



**Programma van Eisen 2023: Applicatiebeheer en
Doorontwikkeling WerkBezoekApplicatie (WBA)**

Versie 1.0

Datum 20 maart 2024
Status Definitief



Colofon
Versie

1.0

Min IenW
FIB-UDAC
Directie Informatie en Exploitatie (IenE)
Postbus 20901
2500 EX Den Haag

Inhoud

Programma van Eisen 2023: Applicatiebeheer en Doorontwikkeling WerkBezoekApplicatie (WBA) 1

1	Begrippen-, synoniemen- en afkortingenlijst	4
2	Inleiding	6
2.1	Dit document.....	6
2.2	Opdrachtgeverschap.....	6
2.3	Ministerie van Infrastructuur en Waterstaat (Min IenW)	6
2.4	Directie Communicatie (DCO)	6
2.5	Directie Informatie en Exploitatie (IenE)	6
2.6	Werkbezoekapplicatie (WBA)	6
2.7	Hosting	6
2.8	Leeswijzer.....	6
3	Algemene eisen aan de Dienstverlening WBA	7
4	Opdracht en scope	10
4.1	Vaste Dienstverlening: Applicatiebeheer en onderhoud van WBA.....	10
4.2	Variabele Dienstverlening: Doorontwikkeling van WBA.....	10
4.3	Eenmalige dienstverlening.....	10
4.4	Samenwerking met Min IenW en Min BZK/Logius (Standaard Platform)	11
4.5	Freezeperiode.....	11
5	Informatiebeveiliging	12
5.1	Uitgangspunten	12
6	Applicatiebeheer en Doorontwikkeling	16
6.1	Inleiding	16
6.2	Applicatiebeheerprocessen	17
6.2.1	Incidentbeheer	17
6.2.2	Overige beheerprocessen	17
6.3	Doorontwikkeling	17
6.3.1	Wijzigingen	17
6.3.2	Impactanalyse	17
6.3.3	Ontwerp	17
6.3.4	Realisatie	18
6.3.5	Testen	18
6.3.6	Implementatie	18
6.3.7	Webcertificaatbeheer	19
7	Service Level Management: afspraken en rapportage	20
7.1	Service Level Management	20
7.2	Dienstverleningsvenster	20
7.3	Prioriteitsindeling Incidenten	20
7.4	Oplostijden Incidenten.....	21
7.5	Dienstverleningsvenster Informatiebeveiliging	22
7.6	Dienstverleningsrapportage	22
7.6.1	Frequentie	22
7.6.2	Sluitende onderbouwing.....	22
7.6.3	Inhoud rapportage	22
8	Hosting.....	23
8.1	Standaard Platform	23



1 **Begrippen-, synoniemen- en afkortingenlijst**

In dit document wordt gebruik gemaakt van de volgende begrippen, synoniemen en afkortingen. Gedefinieerde begrippen zijn in dit document herkenbaar aan hun beginhoofdletter.

Agile

Het voortbrengingsproces is een effectieve en flexibele manier van werken die het mogelijk maakt om complexe projecten ook zonder detailplanning op een productieve wijze op te leveren en eventuele problemen snel te tackelen.

Applicatiebeheer (Vaste Dienstverlening)

Het uitvoeren van beheer, onderhoud en aanpassingen van/aan WBA. Tevens wordt hieronder applicatief beheer van alle aanwezige datakoppelingen verstaan.

Application Programming Interface (API)

Een verzameling definities op basis waarvan systemen onderling kunnen communiceren.

Business Information Services Library (BiSL)

BiSL is een framework dat een beschrijving geeft van de werkzaamheden die een gebruikersorganisatie moet uitvoeren om de informatievoorziening te krijgen die zij nodig heeft.

Baseline Informatiebeveiliging Overheid (BIO)

De Baseline Informatiebeveiliging Overheid (BIO) beschrijft het basisniveau voor informatiebeveiliging. De BIO wordt gehanteerd binnen de Nederlandse overheid, door het Rijk, Gemeenten, Waterschappen en Provincies. Dit is één basisniveau voor informatiebeveiliging en één gezamenlijke taal voor alle overheidsorganisaties.

Call

Melding van een Incident of Service Request (SR) door IenW (zijnde niet eindgebruiker) bij Opdrachtnemer middels het Callregistratiesysteem.

Callregistratiesysteem

Online registratiesysteem die Opdrachtnemer hanteert voor het registreren, prioriteren, routeren en oplossen/beantwoorden van bevindingen, Incidenten en Wijzigingsverzoeken over WBA.

Configuratie Item (CI)

Elk component dat onderdeel uitmaakt van WBA. CI's omvatten onder andere hardware, software en formele documentatie zoals procesdocumentatie en SLA's.

Dienstverlening

De levering van Diensten (in dit geval: Applicatiebeheer en Doorontwikkeling van WBA).

Doorontwikkeling (Variabele Dienstverlening)

Het (projectmatig) aanpassen van WBA naar aanleiding van veranderende technische of functionele eisen.

Dossier Afspraken en Procedures (DAP)

Dit is een schriftelijke vastlegging van de manier van samenwerking tussen partijen die met het (Applicatie)beheer en Doorontwikkeling van WBA te maken hebben.

Functionele AcceptatieTest (FAT)

Een test uitgevoerd door Opdrachtgever en ook door Opdrachtnemer om te bepalen of het doorontwikkelde WBA aan de functionele eisen voldoet.

GebruikersAcceptatieTest (GAT)

Een test, door de toekomstige gebruiker(s) uitgevoerd, om te bepalen of het doorontwikkelde WBA aan de wensen/eisen van de gebruiker voldoet.

Incident

Een incident is een ongeplande onderbreking in een IT-service of vermindering in de kwaliteit van een IT-service. Het falen van een CI (configuratie item) dat nog niet een service heeft beïnvloed, is ook een incident.

Informatiebeveiligingsincident

Een informatiebeveiligingsincident is een gebeurtenis waarbij de mogelijkheid bestaat dat de vertrouwelijkheid, integriteit of beschikbaarheid van informatie en/of informatie verwerkende systemen in gevaar is of kan komen.

Information Security Management System (ISMS)

Een Information Security Management System (ISMS) is een procesgerichte benadering voor informatiebeveiliging. Het is een managementsysteem waarin het risicobeheerproces centraal staat, zodat risico's adequaat worden beheerd. Het doel van het ISMS is het continu beoordelen of beveiligingsmaatregelen passend en effectief zijn, en of deze bijgesteld moeten worden.

Information Technology Infrastructure Library (ITIL v4)

ITIL is een framework bestaande uit een reeks best practices voor het leveren van efficiënte IT-ondersteuningsdiensten aan klanten en gericht op de verbetering van de klanttevredenheid en productiviteit.

Mobile Device Management (MDM)

Mobile Device Management is alle software waarmee IT het beheerbeleid op laptops, smartphones, tablets of elk ander apparaat dat is verbonden met het netwerk van een organisatie kan automatiseren, beheren en beveiligen.

Mobile Application Management (MAM)

MAM beheert apps met specifieke functies, zoals een door de leverancier geleverde app-catalogus, die klanten doorgaans kunnen wijzigen.

Opdrachtgever

De Staat der Nederlanden, vertegenwoordigd door de Minister van Infrastructuur en Waterstaat die met Opdrachtnemer een Overeenkomst in het kader van de aanbesteding sluit.
Synoniemen van Opdrachtgever in dit document zijn: Min IenW of een dienstonderdeel daarvan, zoals IenE en DCO. Synoniemen: klant, afnemer.

Opdrachtnemer

De winnende Inschrijver met wie Opdrachtgever in het kader van deze aanbesteding een Overeenkomst afsluit.
Synoniemen van Opdrachtnemer in dit document zijn: Applicatiebeheerpartij, applicatieleverancier/-beheerder, dienstverlener, aanbieder.

Oplostijd

Tijd, gemeten in werkuren, tussen het tijdstip van aanmelden van een Service Request/Incident en het tijdstip dat een Service Request/Incident bij de indiener afgemeld is, als zijnde gereed c.q. verholpen.

Overeenkomst

Schriftelijke overeenkomst die met de winnende Inschrijver van deze aanbesteding wordt gesloten met betrekking tot de levering van de door de Aanbestedende dienst gevraagde leveringen en/of diensten.

Productie Acceptatie Test (PAT)

Een test om te bepalen of het doorontwikkelde WBA aan de vanuit beheer gestelde eisen voldoet. Een PAT dient bij elke Wijziging/release uitgevoerd te worden.

Programma van Eisen (PvE)

In het Programma van Eisen staat waar u allemaal aan moet voldoen om in aanmerking te komen voor de opdracht. Alle technische en functionele specificaties worden opgenomen in het Programma van Eisen. Een goed programma van eisen geeft gegadigden een goed beeld van de eisen die de opdrachtgever aan de leverancier en de te leveren prestaties stelt.

**Reactietijd**

De tijdspanne vanaf het moment dat Opdrachtgever een Service Request/Incident heeft doorgegeven aan opdrachtnemer c.q. geregistreerd tot het moment dat opdrachtnemer aanvangt met de werkzaamheden betreffende het Service Request/Incident.

Regievoerder

De Regievoerder draagt zorg voor de optimale afstemming tussen de vraag van de organisatie naar ICT-diensten en het aanbod van ICT-diensten. Dit met als doel om de organisatie optimaal te ondersteunen bij het behalen van hun doelen en het verkrijgen van een optimale Dienstverlening. De rol van Regievoerder is belegd bij de Directie Informatie en Exploitatie (IenE).

Request For Change (RFC)

Zie: Wijzigingsverzoek.

