruim 10.000 jongeren doorverwezen naar Halt voor zo'n buitengerechtelijke afdoening.

Daarnaast voert Halt preventieve activiteiten uit voor jongeren die door scholen, sportverenigingen of gemeenten worden doorverwezen na grensoverschrijdend gedrag. Deze jongeren nemen deel aan Halt-schoolinterventies, wijkinterventies of andere herstelgerichte programma's. Halt verzorgt ook regelmatig voorlichtingen op scholen, sportverenigingen en in de wijk.
De organisatie bestaat uit negen teams, verdeeld over vier regio's, met Halt-medewerkers en AO-medewerkers. Elke regio wordt ondersteund door relatiemanagers en een regiomanager. Op centraal niveau bestaat de Halt Service Eenheid met HR, financiën, ICT, facilitair, communicatie, relatiemanagement, beleid en het bestuurssecretariaat. In totaal werken er ongeveer 300 medewerkers en 15–20 stagiaires bij Halt.

Het werk van Halt vindt niet alleen plaats op regiokantoren. Een groot deel van de werkzaamheden wordt uitgevoerd bij ketenpartners op locatie, waaronder scholen, wijkteams, jeugdvoorzieningen, sportverenigingen, gemeenten en politie- of OM-locaties. Daarnaast werken medewerkers thuis of bij ketenpartners op locatie. Hierdoor is de dagelijkse praktijk sterk gedecentraliseerd, mobiel en hybride, en afhankelijk van betrouwbare digitale ondersteuning.

Halt vervult hierin een belangrijke rol als ketenpartner in het veiligheidsdomein en werkt intensief samen met jeugdhulp, politie, het Openbaar Ministerie, Veilig Thuis, schoolbesturen, sportverenigingen, wijkteams en gemeenten. Deze samenwerking vereist een veilige en overal beschikbare digitale werkomgeving en zorgvuldige informatie-uitwisseling.
Deze landelijke en locatieonafhankelijke werkwijze vormt een expliciet uitgangspunt voor deze aanbesteding. De ICT-dienstverlening moet naadloos aansluiten op de praktijk van Halt: mobiel, hybride, maatschappelijk verbonden en actief in honderden lokale en regionale contexten in Nederland.

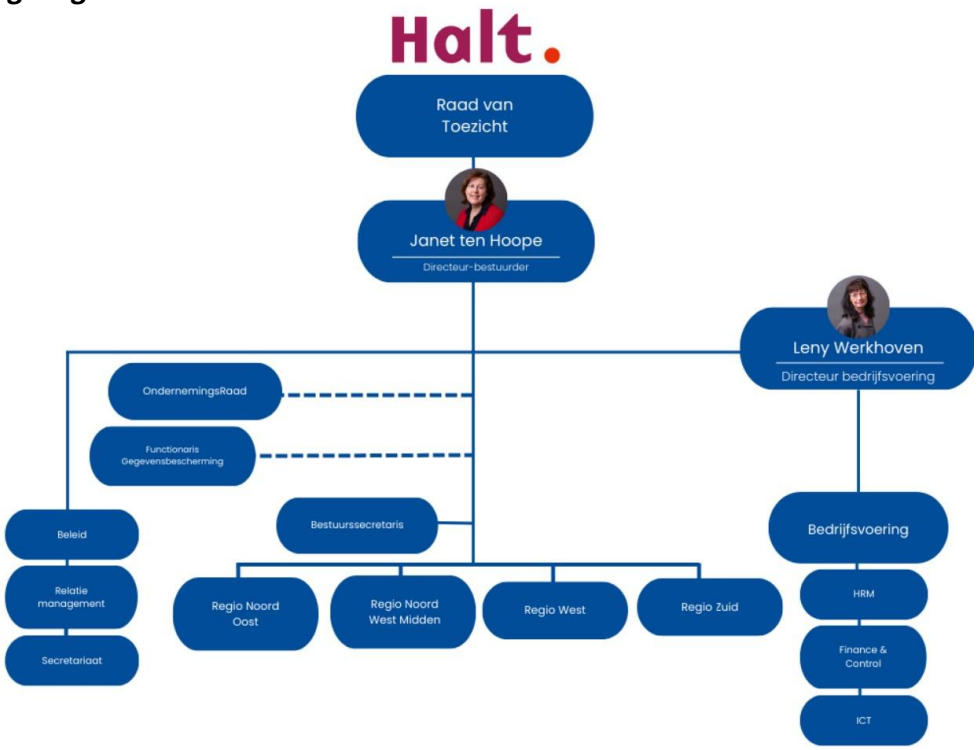
Dit stelt hoge eisen aan betrouwbaarheid, veiligheid en mobiliteit van werkplekken. De MSP moet daarom rekening houden met:

- veilige en tijdige levering van werkplekken op huisadressen van medewerkers;
- ondersteuning van medewerkers die onderweg of bij ketenpartners werken;
- stabiele toegang tot systemen, ongeacht locatie, apparaat of netwerk;
- landelijke beschikbaarheid van onsite-ondersteuning wanneer dat nodig is.

Deze context bepaalt de strategische en operationele eisen die in dit PvE worden gesteld aan de ICT-omgeving, werkplekdienstverlening, servicedesk, logistiek en beveiliging.

Onderstaand organogram toont de actuele organisatiestructuur van Stichting Halt, zoals vastgesteld in het Meerjarenplan 2026–2029. Deze structuur vormt het uitgangspunt voor de inrichting van de regieorganisatie ICT en de samenwerking met de Managed Service Provider.

Organogram Halt:



Stichting Halt werkt landelijk aan het voorkomen en herstellen van grensoverschrijdend gedrag door jongeren. Deze maatschappelijke opdracht vraagt om veilige, wendbare en locatieonafhankelijke ICT-ondersteuning voor alle medewerkers.

Halt.

1.2 Halt als regieorganisatie

Stichting Halt voert de regie over haar bedrijfsvoering en ondersteunende disciplines, waaronder ICT. Dit betekent dat Halt zelf verantwoordelijk blijft voor beleidsvorming, prioritering, informatiebeveiliging, processturing, kwaliteitsbewaking en strategische besluitvorming. De operationele uitvoering van ICT-diensten wordt belegd bij de MSP, maar Halt bewaakt de samenhang, veiligheid, risico's en prestaties via governance, periodieke rapportages en vastgestelde kwaliteitsnormen.

Deze regierol sluit aan bij het Meerjarenplan 2026–2029, waarin Halt inzet op professionalisering van bedrijfsvoering, datagedreven werken, informatiebeveiliging en hybride werken. Binnen deze strategische koers verwacht Halt van leveranciers dat zij voorspelbaar, transparant en in partnerschap samenwerken met de interne regieorganisatie.

1.2.1 Regieorganisatie ICT

De ICT-regieorganisatie van Stichting Halt bestaat uit meerdere rollen die samen verantwoordelijk zijn voor de aansturing van de MSP, kwaliteitsbewaking, security, adoptie en functionele ondersteuning. Halt bewaakt hiermee de samenhang tussen ICT-strategie, dagelijkse uitvoering en gebruikersbeleving.