Retransitieplan

Een plan van aanpak waarin de leverancier omschrijft op welke wijze het (applicatie)beheer van de applicatie wordt overgedragen aan een nieuwe leverancier na einde contractperiode.

Securitybevinding

Een securitybevinding is een tekortkoming die kan leiden tot een informatiebeveiligingsincident.

Service Request

Verzoeken tot ondersteuning die niet direct te relateren zijn aan het zorg dragen voor de juiste werking van WBA, zoals het uitvoeren van een query en het opleveren van eenmalige rapportages.

Service Level Agreement (SLA)

Nederlands: Diensten Niveau Overeenkomst (DNO). Dit is een schriftelijke overeenkomst, tussen Opdrachtnemer en Opdrachtgever van (een) dienst(en), waarin afspraken zijn opgenomen over het kwaliteitsniveau van de te leveren dienst(en) (oftewel het servicelevel).

Transitieplan

Een plan van aanpak waarin een nieuwe leverancier omschrijft op welke wijze het (applicatie)beheer van de applicatie zal overnemen en hoe dit plan aansluit op het re-transitieplan (overdrachtsplan) van de huidige leverancier.

Variabele Dienstverlening

Zie: Doorontwikkeling (Variabele Dienstverlening).

Vaste Dienstverlening

Zie: Applicatiebeheer (Vaste Dienstverlening).

Verklaring Omtrent het Gedrag (VOG)

Een VOG is een verklaring waaruit blijkt dat uw (justitiële) verleden geen bezwaar vormt voor het vervullen van een specifieke taak of functie in de samenleving.

Wijziging

Een Wijziging is de toevoeging, verandering of verwijdering van alles dat een effect kan hebben op het geleverde informatiesysteem.

Wijzigingsverzoek

Ook wel Request For Change (RFC) genoemd. Een formeel voorstel voor een Wijziging aan/van één of meer Configuratie Item(s) die onderdeel uitmaken van de dienst. Een Wijzigingsverzoek bevat de details van de voorgestelde Wijziging en kan zijn vastgelegd op papier of elektronisch.

2 Inleiding

2.1 Dit document

Dit Programma van Eisen maakt onderdeel uit van een Europese aanbesteding. De eisen genoemd in dit document zijn bepalend voor de invulling van de opdracht: het Applicatiebeheer en de Doorontwikkeling van de WerkBezoekApplicatie (WBA).

2.2 Opdrachtgeverschap

Het opdrachtgeverschap valt onder de Directie Communicatie (DCO) van Ministerie van Infrastructuur en Waterstaat (Min IenW). De Directie Informatie en Exploitatie (IenE) van Min IenW treedt op als Regievoerder naar Opdrachtnemer. Zie ook Hoofdstuk 2 van het Beschrijvend document.

2.3 Ministerie van Infrastructuur en Waterstaat (Min IenW)

IenW zet in op leefbaarheid en bereikbaarheid, met een goede doorstroming in een schone en veilige omgeving. IenW werkt aan krachtige verbindingen over de weg, het spoor, het water en door de lucht, beschermt tegen wateroverlast en bevordert de kwaliteit van lucht en water. Het departement maakt daarvoor vernieuwend beleid en zorgt voor de uitvoering en handhaving. Vlot, veilig en leefbaar: dat is IenW.

Voor nadere informatie over IenW verwijzen wij u naar de website via de link:
[Ministerie van Infrastructuur en Waterstaat | Rijksoverheid.nl](#)

2.4 Directie Communicatie (DCO)

DCO helpt de beleidskern de samenleving 'naar binnen te brengen'. We willen de maatschappij actiever betrekken bij beleidsontwikkeling en de realisatie van dit beleid. Daarom zoeken we niet naar een zendende, maar juist naar een verbindende rol. Samenwerking en interactie met de beleidsdirecties staan daarbij voorop.

De Directie Communicatie (DCO) is binnen Min IenW het organisatieonderdeel dat zich richt op het ontwikkelen van, adviseren over en toezien op (corporate) communicatie en interne en externe communicatie op het gebied van de beleids- en communicatieprioriteiten van het ministerie en de bewindspersonen van Min IenW.

DCO/externe optredens en Protocol is verantwoordelijk voor het (strategisch) adviseren op en organiseren/registreren van alle externe optredens en werkbezoeken van de bewindspersonen van IenW.

2.5 Directie Informatie en Exploitatie (IenE)

De Directie Informatie en Exploitatie (IenE) is binnen het ministerie van IenW het organisatieonderdeel dat zich voor de onderdelen van het IenW departement richt op het informatiemanagement, de architectuur, de ICT-regievoering, de projectmatige systeemontwikkeling en - implementatie alsmede het (functioneel) beheren van de bij IenE in beheer zijnde systemen en infrastructuren.

2.6 Werkbezoekapplicatie (WBA)

Werkbezoekapplicatie (WBA) is een applicatie voor de Directies Communicatie van het ministerie van Infrastructuur en Waterstaat (IenW), het ministerie van Volksgezondheid, Welzijn en Sport (VWS) en, op termijn, het ministerie van Sociale Zaken en Werkgelegenheid (SZW), voor het ontvangen, verwerken en weergeven van uitnodigingen voor werkbezoeken van de ministers en staatssecretarissen.

SZW maakt op dit moment nog gebruik van WBA in een testomgeving. Na de gunning van de opdracht dient de Opdrachtnemer de WBA SZW omgeving over te zetten naar Standaard Platform (SP).

Team Externe Optredens en Protocol van de Directie Communicatie (DCO) van het Ministerie van Infrastructuur en Waterstaat (Min IenW) gebruikt WBA als registratiesysteem voor alle uitnodigingen die de bewindspersonen van IenW ontvangen voor werkbezoeken evenementen (publieke optredens). Externe partijen sturen via een formulier (dat gekoppeld is aan WBA) op Rijksoverheid.nl een uitnodiging. Medewerkers van IenW doen dat via een formulier op Rijksportaal. Via WBA doorloopt een uitnodiging een workflow (adviseren, voorleggen aan bewindspersonen, afwijzen/bevestigen en voorbereiden). Communicatie intern/extern verloopt grotendeels via WBA.

Ook andere teams binnen DCO gebruiken WBA om inzicht te krijgen in lopende activiteiten van de bewindspersonen en de communicatie daar omheen. Zie ook 1.1 van het Beschrijvend Document.

2.7 Hosting

Hosting (voor WBA wordt uitgevoerd door Min BZK/Logius (Standaard Platform). Hosting staat beschreven in Hoofdstuk 8.

2.8 Leeswijzer

Hoofdstukken

- De in dit Programma van Eisen gehanteerde begrippen, synoniemen en afkortingen treft u aan in Hoofdstuk 1.
- In Hoofdstuk 3 staan de algemene eisen beschreven die worden gesteld aan de Dienstverlening WBA.
- In Hoofdstuk 4 wordt de opdracht en scope uiteengezet.
- Informatiebeveiliging komt aan de orde in Hoofdstuk 5.
- De processen voor Applicatiebeheer en Doorontwikkeling treft u aan in Hoofdstuk 6.
- De serviceniveaufactspraken en de dienstverleningsrapportage staan in Hoofdstuk 7.
- Informatie over hosting vindt u in Hoofdstuk 8.

Bijlagen

Het Programma van Eisen kent verschillende bijlagen. Vanuit diverse Hoofdstukken/Paragrafen in dit document wordt naar een specifieke bijlage verwezen. Er zijn ook bijlagen waarnaar niet specifiek verwezen wordt, omdat deze als nadere/achtergrond informatie dienen.

Voor het leesgemak volgt hieronder een overzicht van de bijlagen met – indien van toepassing – de duiding naar het Hoofdstuk/Paragraaf waarin de desbetreffende bijlage ter sprake komt:

- | | | |
|--------------|---|-----------|
| • Bijlage 3 | Functioneel Ontwerp WBA | Par. 4.1 |
| • Bijlage 4 | Technisch Ontwerp WBA | Par. 4.1 |
| • Bijlage 15 | IWEA - IenW Enterprise Architectuur | |
| • Bijlage 8 | GAS WBA | |
| • Bijlage 2 | Checklist in beheername WBA | Par. 6.1 |
| • Bijlage 5 | Beheerhandleiding WBA | |
| • Bijlage 6 | Gebruikershandleiding WBA | |
| • Bijlage 7 | Backlog WBA | Hfdstk. 3 |
| • Bijlage 9 | Overzicht bevindingen en incidenten 2020-2023 (aantallen) WBA | Par. 7.4 |
| • Bijlage 11 | Concept Verwerkersovereenkomst - WBA | Hfdstk. 3 |
| • Bijlage 12 | DAP Standaard Platform (SP) | Par. 8.1 |

Overige bijlagen die niet in deze opsomming vermeld staan, komen aan de orde in het Beschrijvend Document.

Eisen

Eisen waaraan Opdrachtnemer dient te voldoen, zijn herkenbaar aan: **E.<volgnummer>:**

N.B. Indien een Inschrijver niet aan een gestelde eis (knock out (KO)) kan voldoen, dan wordt de Inschrijving terzijde gelegd.

3

Algemene eisen aan de Dienstverlening WBA

E.01: Aansluitvoorwaarden Standaard Platform (SP)
Van Opdrachtnemer wordt geëist dat de applicatie blijft voldoen aan de aansluitvoorwaarden van de hostingpartij Min BZK/Logius van het Standaard Platform. Zie Hoofdstuk 8.

E.02: Algemene Verordening Gegevensbescherming (AVG)
Inschrijver dient te voldoen aan de eisen van de Algemene Verordening Gegevensbescherming (AVG/GDPR) van de Europese Unie.