Informatiemanager

- Bewaakt ICT-strategie, architectuur en informatiebeveiliging (BIO2.0/NIS2).
- Toetst de kwaliteit van MSP-uitvoering en beoordeelt risico's.
- Adviseert directie, MT en projectgroepen op ICT-gebied.

ICT Service Manager *(ICT-regie/ leveranciersmanagement)*

- Verantwoordelijk voor contractmanagement, SLA/XLA-sturing en rapportages.
- Stuurt op incidenten, changes, transitie-activiteiten en dagelijkse voortgang.
- Is primair aanspreekpunt richting de MSP en bewaakt escalaties.

Functioneel Beheer (2fte)

- Ondersteunt gebruikers en applicaties (JOIN, Qlik, SharePoint, Elvy, etc.).
- Test nieuwe functionaliteiten, releases en werkplekken.
- Ondersteunt projecten, onboarding/offboarding en adoptie.

Business Analisten

- Vertalen gebruikersbehoeften en organisatieprocessen naar functionele ICT-wensen.
- Bewaken samenhang tussen applicaties, gegevensstromen en werkprocessen.
- Ondersteunen bij requirements, datakwaliteit en procesoptimalisatie.

Data Scientist

- Versterkt datagedreven werken binnen Halt.
- Analyseert gegevens, bouwt dashboards en levert inzichten voor beleidsvorming.
- Werkt samen met ICT en businessteams aan dataveiligheid en datakwaliteit.

Stagiair ICT

Deze regierollen vormen samen de interne ICT-sturing van Halt. De MSP levert de operationele werkplekdienstverlening, servicedeskfunctie, hosting, netwerk, security en Microsoft 365-beheer. De samenwerking wordt geborgd via SLA's, XLA's en de governance zoals beschreven in hoofdstuk 2.4.

Halt.

1.3 Huidige leverancier

De huidige MSP levert en beheert de volledige werkplekdienstverlening, waaronder laptops, telefoons en randapparatuur. Daarnaast verzorgt de huidige MSP de Servicedesk (1e en 2e lijn), het beheer van de Microsoft 365-omgeving (inclusief Entra ID, Intune en security), en het devicebeheer (MDM/MAM). Ook is de huidige MSP verantwoordelijk voor netwerkbeheer en hosting, inclusief VPN, firewalls, switches en koppelingen met Justitienet, en voor securitybeheer volgens BIO2.0 en NIS2. Verder coördineert de leverancier de vaste en mobiele telefonie (Telepo/Odido) en levert maandelijkse SLA-rapportages en ondersteuning bij onboarding/offboarding. De samenwerking is vastgelegd in SLA's en ondersteund door periodiek overleg en rapportages.

De samenwerking is vastgelegd in servicelevel agreements (SLA's) en wordt ondersteund door maandelijkse rapportages en vaste overlegmomenten. De leverancier ondersteunt bij de onboarding en offboarding van medewerkers, voert wijzigingen door volgens het jaarlijkse ICT-jaarplan en draagt bij aan de uitvoering van maatregelen binnen de Baseline Informatiebeveiliging Overheid (BIO).

De dienstverlening van de huidige leverancier omvat de volgende onderdelen:

- Werkplekbeheer, inclusief onboarding en offboarding
- Servicedesk (eerste en tweede lijn)
- Devicebeheer (laptops, telefoons, switches, firewalls, Accespoints(wifi) en overige netwerkcomponenten)
- Netwerkbeheer en hosting
- Securitybeheer volgens BIO2.0 en NIS2
- Microsoft 365-beheer en licentiebeheer
- Coördinatie van vaste telefonie en mobiele telefonie
- Uitvoeren van ICT-verbeterprojecten

Halt voert zelf de regie op de dienstverlening en bewaakt de aansluiting tussen de operationele uitvoering en de strategische ICT-doelen. De leverancier verzorgt de operationele uitvoering en rapporteert maandelijks over prestaties, incidenten en securitymaatregelen. De huidige situatie vormt het uitgangspunt voor de gewenste toekomstige inrichting zoals beschreven in paragraaf 1.4.

1.4 Gewenste situatie

Stichting Halt streeft naar een IT-dienstverlening die niet alleen betrouwbaar en veilig is, maar ook wendbaar, data gedreven en strategisch van waarde. De aanbesteding is bedoeld om een partner te selecteren die verder kijkt dan uitvoering alleen en actief bijdraagt aan innovatie, continuïteit en de digitale volwassenheid van Halt.
De nieuwe leverancier levert een stabiele, schaalbare en veilige ICT-omgeving die hybride werken ondersteunt en naadloos aansluit op de Cloud-first strategie van de organisatie. Daarbij ligt de nadruk op samenwerking, kennisdeling en een gezamenlijke verantwoordelijkheid voor resultaat.

De gewenste dienstverlening kenmerkt zich door:

- Een toekomstbestendige infrastructuur die flexibel meegroeit met de organisatiebehoefte
- Een moderne werkplekdienstverlening met aantoonbare prestaties op beschikbaarheid, responstijd en gebruikerstevredenheid
- Proactief beheer en monitoring op basis van meetbare indicatoren en data-analyse

- Structurele aandacht voor informatiebeveiliging en compliance, met aantoonbare naleving van BIO en NIS2, onderbouwd door periodieke audits en actuele certificeringen zoals ISO14001, ISO20001, NEN7510 en ISAE3402 type 2.
- Heldere governance en rapportage, met real-time inzicht in prestaties en incidenten
- Een cultuur van samenwerking waarin de leverancier actief adviseert over optimalisatie, kostenbeheersing en innovatie.
- Een dienstverlening waarin de dagelijkse gebruikerservaring centraal staat. Halt verwacht dat de MSP actief aandacht besteedt aan medewerkerstevredenheid, werkplekfricties en de kwaliteit van de ondersteuning. De menselijke kant van dienstverlening is een expliciet onderdeel van de beoordeling.

Halt behoudt de regierol over de ICT-strategie, terwijl de leverancier verantwoordelijk is voor de operationele uitvoering, risicobeheersing en structurele verbeteringen. De samenwerking is gebaseerd op vertrouwen, transparantie en een gedeeld commitment aan kwaliteit, veiligheid en toekomstgerichtheid.

1.4.1 Regie-principes

Stichting Halt voert de regie op de ICT-dienstverlening: Halt bepaalt beleid, architectuur en prioritering. De MSP levert de operationele uitvoering en is SPOC via de Servicedesk. We sturen op transparantie, voorspelbaarheid en continue verbetering: SLA's voor performance, XLA's voor gebruikersbeleving. Escalaties, besluitvorming en rapportages volgen de governance in hoofdstuk 2.4.

2. Scope en eisen van de opdracht

Stichting Halt wil met deze aanbesteding een ICT-managed services partner contracteren die verantwoordelijk is voor de continuïteit, kwaliteit en veiligheid van de volledige ICT-dienstverlening. De opdracht omvat het integraal beheren, ondersteunen en doorontwikkelen van de ICT-omgeving van Halt, zodat medewerkers efficiënt, veilig en plaats-onafhankelijk kunnen werken.