Toelichting
Dit houdt in dat Inschrijver dient te kunnen aantonen dat zij de persoonsgegevens van betrokkenen op een rechtmatige, behoorlijke en transparante wijze verwerken, conform de principes van de AVG/GDPR. Inschrijver dient tevens te kunnen aantonen dat zij passende technische en organisatorische maatregelen heeft getroffen om de persoonsgegevens te beveiligen en te beschermen tegen ongeoorloofde of onrechtmatige verwerking, onopzettelijk verlies of vernietiging, of schade aan de persoonsgegevens. Inschrijver dient bereid te zijn om deze gegevens te verstrekken aan de aanbestedende dienst en zich te houden aan eventuele aanvullende eisen met betrekking tot gegevensbescherming die in het kader van de opdracht gesteld worden. Door het indienen van een Inschrijving geeft Inschrijver aan te kunnen voldoen aan deze Eis. De winnende Inschrijver dient de Concept Verwerkersovereenkomst - WBA (Bijlage 11) te ondertekenen.

E.03: Digitoegankelijkheid
Opdrachtnemer dient bij ontwikkeling van bestaande en nieuwe websites, bestaande en nieuwe intranetten/extranetten en (mobiele) apps van de (semi-) overheid te voldoen aan de richtlijnen voor digitoegankelijkheid.

Toelichting:
Via de volgende links zijn de richtlijnen beschikbaar: <https://www.w3.org/TR/WCAG21/> en <https://www.forumstandaardisatie.nl/standaard/digitoegankelijk-en-301-549-met-wcag-21>. Meer achtergrondinformatie is te vinden op www.digitoegankelijk.nl.

N.B. De 2 URL's van WBA zijn digitoegankelijk: werkbezoek.minienw.nl en werkbezoek.minvws.nl.

E.04: Digitoegankelijkheid - WCAG en WDO
Opdrachtnemer zorgt vanaf de start van de opdracht en tijdens de doorontwikkeling van de applicatie dat deze voldoet aan de toegankelijkheidseisen van de norm WCAG 2.1 level A + AA (of opvolgende versies zodra deze verplicht is voor overheden).

Toelichting:
Digitale toegankelijkheidseisen komen voort uit de 'Wet digitale overheid'. Hiermee implementeert Nederland de Europese richtlijn over toegankelijkheid van overheidswebsites en apps. De Web Content Accessibility Guidelines (WCAG) zijn sinds 1999 de internationale standaard voor digitale toegankelijkheid. De organisatie World Wide Web Consortium (W3C) beheert de standaard.

E.05: Digitoegankelijkheid - Toetsing en afwijkingen oplossen
De digitale toegankelijkheid van de oplossing wordt door opdrachtgever minimaal iedere 36 maanden (en tussentijds bij grote wijzigingen) getoetst door een gecertificeerde onafhankelijke externe partij. Deze toetsing bestaat uit een aantal activiteiten:
-De score blijkt uit een op te leveren onderzoeksrapport door een gecertificeerde onafhankelijke externe partij;
-Eventuele bevindingen (afwijking van de op dat moment geldende (voor overheden verplichte) versie van de WCAG) worden door opdrachtnemer opgelost;
-Kosten van aanpassingen om te blijven voldoen aan de huidige norm liggen bij opdrachtnemer;
-Opdrachtnemer zorgt intern voor het juiste niveau van kennis en expertise op gebied van digitale toegankelijkheid.

E.06: Voldoen aan Webrichtlijnen
Opdrachtnemer dient bij ontwikkeling van bestaande en nieuwe websites, bestaande en nieuwe intranetten/extranetten en (mobiele) apps van de (semi-) overheid te voldoen aan de onderstaande webrichtlijnen.

Toelichting:
De Rijksoverheid hanteert verplicht toe te passen richtlijnen. Deze zijn vooral gericht op veiligheid, bescherming persoonsgegevens, toegankelijkheid en transparantie. Zie ook: <https://www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen>.

Webrichtlijnen			
Nr.	Omschrijving eis	Opmerkingen	Meer informatie
NF01	DNSSEC moet worden toegepast op alle overheidsdomeinnamen én op DNS-resolvers die clients van overheidsorganisaties direct of indirect van DNS-antwoorden voorzien.	DNSSEC zorgt voor de beveiliging van DNS door aan het DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren.	https://www.forumstandaardisatie.nl/open-standaarden/dnssec
NF02	HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices.	HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser). Dit maakt het voor cybercriminelen moeilijker om verkeer om te leiden naar valse websites en om de inhoud van webverkeer te onderscheppen.	https://www.forumstandaardisatie.nl/open-standaarden/https-en-hsts
NF03	IPv6 en IPv4 moeten in combinatie ('dual stack') worden toegepast op communicatie tussen toepassingen in (een) netwerk(en).	Internet Protocol (IP) maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals internet, mogelijk. IPv6 heeft een veel grotere hoeveelheid beschikbare IP-adressen ten opzichte van de voorganger IPv4. Dit maakt verdere groei en innovatie van het internet mogelijk.	https://www.forumstandaardisatie.nl/open-standaarden/ipv6-en-ipv4
NF04	security.txt moet worden toegepast op alle systemen die via HTTPS publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.	Met een security.txt-bestand kan een organisatie security-contactinformatie op haar webserver publiceren. Beveiligingsonderzoekers kunnen deze informatie gebruiken om direct contact met de juiste afdeling of persoon binnen de organisatie op te nemen over kwetsbaarheden die zij in de website of IT-systemen van de organisatie hebben gevonden.	https://www.forumstandaardisatie.nl/open-standaarden/securitytxt
NF07	TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie. Er wordt gewerkt met TLS 1.2 of hoger	TLS zorgt voor beveiligde internetverbindingen, met als doel de veilige uitwisseling van gegevens tussen een internetsystemen (zoals websites of mailservers). Dit maakt het voor cybercriminelen moeilijker om internetverkeer te onderscheppen of te manipuleren.	https://www.forumstandaardisatie.nl/open-standaarden/tls

NF08	De tool voldoet aan de Europese standaard voor digitale toegankelijkheid: EN 301 549.	Overheidsorganisaties moeten hun websites en apps toegankelijk maken en houden. En ze moeten voor al die websites en apps verklaringen publiceren. Dat staat in de wet voor digitale toegankelijkheid: het Besluit digitale toegankelijkheid overheid. Standaard EN 301 549 bestaat uit een verzameling van technische eisen, waaronder de WCAG. WCAG staat voor Web Content Accessibility Guidelines en is een internationale standaard.	https://www.forumstandaardisatie.nl/open-standaarden/digitoegankelijk-en-301-549-met-wcag-21
NF08.1	De website en app moeten voldoen aan de toegankelijkheidseisen in de WCAG 2.1 level A + AA en volgende versies zoals WCAG 2.2 A + AA zodra deze in werking treedt en verplicht is voor overheden.	Overheden moeten minimaal voldoen aan de niveaus A en AA. Meer specifieke informatie over de toegankelijkheid van apps is te vinden op https://appt.nl/	https://www.forumstandaardisatie.nl/open-standaarden/digitoegankelijk-en-301-549-met-wcag-21
NF08.2	De website en app voldoet bij configuratie en inrichting aan de digitale toegankelijkheidseisen op basis van de Wet Digitale Overheid, besluit digitale toegankelijkheid overheid'[1] (Te onderbouwen met een onderzoek voor de website volgens WCAG-EM en voor de app volgens WACG-EM of Appt-EM).	Opdrachtnemer committeert zich aan het oplossen van de bevindingen (afwijking van de op dit moment geldende (voor overheden verplichte) versie van de WCAG) die door het ministerie met een onderzoek in kaart zijn gebracht. Deze afwijkingen worden door Inschrijver op eigen kosten weggewerkt. Inrichting van de website en app gebeurt in overleg met de Aanbestedende dienst. De opdrachtgever kan waar nodig bij specifieke vragen faciliteren in het leveren van expertise.	
NF08.3	De digitale toegankelijkheid van de website en app wordt door opdrachtnemer jaarlijks (en tussentijds bij grote wijzigingen) getoetst door een gecertificeerde externe partij.	Eventuele bevindingen (afwijking van de op dat moment geldende (voor overheden verplichte) versie van de WCAG) die niet vooraf zijn afgestemd, worden door opdrachtnemer op eigen kosten weggewerkt. Opdrachtgever laat de digitale toegankelijkheid van de website en app zelf ook toetsen. Ook hiervoor geldt dat eventuele bevindingen (afwijking van de op dat moment geldende (voor overheden verplichte) versie van de WCAG) die niet vooraf zijn afgestemd door opdrachtnemer op eigen kosten worden weggewerkt.	
NF09	Webapplicatie voldoet aan de cookiewetgeving	Artikel 11.7a van de Telecommunicatiewet schrijft voor dat een ieder die via een elektronisch communicatienetwerk gegevens wenst op te slaan in de randapparatuur van een gebruiker daarvoor vooraf toestemming van de gebruiker moet hebben verkregen. Uitzondering: Voor functionele en bepaalde analytische cookies is geen toestemming vereist.	https://www.rijksoverheid.nl/onderwerpen/telecommunicatie/vraag-en-antwoord/mag-een-website-ongevraagd-cookies-plaatsen

E.07: Voldoen aan Mailrichtlijnen

Opdrachtnemer dient bij ontwikkeling van bestaande en nieuwe websites, bestaande en nieuwe intranetten/extranetten en (mobiele) apps van de (semi-) overheid te voldoen aan onderstaande mailrichtlijnen.bijhouden software

Toelichting:

De Rijksoverheid hanteert verplicht toe te passen richtlijnen. Deze zijn vooral gericht op veiligheid, bescherming persoonsgegevens, toegankelijkheid en transparantie. Zie ook: <https://www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen>.

Mailrichtlijnen			
Nr.	Omschrijving eis	Opmerkingen	Meer informatie
NF10	Systeem voldoet aan de mailrichtlijnen van Rijksoverheid		https://www.communicatierijk.nl/vakkennis/rijkswebsites/verplichte-richtlijnen
NF10.1	DKIM moet worden toegepast op alle overheidsdomeinnamen waarvandaan wordt gemaïld én op alle mailservers waarmee de overheid e-mail verstuurt en ontvangt.	Het gebruik van DKIM verkleint de kans op misbruik van e-mailadressen doordat ontvangers betrouwbaar echte e-mails van phishingmails of spam kunnen onderscheiden. Ook kunnen ontvangers controleren of de inhoud van de e-mail door derden is gemanipuleerd.	https://www.forumstandaardisatie.nl/open-standaarden/dkim
NF10.2	DMARC moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaïld, én op alle mailservers waarmee de overheid e-mail ontvangt.	DMARC geeft de verzendende partij de mogelijkheid om beleid te formuleren wat er met e-mails moet gebeuren wanneer de echtheidswaarmerken niet kloppen. Het geeft ook rapportagemogelijkheden voor legitieme en niet-legitieme uitgaande e-mailstromen.	https://www.forumstandaardisatie.nl/open-standaarden/dmarc
NF10.3	SPF moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaïld, én op alle mailservers waarmee de overheid e-mail ontvangt.	Het gebruik van SPF verkleint de kans op misbruik van e-mailadressen doordat ontvangers betrouwbaar echte e-mails van phishing mails of spam kunnen onderscheiden.	https://www.forumstandaardisatie.nl/open-standaarden/spf
NF10.4	STARTTLS en DANE moeten in combinatie worden toegepast op ontvangende en verzendende e-mailservers.	Mailverkeer tussen mailservers verloopt via SMTP. STARTTLS in combinatie met DANE gaan, in aanvulling op SMTP, afluisteren of manipuleren van dit mailverkeer door internetcriminelen tegen.	https://forumstandaardisatie.nl/open-standaarden/starttls-en-dane

E.08: Communicatie in het Nederlands door personeel

Alle door Opdrachtnemer bij de Aanbestedende dienst ingezet personeel dient over sterke communicatieve vaardigheden te beschikken en de Nederlandse taal machtig te zijn in zowel schrift als spraak.

E.09: Communicatie en documentatie in het Nederlands

Communicatie en documentatie m.b.t. de uitvoering van de opdracht geschieden in het Nederlands.

E.10: Social Return

Opdrachtnemer dient jaarlijks ten minste 2,5% van de door hem gefactureerde en door IenW betaalde omzet aanwenden om daarmee bij te dragen aan Social Return. Dit percentage (zoals reeds verdisconteerd in de toegezonden facturen) dient in relatie te staan tot de uit te voeren opdracht en dient te worden aangewend voor één of meer van de volgende activiteiten;



- Werkplekken aanbieden voor mensen met een arbeidshandicap of psychosociale problematiek;
- Stageplekken aanbieden;
- Lezingen/ workshops of colleges geven om zo bij te dragen aan kennisvergroting van een doelgroep die zonder de benoemde bijdrage van de Opdrachtnemer deze kennis niet zou ontvangen, maar deze kan gebruiken voor ontwikkeling op de arbeidsmarkt;
- Bijdrage Social Return reservering om daarmee op een later moment, uiterlijk 1 jaar na het aflopen van de Overeenkomst, een initiatief te ontplooiën;
- Bijdrage aan een derde partij die zich specialiseert in het verwezenlijken van Social Return.

(zie Beschrijvend document, Hoofdstuk 3 Omschrijving van de opdracht)

E.11: Conceptovereenkomst en ARBIT-2022

Inschrijver dient akkoord te gaan met de Conceptovereenkomst ARBIT – WBA (bijlage 10) en de ARBIT-2022, zoals opgenomen in Bijlage 16. De Conceptovereenkomst is gebaseerd op de modelovereenkomst voor de ARBIT-2022 (zie Beschrijvend document, Hoofdstuk 6 Gunningscriteria).

E.12: Voldoen aan totstandkoming totaalscore

Om in aanmerking te komen voor het ontvangen van het voornemen tot gunning dient de inschrijver te voldoen aan de volgende 3 punten:

- alle Eisen (zie dit PvE);
- ten minste een gemiddelde van 60% op de op de kwalitatieve Gunningscriteria (plan van aanpak in beheer name, applicatiebeheer en doorontwikkeling), hierbij mag er maximaal één 40% score bij zitten (b.v. score van 40%-80%-60%) en
- de hoogste totaalscore inclusief het Gunningscriterium Prijs hebben behaald.

(zie Beschrijvend document, Hoofdstuk 7 Beoordelingsprocedure).



4 **Opdracht en scope**

4.1 **Vaste Dienstverlening: Applicatiebeheer en onderhoud van WBA**

De diensten die Opdrachtnemer dient te leveren voor Applicatiebeheer worden Vaste Dienstverlening genoemd.

Opdrachtnemer en IenE leggen in een Dossier Afspraken en Procedures (DAP) met elkaar de wijze vast waarop zij invulling geven aan de overeenkomst. De DAP maakt onderdeel uit van de Overeenkomst. In de DAP wordt onder andere geregeld:

- Wie namens Opdrachtgever bevoegd is dienstverleningsverzoeken in te dienen;
- Hoe dienstverleningsverzoeken aan Opdrachtnemer kenbaar gemaakt moeten worden;
- Welke informatie een dienstverleningsverzoek minimaal moet bevatten;
- Een model voor de dienstverleningsrapportage;
- Escalatieschema.

E.13: Dagelijks Applicatiebeheer (instandhouding)

Opdrachtnemer dient zorg te dragen voor het dagelijks Applicatiebeheer (instandhouding), dat bestaat uit de volgende onderdelen:

- Correctief onderhoud; registreren van gemelde defecten;
- Onderzoeken van gewenste/noodzakelijke aanpassingen, maken en uitwerken van oplossingen, testen van aanpassingen, assisteren bij herstelwerkzaamheden, onderhouden van de documentatie (incident-, probleem-, en wijzigingsbeheer);
- Instandhoudingbeheer; configuratiebeheer, programmatuurbeheer en documentbeheer (FO en TO);
 - FO WBA: zie bijlage 3.
 - TO WBA: zie bijlage 4.
- Beschikbaar stellen van een representatieve ontwikkel- en test omgeving;
 - Acceptatie- en Productie omgeving worden door de hostingpartij (Min BZK/Logius (Standaard Platform)) geleverd. Zie Hoofdstuk 8.
- Informatieverstrekking; verstrekken van instructies, systeemkennis overdraagbaar maken en beschikbaar stellen.

E 14: Actueel houden van het retransitieplan

Opdrachtnemer houdt het retransitieplan gedurende de looptijd van het contract actueel.

De kosten van het up-to-date houden van het retransitieplan dient u te verdisconteren in de maandelijkse beheerkosten.

E.15: Support

Opdrachtnemer dient het volgende te leveren:

- Ondersteuning bij aanmelden/registeren van meldingen door geautoriseerde gebruikers (niet zijnde eindgebruikers) in het Callregistratiesysteem van Opdrachtnemer;
- Vastleggen meldingen (zoals Incidenten, informatieve vragen, Service Requests en Wijzigingsverzoeken) in een online Callregistratiesysteem, geprioriteerd, bewaakt en opgelost; (Voor oplostijden: zie H7: 7.2, 7.3 en 7.4.)

In de DAP dienen hierover nadere afspraken gemaakt te worden.

E.16: Preventief onderhoud

De Opdrachtnemer dient zorg te dragen voor een optimaal functioneren van de applicatie, met een minimum aan middelen en verstoringen in de operatie, d.w.z.:

- Opdrachtnemer treft maatregelen ter voorkoming van Storingen en andere daarmee verband houdende vormen van Dienstverlening;
- Inclusief het (proactief) aanbrengen van verbeteringen op de bestaande Programmatuur waarmee beoogd wordt te voorkomen dat een systeem gaat afwijken van de overeengekomen eisen, dan wel ter voorkoming van defecten;
- "life cycle management ter voorkoming van technische schuld".

E.17: Dienstverleningsrapportage

Opdrachtnemer dient uiterlijk binnen tien (10) werkdagen na afloop van ieder kwartaal de dienstverleningsrapportage te leveren, en voldoet hierbij geheel aan de eisen als omschreven in Par. 7.6.

E.18: Deelname maandelijks operationeel overleg

Opdrachtnemer dient deel te nemen aan het maandelijks operationeel overleg op locatie van IenW of online. In de DAP worden hierover nadere afspraken gemaakt.

E.19: Deelname aan dienstverleningsoverleg

Opdrachtnemer dient eenmaal per kwartaal deel te nemen aan het Dienstverleningsoverleg (tactisch overleg) op een locatie van IenW of online. In de DAP worden hierover nadere afspraken gemaakt.

E.20: Informatiebeveiliging

De opdrachtnemer dient volledig te voldoen aan de eisen m.b.t. Informatiebeveiliging als vermeld in Hoofdstuk 5 van dit document.

4.2 **Variabele Dienstverlening: Doorontwikkeling van WBA**

De diensten die Opdrachtnemer dient te leveren voor Doorontwikkeling worden Variabele Dienstverlening genoemd. Ook het implementeren van additionele omgevingen is onderdeel van deze variabele dienstverlening.

Variabele Dienstverlening wordt geleverd op verzoek van Opdrachtgever.