De leverancier biedt een samenhangende dienstverlening waarin werkplekbeheer, servicedesk, netwerk- en hostingbeheer, Microsoft 365-beheer, securitymanagement en telefoniecoördinatie volledig op elkaar zijn afgestemd. Daarbij ligt de nadruk op betrouwbare dienstverlening, gebruikerstevredenheid, informatiebeveiliging en proactieve samenwerking met het interne ICT-team van Halt.

De leverancier vervult een brede rol die verder gaat dan technisch beheer. Van de partner wordt verwacht dat hij:

- De dagelijkse operationele ICT-diensten uitvoert en bewaakt
- Knelpunten signaleert en structureel verbetervoorstellen aandraagt
- Actief meedenkt over innovatie, cloudadoptie en procesoptimalisatie
- Halt ondersteunt bij strategische besluitvorming met data, rapportages en advies.

De dienstverlening strekt zich uit over alle locaties van Stichting Halt in Nederland, zoals opgenomen in bijlage C van het PvE. Ondersteuning wordt zowel op afstand als op locatie geboden, afhankelijk van de behoefte. De leverancier is verantwoordelijk voor stabiele en veilige werkplekken, actuele software en een goed functionerende ICT-infrastructuur.

Naast de reguliere instroommomenten kent Stichting Halt jaarlijks twee vaste instroomgolven van stagiaires. Tijdens deze perioden ontstaat extra vraag naar nieuwe werkplekken, logistieke capaciteit, servicedeskondersteuning en onboardingactiviteiten. De MSP dient hier proactief op te anticiperen door voldoende capaciteit, voorraad en ondersteuning beschikbaar te hebben, zodat alle stagiaires tijdig een volledig ingerichte werkplek op het huisadres ontvangen.

De leverancier werkt nauw samen met het interne ICT-team van Halt, dat de regie voert over beleid, prioriteiten en architectuur. De leverancier neemt verantwoordelijkheid voor de uitvoering, het naleven van de afgesproken serviceniveaus (SLA's) en het voldoen aan de normen voor informatiebeveiliging (BIO en NIS2).

De samenwerking is gericht op partnerschap, transparantie en continue verbetering van de dienstverlening, zodat de ICT-functie van Halt toekomstbestendig, veilig en wendbaar blijft.

2.1 Diensten binnen de scope

2.1.1 Werkplekbeheer en devicebeheer:

De leverancier is verantwoordelijk voor het leveren, installeren, configureren, beheren en onderhouden van alle werkplekken en bijbehorende randapparatuur binnen Stichting Halt. Dit betreft onder andere laptops, mobiele telefoons, switches, firewalls, access points, multifunctionals en overige netwerkcomponenten.

De leverancier mag hiervoor gebruikmaken van onderaannemers of partners, mits de dienstverlening integraal wordt aangeboden en Halt één aanspreekpunt heeft (Single Point of Contact, SPOC). De MSP blijft verantwoordelijk voor de volledige regie en coördinatie, ook als onderdelen van de dienst door derden worden geleverd, zoals multifunctionals..

Halt neemt de werkplekdienst af tegen een vast bedrag per werkplek per maand. De wijze waarop de leverancier deze dienst intern organiseert (bijvoorbeeld via lease, koop of andere constructie) is diens eigen verantwoordelijkheid. Halt sluit geen afzonderlijke leasecontracten af met derden.

Het volledige traject van aanvraag tot retourname van hardware verloopt als volgt:

- **Aanvraagfase:** Halt meldt via het overeengekomen kanaal een nieuwe werkplek of vervanging aan. De leverancier verwerkt deze aanvraag binnen de afgesproken reactietermijn.
- **Voorbereiding en configuratie:** De leverancier zorgt voor tijdige beschikbaarheid van hardware en voert de benodigde configuraties uit volgens de standaarden van Halt.
- Dit omvat software-installatie, beveiligingsinstellingen via MDM/MAM en koppeling aan Intune of Apple Business Manager.
- **Levering en ingebruikname:** De werkplek wordt geleverd op het huisadres van de medewerker. De leverancier garandeert dat de werkplek direct inzetbaar is voor de eindgebruiker.
- **Beheerfase:** Gedurende de afgesproken levensduur voert de leverancier proactief beheer uit, inclusief updates, monitoring en ondersteuning.
- **Retourname en afhandeling:** Bij einde levensduur of vervanging haalt de leverancier de hardware op, voert dataverwijdering uit volgens geldende normen en zorgt voor correcte afhandeling (bijvoorbeeld recycling of lease-retour).

Hardware wordt centraal beheerd via Microsoft Intune en Apple Business Manager. De leverancier richt automatische softwaredistributie en beveiligingsinstellingen in via Mobile Device Management (MDM) en Mobile Application Management (MAM). Handleidingen en gebruiksprocedures worden in het Nederlands aangeleverd, zodat medewerkers zelfstandig en veilig met de systemen kunnen werken.

De leverancier ondersteunt bij onboarding en offboarding van medewerkers en zorgt dat nieuwe werkplekken volledig gebruiksklaar zijn.

2.1.2 Servicedesk:
De leverancier verzorgt eerstelijns- en tweedelijnsondersteuning voor alle medewerkers van Halt. Medewerkers kunnen meldingen indienen per telefoon, of via een ticketsysteem. Alle meldingen worden in het Nederlands afgehandeld en geregistreerd in een centraal portaal.

De leverancier levert maandelijks servicelevel rapportages (SLR) met de afgesproken KPI's en prestatiegegevens, inclusief een overzicht van security-incidenten, kwetsbaarheden (zoals CVE's) en genomen beveiligingsmaatregelen. Ondersteuning vindt plaats op afstand of op locatie, afhankelijk van de aard en ernst van het incident. De leverancier waarborgt dat de Servicedesk goed bereikbaar is en dat meldingen tijdig en correct worden afgehandeld volgens overeengekomen serviceniveaus.

Omdat gebruikersbeleving een strategisch speerpunt is voor Stichting Halt, wordt van de MSP verwacht dat de Servicedesk niet alleen technisch correct handelt, maar ook communicatief sterk is. De Servicedesk van de MSP is het centrale en eerste aanspreekpunt (SPOC). De MSP borgt dat medewerkers zich geholpen, serieus genomen en tijdig geïnformeerd voelen. Dit wordt meegenomen in de XLA-rapportage.

2.1.3 Microsoft 365- en licentiebeheer:
De leverancier beheert de volledige Microsoft 365-omgeving van Halt, inclusief Entra ID, Intune, het Adobe-portaal en overige beheerportalen. Dit omvat gebruikersbeheer, licentiebeheer, logging, updates en beveiliging.

2.1.4 Hosting en netwerkbeheer
De leverancier beheert en onderhoudt de netwerk- en hostingomgeving van Halt, bestaande uit vijf locaties. Binnen het netwerk worden door de leverancier twee SSID's beheerd: één voor medewerkers en één voor gasten.

De leverancier waarborgt dat medewerkers van Stichting Halt veilig, betrouwbaar en zonder beperkingen kunnen werken, ongeacht tijd en locatie. Dit betekent dat de ICT-diensten en bedrijfsapplicaties altijd toegankelijk zijn, volgens de eisen voor beschikbaarheid, beveiliging en gebruiksgemak zoals vastgelegd in het PvE. De invulling van deze functionaliteit is aan de leverancier, mits aantoonbaar aan de gestelde normen voldaan wordt.