De Variabele Dienstverlening **fluctueert** gedurende de looptijd van het contract. Bezien over de maximale looptijd van tien (10) jaar zal de Variabele Dienstverlening naar schatting liggen tussen de 2000 en 4000 uur aan Variabele Dienstverlening. Verwacht wordt dat de verhouding tussen Doorontwikkeling en onverwachte aspecten/calamiteiten ongeveer 50-50 zal zijn.

Zie ook Beschrijvend Document par 3.3.

N.B.: Aan deze indicatie kan de opdrachtnemer geen rechten ontleen. De omvang van de Variabele Dienstverlening hangt af van de werkelijke behoefte, beschikbare capaciteit bij DCO en de werkelijke looptijd van de overeenkomst.

E.21: Standaard Platform

De opdrachtnemer dient zorg te dragen, t.b.v. de Doorontwikkeling van WBA, voor:

- a) Het aansluiten op CI/CD & container registry op Standaard Platform (zie TO (bijlage 4), DAP Standaard Platform (bijlage 12) en [Logius | Aansluitvoorwaarden Standaard Platform](#))
- b) Het inrichten van een eigen ontwikkel- en testomgeving.

E.22: Doorontwikkeling

De opdrachtnemer dient bij de voorbereiding en realisatie van Doorontwikkeling de volgende taken uit te voeren conform beschrijving in paragraaf 6.3:

- Impactanalyse (incl. specificeren en inschatten van realisatiekosten)
- Ontwerp
- Realisatie
- Testen
- Implementatie

4.3 **Eenmalige dienstverlening**

E.23: Opstellen transitieplan

Opdrachtnemer dient het Applicatiebeheer van WBA over te nemen van de huidige dienstverlener binnen de gestelde termijnen (dus binnen 3 maanden) en conform beschrijving van het door opdrachtnemer in de aanbesteding aangeleverde plan van aanpak (zie Beschrijvend document, Hoofdstuk 6 Gunningscriteria).

De transitie wordt afgesloten met décharge, verleend door Opdrachtgever. Decharge is op basis van de Checklist in beheer name WBA (zie bijlage 2) en ARBIT 2022 - Artikel 11. Acceptatie (zie bijlage 16).



E.24: Opstellen retransitieplan

Opdrachtnemer stelt een retransitieplan op welke u oplevert op het moment van in beheer name van de applicatie.
De eenmalige kosten voor het opstellen van het retransitieplan zijn vaste kosten en worden niet geïndexeerd. Zie Beschrijvend document.

Het retransitieplan bevat tenminste de volgende onderwerpen:

- Introductie WBA en retransitie
- Scope en afbakening
- Afhankelijkheden en verwachtingen
- Risico's en mitigerende maatregelen
- Wijze van kennisoverdracht en ondersteuning
- Welke relevantie expertise u inzet
- Planning / doorlooptijden / uren
- Wijze waarop u de continuïteit waarborgt
- Wijze waarop u samenwerkt
- Wijze waarop u communiceert
- Informatie over en de wijze waarop overdracht plaatsvindt van:
 - Broncode
 - Applicatie- en logmonitoring
 - Documentatie (zoals handleidingen, instructies, FO, TO) van o.a. API autorisaties, Infrastructuur, Gebruikte componenten Standaard Platform, beheerinstructie Certificaten, OTAP-straat
 - Kennis
 - Callinformatie (vragen, incidenten, problemen en known issues) openstaande en historische
 - Backlog (wijzigingen)
 - Dump van de data uit het online Callregistratiesysteem op het moment van beëindiging van de opdracht oplevert aan IenE

4.4 Samenwerking met Min IenW en Min BZK/Logius (Standaard Platform)

Opdrachtgever hecht grote waarde aan een goede samenwerking met Opdrachtnemer en min BZK/Logius (Standaard Platform).

E.25: Opdrachtnemer dient nauw samen te werken met Logius en conformeert zich aan de werkwijze van Logius/SP, zoals beschreven in de DAP Standaard Platform (SP) (zie bijlage 12) om de continuïteit van WBA te garanderen.

E.26: Na de gunning van de opdracht dient de Opdrachtnemer de WBA SZW omgeving over te zetten naar Standaard Platform (SP). SZW maakt op dit moment nog gebruik van WBA in een testomgeving.

4.5 Freezeperiode

Opdrachtgever voert actief beleid om ervoor te zorgen dat de gepresenteerde situatie van WBA zo min mogelijk aan Wijzigingen onderhevig zal zijn gedurende de periode voorafgaande aan de gunning aan de nieuwe Opdrachtnemer:

Alleen noodzakelijke Wijzigingen zullen worden doorgevoerd en Opdrachtnemer zal tijdig – indien van toepassing – het bijgewerkte Functioneel Ontwerp (FO) en Technisch Ontwerp (TO) ontvangen.



5 Informatiebeveiliging

5.1 Uitgangspunten

Opdrachtnemer moet voldoen aan de beveiligingseisen zoals gesteld in de BIO. De BIO kent echter een aantal normen/maatregelen die niet van toepassing zijn voor dit type Opdrachtnemer. De maatregelen die wel van toepassing zijn worden middels een verwijzing naar de Hoofdstukken en nummers van de maatregelen benoemd in onderstaande tabel in "Maatregelen Opdrachtnemer".

E.27: Eisen op gebied van maatregelen informatiebeveiliging BIO

Opdrachtnemer dient aan **alle** BIO-maatregelen als omschreven in de onderstaande tabel te voldoen.

Maatregelen Opdrachtnemer:

BIO-Nr.	Maatregel
Hoofdgroep 5. Informatiebeveiligingsbeleid	
5.1.1.1	Er is een informatiebeveiligingsbeleid opgesteld door Opdrachtnemer. Dit beleid is vastgesteld door de leiding van Opdrachtnemer en bevat tenminste de volgende punten: a) de strategische uitgangspunten en randvoorwaarden die de organisatie hanteert voor informatiebeveiliging en in het bijzonder de inbedding in, en afstemming op het algemene beveiligingsbeleid en het informatievoorzieningsbeleid; b) de organisatie van de informatiebeveiligingsfunctie, waaronder verantwoordelijkheden, taken en bevoegdheden; c) de toewijzing van de verantwoordelijkheden voor ketens van informatiesystemen aan lijnmanagers; d) de gemeenschappelijke betrouwbaarheidseisen en normen die op de organisatie van toepassing zijn; e) de frequentie waarmee het informatiebeveiligingsbeleid wordt geëvalueerd; f) de bevordering van het beveiligingsbewustzijn.
5.1.2.1	Het informatiebeveiligingsbeleid wordt periodiek en in aansluiting op de (bestaande) bestuurs- en P&C-cycli en externe ontwikkelingen beoordeeld en zo nodig bijgesteld.
Hoofdgroep 6. Organiseren van informatiebeveiliging	
6.1.1.1	De leiding van de organisatie van Opdrachtnemer heeft vastgelegd wat de verantwoordelijkheden en rollen zijn op het gebied van informatiebeveiliging binnen haar organisatie.
6.1.2.1	Er zijn maatregelen getroffen die onbedoelde of ongeautoriseerde toegang tot bedrijfsmiddelen waarnemen of voorkomen.
Hoofdgroep 7. Veilig personeel	
7.1.1.1	Elke organisatie heeft een vastgesteld screeningsbeleid. Bij indiensttreding en bij functiewijziging kan een Verklaring Omtrent het Gedrag (VOG) gevraagd worden.
7.1.2.1	Alle medewerkers (intern en extern) van Opdrachtnemer zijn bij hun aanstelling of functiewisseling gewezen op hun verantwoordelijkheden ten aanzien van informatiebeveiliging. De voor hen geldende regelingen en instructies ten aanzien van informatiebeveiliging zijn eenvoudig toegankelijk.
7.2.1.1	Er is aansluiting bij een klokkenluidersregeling, zodat iedereen anoniem en veilig beveiligingsissues kan melden.



BIO-Nr.	Maatregel
7.2.2.1	Alle medewerkers van Opdrachtnemer hebben de verantwoordelijkheid bedrijfsinformatie te beschermen. Iedereen kent de regels en verplichtingen met betrekking tot informatiebeveiliging en daar waar relevant de speciale eisen voor gerubriceerde omgevingen.
7.2.2.3	Het management van Opdrachtnemer benadrukt bij aanstelling en interne overplaatsing en bijvoorbeeld in werkoverleggen of in personeelsgesprekken bij zijn medewerkers en contractanten het belang van opleiding en training op het gebied van informatiebeveiliging en stimuleert hen actief deze periodiek te volgen.
Hoofdgroep 8. Beheer van bedrijfsmiddelen	
8.1.3.1	Alle medewerkers van Opdrachtnemer zijn aantoonbaar gewezen op de gedragsregels voor het gebruik van bedrijfsmiddelen.
8.1.3.2	De gedragsregels voor het gebruik van bedrijfsmiddelen zijn voor extern personeel van Opdrachtnemer in het contract vastgelegd overeenkomstig de huisregels of gedragsregels.
8.3.2.1	Media die vertrouwelijke informatie bevatten, zijn opgeslagen op een plek die niet toegankelijk is voor onbevoegden.
Hoofdgroep 9. Toegangsbeveiliging	
9.1.2.1	Alleen geauthenticeerde apparatuur kan toegang krijgen tot een vertrouwde zone.
9.2.1.1	Er is een sluitende formele registratie- en afmeldprocedure voor het beheren van gebruikersidentificaties.
9.2.2.1	Er is uitsluitend toegang verleend tot informatiesystemen na autorisatie door een bevoegde functionaris.
9.2.2.2	Op basis van een risicoafweging is bepaald waar en op welke wijze functiescheiding wordt toegepast en welke toegangsrechten worden gegeven.
9.2.5.3	Alle uitgegeven toegangsrechten worden minimaal eenmaal per halfjaar beoordeeld.
9.4.1.2	Gebruikers kunnen alleen die informatie met specifiek belang inzien en verwerken die ze nodig hebben voor de uitoefening van hun taak.
9.4.2.1	Als vanuit een onvertrouwde zone toegang wordt verleend naar een vertrouwde zone, gebeurt dit alleen op basis van minimaal two-factor authenticatie.
9.4.3.1	Als er geen gebruik wordt gemaakt van two-factor authenticatie is de wachtwoordlengte minimaal 8 posities en complex van samenstelling. Vanaf een wachtwoordlengte van 20 posities vervalt de complexiteitseis. Het aantal inlogpogingen is maximaal 10. De tijdsduur dat een account wordt geblokkeerd na overschrijding van het aantal keer foutief inloggen is vastgelegd.
9.4.3.2	In situaties waar geen two-factor authenticatie mogelijk is, wordt minimaal halfjaarlijks het wachtwoord vernieuwd.
9.4.4.1	Alleen bevoegd personeel van Opdrachtnemer heeft toegang tot systeemhulpmiddelen.
Hoofdgroep 11. Fysieke beveiliging en beveiliging van de omgeving	
11.1.4.1	Opdrachtnemer heeft geïnventariseerd welke papieren archieven en apparatuur bedrijfskritisch zijn. Tegen bedreigingen van buitenaf zijn beveiligingsmaatregelen genomen op basis van een expliciete risicoafweging.
11.1.4.2	Bij huisvesting van IT-apparatuur wordt rekening gehouden met de kans op gevolgen van rampen veroorzaakt door de natuur en menselijk handelen.
11.2.9.1	Een onbemensde werkplek is altijd vergrendeld.



BIO-Nr.	Maatregel
11.2.9.4	Het overnemen van sessies op remote werkplekken op een andere werkplek is alleen mogelijk via dezelfde beveiligde loginprocedure als waarmee de sessie is gecreëerd. Na een expliciete risicoafweging mag hiervan worden afgeweken.
Hoofdgroep 12. Beveiliging bedrijfsvoering	
12.1.2.1	In de procedure voor wijzigingsbeheer is minimaal aandacht besteed aan: (a) het administreren van Wijzigingen; (b) risicoafweging van mogelijke gevolgen van de Wijzigingen; (c) goedkeuringsprocedure voor Wijzigingen.
12.1.4.1	In de productieomgeving wordt niet getest. Alleen met voorafgaande goedkeuring door de proceseigenaar en schriftelijke vastlegging hiervan, kan hiervan worden afgeweken.
12.2.1.1	Het downloaden van bestanden is beheerst en beperkt op basis van risico en need-of-use.
12.2.1.3	De gebruikte anti-malware software en bijbehorende herstelsoftware is actueel en wordt ondersteund door periodieke updates.
12.2.1.5	De malware scan wordt op verschillende omgevingen uitgevoerd, bijv. op mailservers, desktopcomputers en bij de toegang tot het netwerk van de organisatie.
12.3.1.1	Er is een back-up beleid waarin de eisen voor het bewaren en beschermen zijn gedefinieerd en vastgesteld.
12.3.1.2	Op basis van een expliciete risicoafweging is bepaald wat het maximaal toegestane dataverlies is en wat de maximale hersteltijd is na een informatiebeveiligingsincident.
12.3.1.5	De restore procedure wordt minimaal jaarlijks getest of na een grote wijziging om de goede werking te waarborgen als deze in noodgevallen uitgevoerd moet worden
12.4.1.1	Een logregel bevat minimaal de gebeurtenis; de benodigde informatie die nodig is om het informatiebeveiligingsincident met hoge mate van zekerheid te herleiden tot een natuurlijk persoon; het gebruikte apparaat; het resultaat van de handeling; een datum en tijdstip van de gebeurtenis.
12.4.2.1	Er is een overzicht van logbestanden die worden gegenereerd.
12.4.2.2	Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd.
12.6.1.1	Als de kans op misbruik en de verwachte schade beide hoog zijn (NCSC-classificatie kwetsbaarheidswaarschuwingen), worden patches zo snel mogelijk, maar uiterlijk binnen een week geïnstalleerd. In de tussentijd worden op basis van een expliciete risicoafweging mitigerende maatregelen getroffen.
Hoofdgroep 13. Communicatiebeveiliging	
13.1.2.4	In koppelpunten met externe of onvertrouwde zones zijn maatregelen getroffen om mogelijke aanvallen die de beschikbaarheid van de informatievoorziening negatief beïnvloeden (bijv. DDoS attacks, Distributed Denial of Service) te signaleren en hierop te reageren.
Hoofdgroep 14. Acquisitie, ontwikkeling en onderhoud van informatiesystemen	
14.2.1.1	De gangbare principes rondom 'security by design' zijn uitgangspunt voor de ontwikkeling van software en systemen.
14.2.2.1	Wijzigingsbeheer vindt plaats op basis van een algemeen geaccepteerd beheerframework.
14.2.7.1	Een voorwaarde voor uitbestedingstrajecten is een expliciete risicoafweging. De noodzakelijke beveiligingsmaatregelen die daaruit volgen worden aan de leverancier opgelegd.



BIO-Nr.	Maatregel
14.2.9.1	Voor acceptatietesten van systemen worden gestructureerde testmethodieken gebruikt. De testen worden bij voorkeur geautomatiseerd uitgevoerd.
14.2.9.2	Van de resultaten van de testen wordt verslag gemaakt.
Hoofdgroep 15. Leveranciersrelaties	
15.1.1.1	Bij offerteaanvragen waar informatie(voorziening) een rol speelt, worden eisen t.a.v. informatiebeveiliging (beschikbaarheid, integriteit en vertrouwelijkheid) benoemd.
15.1.1.3	Met alle leveranciers die als verwerker voor of namens de organisatie persoonsgegevens verwerken, worden verwerkersovereenkomsten gesloten waarin alle wettelijk vereiste afspraken zijn vastgesteld.
Hoofdgroep 16. Beheer van informatiebeveiligingsincidenten	
16.1.2.1	Er is een meldloket waar informatiebeveiligingsincidenten kunnen worden gemeld.
16.1.2.2	Er is een meldprocedure waarin de taken en verantwoordelijkheden van het meldloket staan beschreven.
16.1.2.3	Alle medewerkers van Opdrachtnemer en contractanten van Opdrachtnemer hebben aantoonbaar kennisgenomen van de meldingsprocedure van informatiebeveiligingsincidenten.
16.1.2.4	Informatiebeveiligingsincidenten worden zo snel mogelijk, maar in ieder geval binnen 24 uur na bekendwording, intern gemeld.
16.1.2.6	De opvolging van informatiebeveiligingsincidenten wordt maandelijks gerapporteerd aan de verantwoordelijke.
Hoofdgroep 18. Naleving	
18.1.4.2	Organisaties controleren regelmatig de naleving van de privacyregels en informatieverwerking en -procedures binnen hun verantwoordelijkheidsgebied aan de hand van de desbetreffende beleidsregels, normen en andere eisen betreffende beveiliging.

Naast de benoemde BIO maatregelen (zie tabel hierboven) dient Opdrachtnemer te voldoen aan de volgende eisen wat betreft de afgesproken Dienstverlening van het product WBA:

- E.28:** Opdrachtnemer meldt informatiebeveiligingsincidenten binnen 48 uur aan de opdrachtgever;
- E.29:** Na elke patch levert Opdrachtnemer maximaal binnen een maand een patch report aan de Opdrachtgever van welke patches zijn doorgevoerd;
- E.30:** Na elke security bevinding levert Opdrachtnemer een security advies binnen 48 uur;
- E.31:** Opdrachtnemer is in staat vragen omtrent kwetsbaarheden te beantwoorden;
- E.32:** De Opdrachtgever heeft een 'right to audit';
- E.33:** Opdrachtnemer levert maandelijks een overzicht aan van de status van bestaande kwetsbaarheden;
- E.34:** Opdrachtnemer is in staat vragen omtrent kwetsbaarheden te beantwoorden;
- E.35:** Opdrachtnemer heeft een contactpersoon voor informatiebeveiliging die invulling geeft op bovenstaande punten;
- E.36:** Bij gebruik van softwarecomponenten van derden, draagt Opdrachtnemer er zorg voor dat deze componenten minimaal hetzelfde beveiligingsniveau kennen zoals gesteld aan de software die door Opdrachtnemer wordt geleverd.



6 Applicatiebeheer en Doorontwikkeling

6.1 Inleiding

Informatiesystemen worden gemaakt, onderhouden en aangepast om voortdurend de functionaliteit te leveren die gewenst is, passend bij de bedrijfsprocessen.

Het bedrijfsproces van IenW is continu onderhevig aan wijzigingen. Dit leidt ertoe dat de informatievoorziening ook aan verandering onderhevig is. De doelstelling van de processen t.a.v. Applicatiebeheer en Doorontwikkeling is zorgdragen dat WBA tijdens exploitatie wordt aangepast en daarmee het bedrijfsproces optimaal blijft ondersteunen.

De doelstelling van Applicatiebeheer is ervoor zorgen dat WBA tijdens exploitatie en gebruik optimaal wordt ingezet ter ondersteuning van het bedrijfsproces van Min IenW, met een minimum aan middelen en verstoringen in de operatie.