2.1.5 Securitybeheer:
De leverancier is verantwoordelijk voor het waarborgen van de informatiebeveiliging binnen de ICT-omgeving van Halt. Daarbij gelden de Baseline Informatiebeveiliging Overheid (BIO2.0) en de richtlijnen vanuit NIS2 als uitgangspunt.

De leverancier zorgt dat kritische partners aantoonbaar ISO 27001-gecertificeerd zijn en dat authenticatie- en autorisatieprocessen correct zijn ingericht volgens de autorisatiematrix van Halt. Fouten in toegangsbeheer of authenticatie worden actief gesignaleerd en verholpen.

De leverancier voert jaarlijks een onafhankelijke audit uit, zoals een ISAE 3402 type 2-verklaring en/of een ISO 27001-certificeringsaudit. De resultaten van deze audit worden gedeeld met Stichting Halt. Indien relevant worden ook audits volgens BIO2.0 en NEN7510 uitgevoerd.

De leverancier rapporteert periodiek over de beveiligingsstatus en adviseert over verbetermaatregelen. Halt maakt gebruik van een externe SIEM-SOC-dienst voor monitoring en incidentdetectie. Deze partij dient gecontroleerde en beveiligde toegang te hebben tot specifieke omgevingen van Halt, waaronder de netwerk- en serverinfrastructuur, Microsoft 365-tenant (incl. Entra ID en Intune), en relevante logging- en monitoringplatformen. Toegang wordt verleend op basis van het least-privilege-principe en moet voldoen aan de BIO2.0- en NIS2-richtlijnen. Authenticatie vindt plaats via MFA en alle activiteiten worden gelogd en periodiek geaudit.

2.1.6 Coordinatie telefonie
De leverancier coördineert telefonie in samenwerking met de telecomprovider. Medewerkers binnen Nederland moeten onbeperkt kunnen bellen en gebruik maken van internet. Roaming is standaard uitgeschakeld op abonnementsniveau, zodat medewerkers dit niet zelf kunnen activeren.

De leverancier fungeert als single point of contact (SPOC) voor alle telefonie gerelateerde vragen en incidenten en zorgt voor een goed afgestemde afhandeling met de telecomprovider.

2.2 Applicaties binnen en buiten scope
De MSP levert technisch enablement en platformbeheer voor Microsoft 365 (incl. Entra ID/Intune/Defender), identity & access (MFA/Conditional Access), endpoint-compliance, netwerk & security, en levert SSO/CA/connectiviteit richting businessapplicaties. Functioneel beheer van businessapplicaties valt buiten scope, tenzij expliciet anders belegd. Binnen scope (technisch enablement/platform):
Microsoft 365-tenant (Entra ID, Intune, Teams, SharePoint technisch, Outlook/Exchange), VPN/ADFS/DC's/IronPort/monitoring, netwerkbeheer (5 locaties, 2 SSID's) en koppelingen (o.a. Justitienet).

2.2.1 Coördinatie-only:
Telefonie via externe leverancier (Telepo/Odido); MSP als SPOC. Beleidsuitgangspunt: NL onbeperkt bellen/data; roaming uit op abonnementsniveau.

Buiten scope:
De volgende onderdelen vallen buiten de scope van deze aanbesteding:

- Functioneel beheer van applicaties zoals JOIN, Educatieportaal, Qlik Sense, DWH, HINT (SharePoint), Youforce, Reisbalans, Elvy en AccountView
- Beheer en onderhoud van audiovisuele middelen zoals touchscreens, VR-brillen Frankeermachines
- Specifieke softwareontwikkeling of maatwerkapplicaties

2.2.2 Overig applicatielandschap:

JOIN NOW, Fileshare, Zoho, Qlik Sense Server, YouForce HR Core, Enable-U, Veilig Thuis, Multisignaal, Visma, JobPromo website, WhatsApp SSU, VR-app, Toestemming SSU (website formulieren), Postmark, Formulier SSU website, Power BI. Voor deze applicaties levert indien mogelijk de MSP SSO/CA, endpoint-compliance en connectiviteit waar relevant.

2.3 Verwacht resultaat

De leverancier levert een volledig beheerde ICT-dienstverlening die medewerkers in staat stelt veilig, efficiënt en locatieonafhankelijk te werken. De dienstverlening is proactief, schaalbaar en toekomstgericht, met aantoonbare focus op betrouwbaarheid, beveiliging en gebruiksgemak.

De samenwerking met Stichting Halt is gebaseerd op transparantie, professionaliteit en wederzijds vertrouwen. De leverancier levert periodieke rapportages, signaleert risico's tijdig en doet concrete verbetervoorstellen. Op deze manier draagt de leverancier actief bij aan de digitale volwassenheid en strategische ambities van Stichting Halt.

2.4 Regie-organisatie en governance

Deze paragraaf borgt heldere verantwoordelijkheden, besluitvorming, overleg en rapportage tussen Stichting Halt (regie) en de MSP (uitvoering).

2.4.1 Rollen en verantwoordelijkheden

- **Halt (regie):**
  - ICT-beleid, architectuurkaders en prioritering (jaarplan/kwartaalprioriteiten).
  - Leveranciersmanagement en contractbewaking (SLA, XLA, compliance BIO2.0/NIS2/AVG).
  - Acceptatie van changes en project-gateways.
  - Security-beleid en risicosturing (DPIA's, auditplanning, mitigaties).
- **MSP (uitvoering):**
  - End-to-end operationele levering van de managed services.
  - Landelijke ondersteuning en bereikbaarheid
  - Proactieve monitoring, capaciteits- en probleembeheer; structurele verbetervoorstellen.
  - SPOC/Servicedesk voor alle eindgebruikers; juiste routering en eigenaarschap tot oplossing.
  - Dossieropbouw en rapportage (SLA/KPI's, XLA, security-events, root-cause reports).
- **Derdenleveranciers:** MSP coördineert technische afstemming; Halt bewaakt contracten op hoofdlijnen.

De Servicedesk van de MSP is het centrale en eerste aanspreekpunt (SPOC) voor alle medewerkers van Halt (incidenten, serviceverzoeken, vragen). MSP bewaakt end-to-end voortgang, ook wanneer derden betrokken zijn, en communiceert tijdig en begrijpelijk.

2.4.2 Overlegstructuur

- **Operationeel overleg (wekelijks of 2-wekelijks, 30 min)**
  Doel: lopende incidenten/problems/changes, capaciteit, open acties.
  Deelnemers: Servicedesk lead MSP, Functioneel Beheer Halt, ICT Service Manager.
- **SLA/XLA-review (maandelijks, 60–90 min)**
  Doel: performance (SLA), beleving (XLA), trends, verbeteracties, security-status.
  Deliverables: SLR incl. KPI's, MTTP (Mean Time to Productivity), CSAT (Customer Satisfaction Score), NPS (Net Promoter Score)/werkplekbeleving.
- **Kwartaalboard (strategisch, per kwartaal, 90–120 min)**
  Doel: roadmap, architectuurfit, kosten/waarde, risico's/audits, innovatie en besluitvorming.
  Deelnemers: Directeur Halt, Directeur MSP, ICT-manager Halt (voorzitter), MSP-servicemanager, CISO/Privacy officer (adviserend).

2.4.3 Escalatie (functioneel & hiërarchisch)

Doel. Escalatie zorgt voor snelle bijsturing bij verstoringen, structurele tekortkomingen of samenwerkingsproblemen, met duidelijke eigenaarschap, doorlooptijden en communicatieafspraken, volgens het interne *Escalatieproces IT-Leveranciers* van Stichting Halt.

A. Escalatieniveaus, triggers en doorlooptijden

- **Niveau 1 – Operationeel**
  Trigger: eenmalige verstoring of SLA-afwijking.
  Actiehouder: Functioneel Beheer Halt.
  Doorlooptijd start: binnen 1 werkdag; handmatige opvolging in regulier operationeel overleg.

- **Niveau 2 – Tactisch**
  Trigger: herhaling/structureel probleem of impact op meerdere processen.
  Actiehouder: ICT Service Manager (dossiervorming, regie).
  Doorlooptijd start: overleg met leverancier binnen 3 werkdagen; wekelijks voortgang en, waar nodig, aanscherping van contractafspraken. [

- **Niveau 3 – Strategisch**
  Trigger: kritieke verstoring, (dreigende) contractbreuk of ernstige nalatigheid.
  Actiehouder: Informatiemanager en/of Directeur Bedrijfsvoering (besluitvorming/maatregelen).
  Doorlooptijd start: escalatie binnen 5 werkdagen; juridische toetsing en besluitvorming over maatregelen.

NB: Zodra een issue operationeel overstijgend is, classificeert Halt dit als tactisch en valt het onder regie van de ICT Service Manager.

B. Stappen en communicatie (per niveau)

1. **Signalering & registratie**
   ICT Service Manager registreert issues (datum, leverancier, omschrijving, classificatie) en wijst het niveau toe.

2. **Start escalatie & informeren**
    - N1: intern informeel melden.
    - N2: Informatiemanager betrekken.
    - N3: ook Directeur Bedrijfsvoering informeren.
      MSP/leverancier ontvangt het formele herstelverzoek met termijnen.
3. **Overleg & maatregelen**
   ICT Service Manager organiseert (vanaf N2) overleg; legt herstelacties, termijnen en eigenaarschap schriftelijk vast (mail/verslag). Actielijst en voortgangsoverzicht worden beheerd bij N2/N3.
4. **Monitoring & updates**
   ICT Service Manager bewaakt voortgang. Bij N2/N3: minimaal wekelijkse interne update aan Informatiemanager; leverancier levert periodieke statusrapportage. Extra drukmiddelen kunnen worden ingezet als voortgang uitblijft.
5. **Evaluatie & afsluiting**
   Na oplossing: evaluatie op oplossingskwaliteit, snelheid en samenwerking; bevindingen gaan naar kwartaalreview/scorecard en worden als lessons learned gedeeld.

C. Rapportage en sturing

- Maandelijks: de SLR bevat escalatie-overzicht, oorzaken (RCA), trends en corrigerende maatregelen.
- Per kwartaal: bespreekt Halt de leveranciers-scorecard (aard/ernst issues, reageren/oplossen, communicatie, herhaling/verbeterpotentieel) met interne stakeholders en, indien relevant, met de leverancier. Dit kan leiden tot bijsturing of strategische escalatie.

D. Maatregelen bij structurele tekortkomingen

Afhankelijk van ernst en herhaling kan Halt maatregelen nemen: formele waarschuwing/ingebrekestelling, aanpassing SLA/contract, bevriezing opdrachten/projecten, beëindiging samenwerking.

3. Kwaliteitscriteria

De leverancier moet voldoen aan de volgende prestatie- en kwaliteitsnormen:

- **Beschikbaarheid:**
  Minimaal 99,8% uptime voor werkplekdiensten en infrastructuur. De responstijd in productieprocessen moet aantoonbaar stabiel blijven, ook bij piekbelasting. In kritieke situaties (zoals verstoringen met impact op bedrijfscontinuïteit) moet de leverancier binnen één uur reageren en herstelmaatregelen inzetten.

- **Serviceniveau – afhandeling van incidenten:**

    - *Kritiek:* binnen 4 uur opgelost of werkbare noodoplossing beschikbaar
    - *Hoog:* binnen 1 werkdag afgehandeld.
    - *Standaard:* binnen 2 werkdagen afgehandeld.
- **Gebruikerstevredenheid:** Minimaal een gemiddelde score van 8, gemeten via een gebruikersenquête die 2 keer per jaar wordt uitgevoerd.
- **Certificeringen:** De leverancier beschikt over actuele certificeringen voor informatiebeveiliging en kwaliteitsmanagement, minimaal ISO 27001 en ISO 9001, ISO14001, ISO20001, NEN7510 en ISAE3402 type 2
- **Escalatieprocedure:** Er is een duidelijke en aantoonbaar werkende escalatieprocedure beschikbaar voor incidenten en klachten.

- **Changebeheer en compliance:** De leverancier ondersteunt actief bij changebeheer en naleving van relevante wet- en regelgeving, waaronder de AVG en de uitvoering van Data Protection Impact Assessments (DPIA's).

3.1 Kwaliteitseisen laptops en telefoons

De standaardlaptop die door de leverancier wordt aangeboden, is qua specificaties gelijkwaardig aan de Dell Pro 16 en voldoet minimaal aan de volgende eisen:
Touchscreen
Intel Core i5 of i7 processor
16 GB RAM
Minimaal 512 GB SSD
Wi-Fi 6E
Thunderbolt 4
Volledige compatibiliteit met Windows Autopilot en Microsoft Intune
Ondersteuning voor BitLocker en remote BIOS-beheer
TPM 2.0 aanwezig
On-site Next Business Day (NBD) garantie

De laptop voldoet aan de geldende BIO2.0- en NIS2-vereisten en is geschikt voor centraal beheer via Mobile Device Management (MDM) en Mobile Application Management (MAM).

De economische levensduur van de laptop wordt door Halt vastgesteld en contractueel vastgelegd, bijvoorbeeld op 48 maanden. Touchscreenfunctionaliteit is verplicht. Alle laptops die onder dit contract worden geleverd, beschikken standaard over een touchscreen. Touchscreen is onderdeel van de gelijkwaardigheidseis en is niet optioneel. Migratie van laptops vindt plaats bij het bereiken van deze termijn. Vervanging vóór het einde van de levensduur is uitsluitend aan de orde als de hardware aantoonbaar niet meer voldoet aan vooraf vastgelegde technische minimumspecificaties, zoals compatibiliteit met Windows Autopilot, aanwezigheid van TPM 2.0, of andere objectief meetbare prestatiecriteria.

Halt heeft een duidelijke voorkeur voor een iOS-werktelefoon.
Voor mobiele telefonie geldt dat de iPhone SE 2022 als referentieniveau wordt gehanteerd. Omdat dit model niet meer leverbaar is, geldt "gelijkwaardig aan iPhone SE 2022" als kwaliteitscriterium voor formaat, prestaties, gebruiksgemak, beveiliging en beheersbaarheid.