- E.37:** Min IenW hanteert voor de te leveren Dienstverlening een aantal standaarden (frameworks), zoals ITIL, BiSL en Agile. Opdrachtnemer dient de standaarden die Min IenW hanteert als uitgangspunt te nemen voor de te leveren Dienstverlening van deze opdracht.
- E.38:** Voor het opleveren en in productie brengen van Wijziging(en) en/of releases, al dan niet gegroepeerd, zal er een vaste opleverdag per week worden afgesproken. Hier kan in onderling overleg van worden afgeweken.
- E.39:** Alle Wijzigingen en meldingen worden geregistreerd in het Callregistratiesysteem van Opdrachtnemer. Het registreren, actueel houden en bewaken van deze registraties is een gezamenlijke verantwoordelijkheid van Opdrachtnemer en Opdrachtgever en zal in het periodieke overleg worden besproken met betrokken partijen.
- E.40:** Bijlage 2 betreft de checklist die wordt gehanteerd bij het in beheer nemen van Wijzigingen WBA. IenE stemt per in beheer te nemen Wijziging met Opdrachtnemer af welke items op de checklist van toepassing zijn. Opdrachtnemer dient aan de items te voldoen die van toepassing zijn.
- E.41:** Bij het doorvoeren van veranderingen zorgt opdrachtnemer ervoor dat WBA blijft voldoen aan de volgende uitgangspunten ten aanzien van de werkplek
 - Toegankelijkheid via browsers (OS, browser, versie):
 - Windows:
 - Edge, n/n-1
 - FireFox, ESR
 - Chromebook:
 - Chrome n/n-1
 - IOS/Android: BB Access, n
 - De applicatie dient geen gebruik te maken van applicatiecomponenten, zoals plug-ins en applets.
 - Applicatie en gegevens zijn van elkaar gescheiden, zodat het vervangen van een applicatie geen nadelige consequenties heeft voor de ontsluiting van de gegevens.

In dit Hoofdstuk worden diverse werkzaamheden, taken en verantwoordelijkheden nader beschreven en toegelicht. Min IenW realiseert zich dat de uitwerking in dit document gegeven de omvang en de diepgang van de standaarden beperkt is.



6.2 Applicatiebeheerprocessen

De voorziene werkzaamheden m.b.t. Applicatiebeheer en onderhoud WBA (Vaste Dienstverlening) worden in deze paragraaf gerelateerd aan de applicatiebeheerprocessen. De volgende sub paragrafen geven een opsomming van voorziene processen (is niet uitputtend, maar geeft wel een goed beeld).

- E.42:** Opdrachtnemer dient zich te conformeren aan de werkwijze zoals beschreven in deze paragraaf en in de subparagrafen (**6.2.1 en 6.2.2**) van deze paragraaf.

6.2.1 Incidentbeheer

Daartoe geautoriseerde medewerkers zullen Incidenten melden aan Opdrachtnemer. Doelstelling, bij het oplossen van gemelde Incidenten, is het zorgen voor een zo spoedig mogelijk herstel van het afgesproken servicelevel (vastgelegd in de SLA). Opdrachtnemer dient een derdelijns Servicedesk te leveren en, waar nodig, operationele ondersteuning aan IenE.

6.2.2 Overige beheerprocessen

Naast Incidentbeheer onderkent Min IenW nog meer beheerprocessen, namelijk: Configuratiebeheer, Beschikbaarheidsbeheer, Capaciteitsbeheer en Continuïteitsbeheer. Deze processen worden ook uitgevoerd door de hostingpartij Min BZK/Logius (Standaard Platform).

6.3 Doorontwikkeling

- E.43:** Acceptatie (FAT, GAT, PAT) vindt plaats in de acceptatieomgeving op het Standaard Platform.

Opdrachtnemer dient zorg te dragen na goedkeuring van Min IenW dat de Wijzigingen overgezet worden van de acceptatieomgeving naar de productieomgeving van Opdrachtgever. Dit zal onder regie van IenE plaatsvinden.

Doorontwikkeling van WBA valt uiteen in verschillende gebieden die nauw aan elkaar gerelateerd zijn. In de volgende subparagrafen volgt een korte toelichting van elk gebied.

Opdrachtnemer dient zich te conformeren aan de werkwijze zoals beschreven in deze inleidende paragraaf en in de subparagrafen (**6.3.1 t/m 6.3.7**) van deze paragraaf.

6.3.1 Wijzigingen

Het doel van wijzigingsmanagement is het gecontroleerd laten doorvoeren van Wijzigingen met zo weinig mogelijk risico voor de continuïteit van de bedrijfsvoering. Het resultaat van het wijzigingsproces is een nieuwe, functioneel gewijzigde of verbeterde, versie van de applicatie op de productieomgeving.

6.3.2 Impactanalyse

Opdrachtnemer is verantwoordelijk voor het uitvoeren van een impactanalyse op de (gewenste) Wijziging.

In dit proces wordt uitgezocht wat de gevolgen (impact) zijn van voorgestelde Wijzigingen.

Doel van het proces is het op een effectieve wijze in kaart brengen van voldoende betrouwbare en nauwkeurige consequenties in termen van inspanning, toekomst, gebruik en exploitatie van voorgestelde Wijzigingen, zodat de optimale oplossingsrichting gekozen kan worden.

6.3.3 Ontwerp

Het proces 'ontwerp' heeft als doel de door IenE aangeleverde (gebruikers)specificaties voor WBA op een dusdanige wijze op te stellen en vast te leggen, zodat deze daarna op een eenduidige wijze kunnen worden gerealiseerd en getest.



De voorziene werkzaamheden zijn:

- Het eenduidig specificeren van de oplossingsrichting en bijbehorende werkzaamheden;
- Opstellen en onderhouden van het functioneel ontwerp, met daarin een uitwerking van de oplossingsrichting;
- Opstellen en onderhouden van testspecificaties/testontwerp;
- Het opstellen en uitwerken van een plan van aanpak voor de realisatie inclusief en testplan.

6.3.4 Realisatie

Tijdens de realisatie wordt de functionele specificatie uit het ontwerpproces omgezet naar concrete wijzigingen aan WBA. Waar nodig wordt er een technisch ontwerp opgesteld of aangepast en wordt de technische impact getoetst. Na de technische uitwerking vindt de daadwerkelijke realisatie plaats.

Het resultaat is een change package, met daarin de gewijzigde programmaonderdelen en databestanden.

Opdrachtnemer moet voorkomen dat fouten die er reeds bij eerdere releases uit zijn gehaald, opnieuw optreden.

6.3.5 Testen

Het uitvoeren van testen (w.o. Unit Test, Integratietest, Systeemtest en PAT) op basis van een testplan, testdata en testscripts, om vast te stellen dat hetgeen is gevraagd, beschreven en ontworpen ook daadwerkelijk is gerealiseerd en zo voldoet aan de eisen 'op te leveren werk'. Deze testen dienen uitgevoerd te worden in een 'zo veel als mogelijk' aan Min IenW gelijkwaardige omgeving(en).

Hieronder vallen ook de volgende verantwoordelijkheden:

- Oplevering aan Min IenW van deze testscripts, testdata en testrapporten zodat Min IenW weet dat er door Opdrachtnemer afdoende is getest en wat er is getest. Op basis daarvan kan Min IenW zonder inrichtingsinspanning starten met de acceptatie (FAT en GAT) in de acceptatieomgeving;
- Ondersteuning bij de acceptatietesten en het herstellen van fouten en onvolkomenheden in de acceptatieomgeving.

De testen vinden plaats in afstemming met IenE samen met de gebruikers (DCO). Initiatief hiervan ligt bij IenE.

6.3.6 Implementatie

Onder implementatie verstaat Min IenW de in productie name van het gewijzigde WBA, zoals:

- Installeren van nieuwe versies/patches op acceptatie- en na afstemming én akkoord in productieomgeving.
Het installeren van nieuwe versies/patches op de acceptatie- en productieomgeving vindt plaats onder begeleiding van IenE en, daar waar nodig, de hosting partij MinBZK/Logius
- Bijwerken implementatiedocumentatie;
- Stand-by zijn voor installatie, roll back en vragen;
- Afronden projectdocumentatie;
- Verzoek tot decharge;
- Overdragen aan IenE (aanpassen beheerdocumentatie).

Opdrachtnemer biedt ondersteuning bij de in gebruik- en in productie name. Ook documenteert Opdrachtnemer, tijdens de uitvoering van deze opdracht, in een projectdossier (archief) alles wat redelijkerwijs noodzakelijk en/of van belang is, als (achtergrond)informatie, ten behoeve van Applicatiebeheer én Doorontwikkeling. Het onderhouden van het projectdossier en opstellen van documentatie is een integraal onderdeel van het leveringsproces. Na elke oplevering geeft



Opdrachtnemer aan welke documentatie is aangepast of legt uit dat de documentatie geen aanpassing behoeft.

Er worden twee soorten documentatie onderscheiden:

1. Systeemdokumentatie, waaronder het functioneel ontwerp (FO), technisch ontwerp (TO), datamodel, broncode, testdossier en de implementatiedokumentatie.
2. Beheerdokumentatie, waaronder de installatie- en configuratiehandleiding.

6.3.7

Webcertificaatbeheer

In de loop van 2024 kan het zijn dat Min IenW overstapt op een nieuw aanvraagplatform voor webcertificaten, waardoor onderstaande procedure zou kunnen veranderen. Tot die tijd dient Opdrachtnemer het onderstaande proces te ondersteunen:

Het webcertificaat wordt geleverd door Min IenW.

Om een webcertificaat te maken voor WBA zal Opdrachtnemer het benodigde CRS-bestand door een technische beheerder van Opdrachtnemer creëren op de server waar het webcertificaat later geïnstalleerd wordt.

Het complete bestand zal door Opdrachtnemer aan Functioneel Beheer worden overhandigd die er voor zorg draagt dat het webcertificaat wordt gemaakt.