De leverancier levert aan iedere medewerker een volledige, gebruiksklare werkplek volgens de onderstaande gebruikersaspecten:

1. **Standaard hardwarepakket**
    - Laptop (gebruiksklaar, Autopilot/Intune ready)
    - Smartphone incl. oplader en oortjes,
    - Hotspot mogelijkheid voor remote werken.
    - Hoesje met val- en stootbescherming
    - Headset (Teams-geschikt)
    - Stroomadapters en noodzakelijke bekabeling

2. **Bescherming & randvoorwaarden**
    - Telefoonhoesjes moeten voldoen aan een minimale beschermingsklasse (valbestendig, stootabsorberend).

- Laptops moeten beschikken over een stevige behuizing met basis-valbescherming.

3. **Touchscreen-functionaliteit**
   - Alle laptops dienen een touchscreen mogelijkheid te hebben.
4. **Gebruikersomgevings-eisen**
   - Maximaal gewicht laptop: ≤ 2,0 kg
   - Batterijduur van minimaal 8 uur actief gebruik
   - Volledige ondersteuning van hybride werken
   - Stil en energiezuinig ontwerp (kantoor-geschikt)
   - Privacy scherm voor elke laptop
   - Webcam afscherming.

3.1.1 Levering aan huis

De leverancier levert nieuwe laptops, telefoons en vervangende hardware veilig en tijdig op huisadressen van medewerkers. Levering vindt plaats via secure courier, inclusief track-and-trace en schokbestendige verpakking. De werkplek is direct inzetbaar bij ontvangst.

4. Overdrachteisen werplek devices bij contractwissel

Bij beëindiging van het contract is de vertrekkende MSP verplicht om alle relevante configuraties, registraties en beveiligingsinstellingen over te dragen aan Stichting Halt. Dit omvat onder meer:

- Intune- en Apple Business Manager (ABM)-registraties
- Autopilot-profielen en MDM/MAM-configuraties
- Encryptiesleutels (BitLocker), BIOS-wachtwoorden en security policies
- Documentatie van alle relevante configuraties en beheerinstellingen

4.1 Exit-strategie en offboarding van devices

Bij offboarding van devices dient de MSP zorg te dragen voor:

- Veilige datawissing
- Ontkoppeling van MDM/ABM-platformen
- Teruglevering aan de leasemaatschappij volgens leasecontract
- Verwijdering van bedrijfsdata en accounts

De MSP stemt de exit-strategie af met zowel Stichting Halt als de leasemaatschappij, zodat overdracht en offboarding compliant en risicoloos verlopen.

5. Transitie- en Migratie-eisen

Dit hoofdstuk beschrijft de eisen voor de overgang van de huidige ICT-dienstverlening naar de nieuwe MSP. De volledige transitie en migratie vallen binnen de scope van de opdracht en zijn inbegrepen in de inschrijfprijs. De MSP is verantwoordelijk voor een gecontroleerde, veilige en minimale verstorende overdracht van alle werkplekdiensten, devices en ondersteunende processen

Halt.

5.1 Doel en uitgangspunten

De transitie heeft als doel:

- Een soepele overdracht van dienstverlening van de huidige MSP naar de nieuwe MSP;
- Continuïteit van de bedrijfsvoering zonder verstoring voor medewerkers;
- Tijdige en volledige migratie van alle werkplekken, telefoons en beheerdiensten;
- Directe beschikbaarheid van een volledig operationele ICT-omgeving volgens de eisen in het PvE.

Leidende principes:

- Continuïteit eerst – voorkomen van productiviteitsverlies;
- Minimale impact voor eindgebruikers;
- Veiligheid en compliance tijdens de gehele transitieperioden;
- Volledige verantwoordelijkheid bij de MSP.

5.2 Verplicht transitie- en migratieplan (bij inschrijving)

De MSP levert bij inschrijving een uitgewerkt transitie- en migratieplan aan. Dit plan bevat minimaal:

5.2.1 Fasering van de transitie

- Intake en overdracht van documentatie, configuraties, accounts en technische instellingen;
- Pilotmigratie (5–10% gebruikers);
- Gefaseerde migratie per regio/kantoor;
- Landelijke uitrol;
- Nazorgfase tot volledige stabilisatie.

5.2.2 Migratiescope

Het transitieplan omvat in ieder geval:

- Vervanging en uitgifte van laptops;
- Vervanging en uitgifte van mobiele telefoons en accessoires;
- Configuratie en enrolment via Autopilot, Intune, MDM-profielen en security policies;
- Overzetten van instellingen, profielen, MFA en toegangsrechten;
- Ontkoppeling van oude apparaten uit Intune/MDM/ABM;
- Retourname en veilige verwerking van oude apparatuur.

5.2.3 Logistieke uitvoering

De MSP organiseert alle logistieke activiteiten, waaronder:

- Levering van de werkplek op huisadressen van medewerkers via secure courier verzending met track-and-trace;
- Schokbestendige verpakking en veilige handling;
- onsite-ondersteuning waar nodig;
- Beschikbaarheid van fallback/loaner-apparatuur voor noodgevallen.

5.2.4 Wisselen van laptops en telefoons

Het plan bevat een uitgewerkte strategie voor:

- Distributie en uitrol van nieuwe devices naar alle regioteams;
- Gebundelde uitlevermomenten per kantoor/regio;
- Individuele levering aan locatieonafhankelijke medewerker;
- Configuratie en directe inzetbaarheid van iedere werkplek.

Voor medewerkers die locatieonafhankelijk werken, waaronder thuiswerkende medewerkers en medewerkers die veel op pad zijn naar scholen, gemeenten of ketenpartners moeten laptops en telefoons veilig en tijdig kunnen worden geleverd op het huisadres van de medewerker.
De MSP moet hier standaard in voorzien, inclusief secure courier, track-and-trace en schokbestendige verpakking. Levering aan huisadressen geldt zowel voor initiële uitrol, vervangingen als tijdens de transitie.

5.2.5 Servicedesk tijdens transitie

De MSP levert een **vaste kern servicedeskmedewerkers** gedurende de gehele transitie, die:

- Volledig aan Halt zijn toegewezen;
- Aantoonbaar zijn opgeleid in Halt-processen, applicaties en kritische werkwijzen;
- Migratievragen direct oppakken;
- Op locatie inzetbaar zijn indien nodig.

5.2.6 Rol Functioneel Beheer Halt (FB)

- Halt stelt Functioneel Beheer tijdelijk vrij voor transitieactiviteiten;
- MSP ondersteunt FB met extra capaciteit;
- MSP levert indien nodig fysieke ondersteuning op regiokantoren.

5.2.7 Risicoanalyse en mitigerende maatregelen

Het plan bevat een risicoanalyse, inclusief:

- Risico’s op verstoringen, capaciteitstekorten en afhankelijkheden;
- Maatregelen voor continuïteitsborging;
- fallback- en escalatiescenario’s.

5.3 Geen extra kosten (all-in transitie)

De volledige transitie en migratie zijn inbegrepen in de inschrijfprijs. De MSP brengt geen aanvullende kosten in rekening voor:

- Implementatieactiviteiten;
- Logistiek, verzending en koerierskosten;
- Werkplekwissels, telefoniewissels en gebruikerscommunicatie;
- Inzet van servicedeskmedewerkers tijdens transitie;
- Projectmanagement en technische ondersteuning;
- Configuratie, enrolment en beveiligingsinrichting.