Tevens moet duidelijk zijn of het een public (browser) of private (machine-to-machine) webcertificaat moet zijn. Bij private is de vraag of het een webcertificaat voor 1, 2 of 3 jaar moet zijn. Bij public is het altijd max 1 jaar.

Min IenW houdt de geldigheid in de gaten en neemt tijdig contact op met Opdrachtnemer om een eventuele verlenging te bespreken.



7 Service Level Management: afspraken en rapportage

7.1 Service Level Management

Service Level Management heeft als doelstelling het bewaken en verbeteren van de klanttevredenheid en het verbeteren van de aan klant geleverde Dienstverlening. Dit houdt in: het vormgeven van de klant-leveranciersverhouding, het maken en bewaken van de afspraken tussen Opdrachtgever en Opdrachtnemer en het actualiseren van deze afspraken.

De afspraken over het vereiste kwaliteitsniveau van de Dienstverlening worden vastgelegd in een Service Level Agreement (SLA).

E.44: De SLA dient opgesteld te worden door Opdrachtnemer.

Toelichting:

Van de Opdrachtnemer wordt vereist om een integrale SLA bij de offerte aan te bieden die conformeert aan de serviceniveau eisen in het programma van eisen van applicatiebeheer en ontwikkeling waarvan de Opdrachtnemer de eindverantwoordelijkheid draagt. Deze SLA maakt onderdeel uit van de Overeenkomst en normeert het overeengekomen dienstverleningsniveau. (zie Concept Overeenkomst ARBIT – WBA (bijlage 10).

7.2 Dienstverleningsvenster

E.45: Opdrachtnemer dient de Dienstverlening te leveren op werkdagen van Min IenW (van maandag t/m vrijdag) tussen 07.00 uur en 18.00 uur.

E.46: Onbeschikbaarheid WBA altijd in/na overleg met Opdrachtgever

Toelichting

Alle aanpassingen waarbij WBA "uit de lucht" moet (zowel gepland als ongepland) geschieden uitsluitend in overleg met Opdrachtgever. Deze aanpassingen zullen tijdens kantooruren worden uitgevoerd, in sommige gevallen daarbuiten, tussen 17.30 uur en uiterlijk 20.00 uur diezelfde dag.

Werkzaamheden in de acceptatieomgeving kunnen tijdens de reguliere werktijden worden uitgevoerd.

7.3 Prioriteitsindeling Incidenten

E.47: Er zijn drie categorieën van urgentie om de oplossingstijd van een Incident te bepalen:

- | | |
|---------|--|
| Hoog: | Oplossing Incident kan geen uitstel verdragen, bijvoorbeeld omdat betrokkenen de functionaliteit in zijn geheel niet meer kunnen gebruiken. |
| Midden: | Oplossing Incident kan enige uitstel verdragen, bijvoorbeeld omdat er een work around is of betrokkenen nog deels gebruik kunnen maken van de functionaliteit. |
| Laag: | Oplossing Incident kan uitstel verdragen, bijvoorbeeld omdat betrokkenen de functionaliteit wel kunnen gebruiken maar de werking enigszins verstoord is (bijv. slechte performance). |

De prioritering van een Incident is ook afhankelijk van het aantal gebruikers dat getroffen is:

- | | |
|---------|--|
| Hoog: | Alle of een zeer groot aantal gebruikers is getroffen door de verstoring. Tevens wordt een Incident als hoog aangemerkt indien een prioritair proces verstoord wordt (samenstelling knipselkranten en het proces van sociale media monitoring) |
| Midden: | Een substantieel aantal gebruikers is getroffen door de verstoring. |



Laag: Eén of enkele gebruikers zijn getroffen door de verstoring.

Dit leidt tot de volgende prioriteitsindeling:

Prioriteit		Urgentie		
		Hoog	Midden	Laag
Impact	Hoog	M(ajor)	1	2
	Midden	1	2	3
	Laag	2	3	3

Opdrachtnemer dient zich te conformeren aan de prioriteitsindeling zoals beschreven in deze paragraaf.

7.4 Oplostijden Incidenten

E.48:

Prioriteit	Reactietijd (aangevangen met analyse)	Oplostijd	norm
Prioriteit M (Major)	1 uur	4 uur	98%
Prioriteit 1 (Hoog)	4 uur	2 werkdagen *	98%
Prioriteit 2 (Midden)	2 werkdagen	5 werkdagen *	98%
Prioriteit 3 (Laag)	2 werkdagen	10 werkdagen *	98%

* Indien Incidenten met prioriteit 1, 2 of 3, middels een bugfix moeten worden opgelost, dan worden deze in de eerstvolgende release meegenomen, tenzij anders is besproken en uiteindelijk besloten door Min IenW. Voor deze Incidenten geldt dat er binnen de afgesproken Oplostijd een impactanalyse moet worden opgeleverd.

N.B. Bijlage 9 geeft inzicht in de aantallen Incidenten en bevindingen van de afgelopen jaren.

Oplostijden Service Requests

Hoog: Service Requests waarvoor geldt dat het gevraagde resultaat of product van cruciaal belang is voor de gebruiker ofwel voor de uitvoering van een kritiek bedrijfsproces.

Standaard: Service Requests waarvoor geldt dat het gevraagde resultaat ofwel product van belang is voor de gebruiker ofwel voor de uitvoering van een bedrijfsproces.

Categorie	Oplostijd	norm
Hoog	1 werkdag	98%
Standaard	5 werkdagen	98%

Oplostijden Wijzigingsverzoeken

Voor die gevallen waarin een uitgebreide impactanalyse noodzakelijk is: de Oplostijd voor het opstellen van een impactanalyse voor een Wijzigingsverzoek is 10 werkdagen. Ook hierbij is de norm 98%.

Opdrachtnemer dient zich te conformeren aan alle Oplostijden (voor zowel incidenten, service requests en wijzigingsverzoeken) zoals beschreven in deze paragraaf.



7.5 Dienstverleningsvenster Informatiebeveiliging

Hoofdstuk 5 handelt over Informatiebeveiliging, waarin ook een aantal servicelevels staat genoemd (zie eis E.23).

7.6 Dienstverleningsrapportage

E.49: Opdrachtnemer dient zich te conformeren aan de werkwijze zoals beschreven in deze paragraaf en in de subparagrafen (**7.6.1 t/m 7.6.3**) van deze paragraaf.

7.6.1 Frequentie

Opdrachtnemer rapporteert gedurende de looptijd van de Dienstverlening over de geleverde Dienstverlening: eenmaal per kwartaal.

7.6.2 Sluitende onderbouwing

De rapportage dient informatie te bevatten zodat verifieerbaar is dat de Diensten, zoals Reactietijden en Oplostijden verricht zijn zoals overeengekomen.

7.6.3 Inhoud rapportage

Opdrachtnemer rapporteert over:

Vaste Dienstverlening (Applicatiebeheer)

In de Dienstverleningsrapportage wordt aandacht besteed aan de vereiste Dienstverlening. Tenminste de volgende onderwerpen maken deel uit van deze rapportage:

- Geleverde Dienstverlening zoals voor instandhouding beheer en preventief beheer en onderhoud.
 - Incidentbeheer (overzicht van Calls)
 - Per Call staat de aangemerkte prioriteit, Reactietijd en de gerealiseerde Oplostijd.
 - 98% norm gehaald of niet, inclusief argumentatie.
 - Nog openstaande Incidenten, inclusief de acties die ondernomen zijn en nog worden, teneinde tot een oplossing te komen (inclusief uiterlijke hersteldatum)

Indien er afwijkingen zijn dienen deze vermeld te worden samen met een beschrijving van de acties die ondernomen worden om de Dienstverlening uiterlijk te herstellen.

Variabele Dienstverlening (Doorontwikkeling)

Er moet gerapporteerd worden over tenminste:

- Overzicht aantal Wijzigingsverzoeken
 - Per Call staat de aangemerkte prioriteit, Reactietijd en de gerealiseerde Oplostijd
 - 98% norm gehaald of niet, inclusief argumentatie
- Alle dienstverleningsverzoeken die nog niet gesloten zijn.
- Alle dienstverleningsverzoeken die in de betreffende maand ingediend zijn.
- Overzicht aantal verbeterplannen en de genomen maatregelen.
- Besteding uren Variabele Dienstverlening en resterend tegoed aan uren
- Evaluatie van doorgevoerde Wijzigingen/releases: korte beschrijving verloop van de Wijziging/release, inclusief samenwerking hosting partij SP en IenE/DCO en leerpunten volgende release.
- Rapportage voortgang doorontwikkelprojecten, inclusief urenbesteding en te besteden budget. Eventueel (voorziene) afwijkingen ten aanzien van de afgegeven planning/deadline en de reden(en) daarvoor.
- Vermelden welke documentatie n.a.v. welke doorgevoerde Wijziging is bijgewerkt.

8 Hosting

8.1 Standaard Platform

De productie- en de applicatie-omgevingen van WBA zijn op het Standaard Platform van Min BZK/Logius geplaatst. Van het Standaard Platform worden algemene diensten afgenomen: Loadbalancing & Ingress, E-mail Gateway, Monitoring, Logging, Backups, Deployment via GitLab en een Container Registry (Harbor). Deze diensten zijn geen onderdeel van de uitvraag.

Op de website van Min BZK/Logius staat nadere informatie over het Standaard Platform via de link: [Standaard Platform | Logius](#)

E.50: Opdrachtnemer dient zich te conformeren aan de eisen en voorwaarden van het Standaard Platform. Per 1 januari 2024 is er een nieuwe versie van de aansluitvoorwaarden actief, deze zijn te vinden via de link: [Aansluitvoorwaarden Standaard Platform | Logius](#)

Bijlage 12 betreft de DAP van Min BZK/Logius m.b.t. Standaard Platform.