Alle kosten vallen onder de aangeboden prijs voor werkplekdienstverlening.

5.4 Acceptatiecriteria transitie

De transitie is pas afgerond wanneer aan alle onderstaande eisen is voldaan:

1. Alle medewerkers zijn gemigreerd en kunnen volledig werken op de nieuwe werkplek.
2. Alle devices functioneren volgens hoofdstuk 3.1 (hardware-eisen).
3. Servicedesk werkt stabiel en voldoet aan de afgesproken SLA's.
4. Devicebeheer, securityprofielen en policies zijn volledig operationeel.
5. Kritieke meldingen zijn opgelost en er is geen productiviteitsimpact meer.
6. Restpunten worden binnen 10 werkdagen opgelost.
7. MSP levert volledige documentatie op (transitierapport, configuraties, risico's, nazorgregister

5.5 Overdracht naar reguliere dienstverlening

Na afronding van de transitie:

- Wordt de dienstverlening formeel overgedragen aan de reguliere SLA-/XLA-structuur;
- Worden alle beheerprocessen geactiveerd volgens hoofdstuk 2.4 (regie & governance);
- Wordt de MSP volledig verantwoordelijk voor de stabiliteit, security en continuïteit van de dienstverlening

6. Selectiecriteria (minimum Eisen)

- Minimaal 5 jaar ervaring met soortgelijke dienstverlening
- Ervaring bij ten minste 2 organisaties van vergelijkbare omvang (100–500 werkplekken)
- Bereidheid tot samenwerken met externe leveranciers
- Nederlandstalige Servicedesk voor alle eindgebruikers, bereikbaar tijdens kantooruren
- Securitybeheer volgens BIO2.0 en NIS2
- Actuele certificeringen: minimaal ISO 27001 en ISO 9001
  Jaarlijkse onafhankelijke audit
- Aantoonbare ervaring met samenwerking met externe leveranciers
- Volledige Werkplek-dienstverlening incl. lifecycle-management
- Performance – Selectiecriterium: aantoonbaar minimaal basisniveau stabiliteit & continuïteit

7. Functionele eisen

- De leverancier biedt ondersteuning voor hybride werkvormen (cloud-first strategie)
- Er wordt proactief beheer gevoerd op updates, patches en securitymeldingen
- Devices worden centraal beheerd en voldoen aan de veiligheidsnormen van Halt
- Inzichtelijke rapportages worden maandelijks aangeleverd (incidenten, performance, verbruik)
- SSO-ondersteuning en self-service portaal
- Automatisering onboarding/offboarding

8. Technische eisen (indicatief)

- Volledige integratie met Microsoft 365-omgeving
- Support voor Azure Active Directory en Intune
- Monitoringtools zijn toegankelijk voor Halt ter inzage
- Support voor Conditional Access, MFA

Halt.

9. Prestatie-eisen/ KPI's

- SLA's vastgelegd in contract (minimaal zoals bij huidige leverancier)
- Meetbare KPI's:

10. Incidentafhandeling (reactie- en oplostijden) – kritiek voor Halt

Voor Halt is de continuïteit van het dagelijkse werk cruciaal: de werkplek is waar het werk gebeurt. Medewerkers werken door heel Nederland en moeten altijd snel door kunnen. Dit hoofdstuk is daarom een sleutelonderdeel van het contract: het bepaalt hoe snel de MSP reageert, oplost en – waar nodig – direct een vervangende werkplek (laptop/telefoon) levert zodat medewerkers weer kunnen werken.

10.1 Prioriteitenmodel (P1–P4)

P1 – Kritiek (bedrijf kritieke hinder/ dienstverlening ligt stil)
Situaties:

- Onbeschikbaarheid Microsoft 365, netwerk, VPN of kernapplicaties met brede impact.
- Security-incident met hoog risico (bijv. datalek, actieve aanval).
- Context-uplift (één medewerker) kritieke taak/rol waardoor bedrijfscontinuïteit of reputatie wordt geraakt.

Reactietijd: ≤ 15 min (telefonisch contact verplicht)
Oplostijd: ≤ 4 uur, of noodoplossing binnen 4 uur
Communicatie: statusupdate elke 30 min

De genoemde criteria zijn indicatief. Eén of meerdere factoren kunnen aanleiding zijn om een incident als P1 te classificeren. De beoordeling gebeurt op basis van impact op continuïteit, veiligheid en de publieke taak van Halt.

P2 – Hoog (organisatiebrede hinder/ team of locatie kan niet werken)
Situaties:

- Meerdere teams/locaties/regio's met substantiële hinder.
  Reactietijd: ≤ 1 uur · Oplostijd: ≤ 8 uur · Updates: elke 2 uur

P3 – Medium (individuele hinder/ werk kan deels door)
Situaties:

- Eén medewerker of klein team met hinder (software, rechten, netwerk, hardware).
  Reactietijd: ≤ 4 uur · Oplostijd: ≤ 24–32 uur · Updates: dagelijks

P4 – Laag (informatie, advies, standaardaanvragen)
Situaties:

- Vragen, lichte verstoringen of standaard service requests (accounts, rechten, autorisaties).
  Reactietijd: ≤ 1 werkdag · Oplostijd: ≤ 5 werkdagen · Updates: op afgesproken datum

10.1.2 Context-gebaseerde P1-uplift (één medewerker)

Een incident dat één medewerker treft krijgt P1 als cumulatief geldt:

- De medewerker heeft nu een kritieke rol of tijdkritische verplichting (bijv. directie/woordvoering, crisisoverleg, zitting/rechtszaak, les/voorlichting aan een klas of grote groep, bestuurlijk overleg met ketenpartners);

- Er is directe impact op continuïteit, veiligheid, publieke taak of reputatie van Halt;
- De medewerker kan zijn/haar taak niet uitvoeren.

Afhandeling: zelfde normen als P1 (reactie ≤15 min, updates elke 30 min, oplossing/noodoplossing ≤4 uur). De Servicedesk markeert het ticket als “P1-uplift (één medewerker)”, informeert regie direct en legt de motivatie vast in het ticket (komt terug in de SLR).

10.1.3 Landelijke onsite-SLA

Omdat Halt landelijk werkt, levert de MSP landelijke fysieke ondersteuning op alle werkplekken (Halt-locaties, gemeenten, scholen, wijklocaties, thuis/remote):

- P1: onsite ≤ 4 uur (landelijk)
- P2: onsite ≤ 8 uur (landelijk)
- P3/P4: onsite ≤ 2 werkdagen (landelijk)

MSP mag partners inzetten, maar Halt heeft altijd één aanspreekpunt (SPOC) en de MSP behoudt end-to-end eigenaarschap.

Normeringen (maandelijkse SLA-meting)
Minimaal het volgende percentage tickets wordt binnen norm afgehandeld (per prioriteit):
P1: ≥ 98%
P2: ≥ 95%
P3: ≥ 90%
P4: ≥ 90%

Afwijkingen worden in de maandelijkse SLR verklaard en voorzien van concrete verbeteracties met eigenaar en datum.

Beschikbaarheidseisen

- Microsoft 365/ werkplekdiensten/ netwerk: ≥ 99,8% per maand
- VPN/ telefonie/ connectiviteit: ≥ 99,7% per maand

Gepland onderhoud: buiten kantooruren, **≥48 uur** vooraf communiceren, niet tijdens piekperioden (zoals jaarlijkse instroompieken).

Communicatie en ticketafhandeling

- P1: updates elke 30 min · P2: elke 2 uur · P3: dagelijks · P4: op afgesproken datum
- Alle communicatie in het Nederlands.
- MSP blijft eindverantwoordelijk voor voortgang en oplossing, ook met derden.
- P1-uplift (één medewerker) volgt exact dezelfde communicatie- en escalatieregels als P1.

10.1.4 MTTR & MTTP (herstel en weer productief werken)

Naast klassieke oplostijden (MTTR) rapporteert de MSP verplicht MTTP (Mean Time to Productivity): de tijd totdat een medewerker weer daadwerkelijk kan werken. MTTP is voor Halt een kritische stuurwaarde en wordt gelijkwaardig aan MTTR beoordeeld.

10.1.5 Device-fallback: spoedvervanging & loaners (essentieel voor Halt)

Als een laptop/werkplek niet werkt, geldt dat medewerkers zo snel mogelijk weer moeten kunnen werken. Daarom zijn de volgende verplichtingen van kracht:
Voorraad direct inzetbare Windows-laptops (Intune/Autopilot-ready, BitLocker, basissoftware) bij MSP of landelijk partnerdepot.

P1 en P1-uplift:

1. Same-day swap (zelfde dag) via koerier of onsite-uitgifte; anders nood-werkplek binnen 4 uur (bijv. gestandaardiseerde loaner met tijdelijke profielen).
2. P2: volgende werkdag swap; P3/P4: ≤ 2 werkdagen.
3. **Logistiek & onboarding**
    - MSP regelt koerier/afspraak met medewerker en zorgt dat de loaner out-of-the-box werkt (Autopilot, MFA, basisapps).
    - Oude device: veilig ophalen, encryptie borgen, data-sanitization en retour naar depot of leasemaatschappij.
4. **Voorraad- en leveringsgaranties:**
    - MSP houdt aantoonbaar bufferstock aan (quantum en locaties beschreven in implementatieplan).
    - Bij structurele tekorten levert MSP een mitigatieplan (tijdelijke uitbreiding voorraad, extra depots, prioritering).

Doel: downtime minimaliseren en MTTP verlagen. Indien swap/loaner niet tijdig mogelijk is, moet de MSP alternatieve werkplekmogelijkheden bieden (bijv. VDI/virtuele werkplek of tijdelijke device-pool) zodat de medewerker door kan

10.2 Change Management

KPI Nr.	Type change	Servicelevel	Norm
5	Standaard-changes	≥95% van de standaard changes binnen planning geïmplementeerd	95% per maand
6	Minor changes	Eerste plandatum terugkoppeling binnen 5 werkdagen na aanmelding	95% per maand
–	Major changes	Planning en prijsmodel in overleg	n.v.t.
–	Spoedchanges	In overleg met Halt, met hoge prioriteit	n.v.t.
–	Projectchanges	Planning en uitvoering per project in overleg	n.v.t.

Halt.

10.3 Continuïteitsbeheer/ Backup & Recovery

Indicator	Servicelevel	Norm
Back-up & recovery	Dagelijkse controle + maandelijkse restore test	99%
RPO – restore	Maximaal dataverlies: 24 uur	99%
Uitwijkbeschikbaarheid	Cybercenter beschikbaar	100%
Uitwijkcentrum beschikbaarheid	Functioneel buiten onderhoud	99%
RTO uitwijk	Opstarttijd bij calamiteit	4 uur
RTO restore	Restoretijd bij herstel	24 uur
RPO uitwijk	Maximaal dataverlies bij calamiteit	8 uur
RPO restore	Maximaal dataverlies bij herstel	24 uur

10.4 Klanttevredenheid

Indicator	Definitie/ Meetmoment	Frequentie	Norm
Klanttevredenheid contact	Meting via enquête tijdens SLA-gesprekken	2 x per jaar	≥8
Klanttevredenheid eindgebruikers	Gebruiker vult enquête in bij afsluiting van een call	Doorlopend	≥8
Klanttevredenheid algemeen	Online vragenlijst met focus op: werkplek, betrouwbaarheid, kwaliteit en snelheid	2x per jaar	≥8

10.5 Experience Level Agreements (XLA's) – gebruikersbeleving

Naast de operationele SLA's hanteert Stichting Halt Experience Level Agreements (XLA's) om de gebruikersbeleving van de dienstverlening te borgen. Halt vindt de dagelijkse ervaring van haar medewerkers een essentieel onderdeel van de kwaliteit van de ICT-dienstverlening.
De leverancier wordt beoordeeld op onder meer:

A. Werkplekbeleving

- De ICT-werkplek moet medewerkers ondersteunen bij hun dagelijkse taken zonder merkbare frictie.
- Minimaal twee keer per jaar wordt een belevingsmeting uitgevoerd.
- Doelscore: gemiddeld ≥ 8.

B. Servicedesk-ervaring (menselijk aspect)

- Duidelijke, begrijpelijke en respectvolle communicatie.
- Medewerkers ervaren dat de Servicedesk meedenkt en eigenaarschap toont.
- Score ≥ 8 op Servicedesk-beleving.

C. Mean Time to Productivity (MTTP)

- De tijd tussen melding en "weer volledig kunnen werken".
- MTTP wordt gerapporteerd naast de technische oplostijd.
- Trend moet dalend blijven of stabiel onder afgesproken norm.

D. Proactiviteit en communicatie

- De MSP informeert medewerkers tijdig bij verstoringen, changes of onderhoud.
- Medewerkers ervaren voorspelbaarheid en duidelijkheid.

- Score ≥ 8 op “informatievoorziening”.

E. Aansluiting bij MTO
De leverancier levert input voor het jaarlijkse MTO en werkt verbetervoorstellen uit op basis van de MTO-resultaten die betrekking hebben op ICT-gebruikersbeleving.
De resultaten van de XLA’s worden opgenomen in de maandelijkse SLR en besproken in het kwartaaloverleg.

11. Ambities & wensen

- Leverancier toont initiatieven op gebied van duurzaamheid (bijv. CO2-neutraal datacenter)
- Oplossingen die schaalbaar en flexibel zijn bij groei of krimp
- Innovatie en meedenken in toekomstige digitaliseringsstappen
- Continue verbeterprocessen

12. Planning

- Publicatie aanbesteding: Q1 2026
- Gunning: Q3 2026
- Start dienstverlening: 1 januari 2027

13. Overige bepalingen

- Het contract heeft een looptijd van 4 jaar, met een optie tot 2 keer een verlenging van 2 jaar.
- Alle communicatie verloopt via TenderNed.
- Het PvE is onder voorbehoud van wijzigingen tot aan publicatie van de aanbesteding.
- Vragen over het PvE kunnen uitsluitend worden gesteld via een Nota van Inlichtingen (NVI) binnen TenderNed.