

Service level Agreement

Applicatie voor digitale brede handhaving 2027-2037

gemeente Soest



Inhoudsopgave servicelevel afspraken

1. Inleiding	3
1.1 Doel van de SLA	3
1.2 Geldigheidsduur	3
1.3 Wijzigingsprocedure	3
2. Service- en onderhoudsvenster	4
2.1 Servicevenster	4
2.2 Onderhoudsvenster	4
3. Helpdesk	4
3.1 Verantwoordelijkheden	4
3.2 Bereikbaarheid en beschikbaarheid	4
3.3 Kosten	4
4. Prestaties	5
4.1 Beschikbaarheid Applicatie en bijbehorende dienstverlening	5
4.2 Capaciteit en performance	5
4.3 Afwijking van afspraken	5
5. Processen	6
5.1 Rapportages	6
5.2 Incidentenbeheer	6
5.3 Wijzigingsbeheer	7
5.4 Problem management	8
5.5 Vraag- en adviesproces	9
5.6 Klachtenmanagement	9
6. Softwareonderhoud en Releasebeheer	10
6.1 Continuïteit van functionaliteit	10
6.2 Uitfasering en doorontwikkeling	10
6.3 Releasekalender en aankondigingen	10
6.4 Releasenotes	10
6.5 Patch- en kwetsbaarhedenbeheer	10
6.6 Beveiligings- en compliancerapportage	11
7. Back-up & Herstel	13
7.1 Back-upvoorzieningen	13
7.2 Testen en validatie	13
7.3 Rapportage en inzicht	13



1. Inleiding

1.1 Doel van de SLA

Dit document 'Service Level Afspraken' (verder te noemen SLA) bevat een concrete beschrijving van servicelevels en prestatie indicatoren die gelden voor de levering, implementatie en beheer van de Handhavingsapplicatie door Opdrachtnemer. Dit document is onlosmakelijk verbonden met de Overeenkomst en het Programma van Eisen en Wensen.

1.2 Geldigheidsduur

Deze SLA kent een looptijd vanaf de startdatum van de overeenkomst tot en met de beëindiging van de overeenkomst.

1.3 Wijzigingsprocedure

De inhoud van de SLA is de gezamenlijke verantwoordelijkheid van Opdrachtnemer en Opdrachtgever. Voorstellen tot wijzigingen op dit document worden tussen Opdrachtnemer en de Contract manager van Opdrachtgever vastgesteld. Wijzigingen op de SLA dienen te passen binnen de kaders die gedefinieerd zijn in de geldende overeenkomst tussen Opdrachtgever en Opdrachtnemer. In het Dossier van Afspraken en Procedures (DAP) staan de betrokken rollen en contactpersonen beschreven.



2. Service- en onderhoudsvenster

2.1 Servicevenster

Het servicevenster is de tijd waarbinnen een beroep gedaan kan worden op de dienstverlening van Opdrachtnemer. Het servicevenster is op werkdagen van maandag tot en met vrijdag van 08:00 u tot 17:00 uur, met uitzondering van nationaal erkende feestdagen.

2.2 Onderhoudsvenster

Het onderhoudsvenster is de periode waarbinnen geplande werkzaamheden met een (verhoogd risico op) downtime van de dienst(en) kunnen worden uitgevoerd. Geplande werkzaamheden die gevolgen kunnen hebben voor de beschikbaarheid van de dienstverlening worden vooraf afgestemd met Opdrachtgever.

Het onderhoudsvenster voor (geautomatiseerde) werkzaamheden van Opdrachtnemer is dagelijks van 18:00 uur tot 08:00 uur. In gevallen waarin spoedwerkzaamheden of incidenten directe actie vereisen, kan na voorafgaande toestemming van Opdrachtgever van dit onderhoudsvenster worden afgeweken.

3. Helpdesk

Opdrachtnemer levert een Nederlandstalige helpdesk die fungeert als single point of contact voor de beheerders van Opdrachtgever. De helpdesk is het centrale aanspreekpunt voor het stellen van vragen, het melden van incidenten en het indienen van wijzigingsverzoeken, evenals voor het verstrekken van informatie over de voortgang en afhandeling daarvan.

3.1 Verantwoordelijkheden

De helpdesk is verantwoordelijk voor de registratie, behandeling en afhandeling van alle meldingen, incidenten, wijzigingsverzoeken, problems en vragen die betrekking hebben op de geleverde Applicatie en bijbehorende dienstverlening.

3.2 Bereikbaarheid en beschikbaarheid

- De helpdesk is toegankelijk via een beveiligd webportaal en daarnaast telefonisch bereikbaar voor meldingen of vragen met een hoge prioriteit of urgentie.
- De telefonische helpdesk is bereikbaar gedurende het servicevenster zoals beschreven in paragraaf 2.1.
- Het webportaal is 24 uur per dag, 7 dagen per week beschikbaar voor het indienen van vragen, incidentmeldingen en wijzigingsverzoeken.
- Alle via het webportaal ingediende meldingen worden automatisch geregistreerd en bevestigd.
- De voortgang en status van meldingen kunnen door Opdrachtgever via het webportaal real-time worden geraadpleegd.
- Meldingen die buiten het servicevenster worden ingediend, worden geregistreerd op het moment van ontvangst en in behandeling genomen vanaf het eerstvolgende servicevenster, tenzij in deze SLA anders is bepaald.

3.3 Kosten

Voor het gebruik van de helpdesk en de ondersteuning die door Opdrachtnemer via deze helpdesk wordt geleverd, worden geen aanvullende kosten in rekening gebracht.



4. Prestaties

4.1 Beschikbaarheid Applicatie en bijbehorende dienstverlening

De beschikbaarheid is de totale tijdsduur waarin de Applicatie en bijbehorende dienstverlening daadwerkelijk voor Opdrachtgever beschikbaar is geweest, uitgedrukt in een percentage van de totale tijdsduur.

- Opdrachtnemer heeft een resultaatsverplichting om de geleverde dienst(en) 24/7/365 beschikbaar te laten zijn voor Gebruikers. Voor deze verplichting geldt dat de Applicatie en bijbehorende dienstverlening beschikbaar is indien er, gedurende het tijdsvenster, geen incidenten zijn met prioriteit 1.
- De maximaal aaneengesloten periode gedurende het servicevenster waarin de Applicatie en bijbehorende dienstverlening niet beschikbaar is, mag de grens van vier (4) aaneengesloten uren niet overschrijden.
- Gepland onderhoud binnen het servicevenster, waarvoor toestemming door Opdrachtgever is verleend, telt niet mee voor de bepaling van de beschikbaarheid.
- De beschikbaarheid van Testomgevingen tellen niet voor de bepaling van deze beschikbaarheid.
- De norm voor de beschikbaarheid van de Applicatie en bijbehorende dienstverlening is 99,8% per kalendermaand binnen het gegarandeerde beschikbaarheidsvenster van 08:00 uur tot 17:00 uur. Een beschikbaarheid van 99,8% betekent een maximale niet-beschikbaarheid van 0,2% per kalendermaand. Uitgaande van een beschikbaarheidsvenster van 9 uur per werkdag en gemiddeld 21,75 werkdagen per maand bedraagt de maximale niet-beschikbaarheid $0,2\% \times 9 \times 21,75 = 0,39$ uur, oftewel circa 23,5 minuten per maand binnen het beschikbaarheidsvenster.

4.2 Capaciteit en performance

In de Applicatie en bijbehorende dienstverlening kan met het aantal aangegeven gebruikers tegelijkertijd worden gewerkt zonder merkbaar performanceverlies. Afwijking van bovenstaande normen heeft geen consequenties indien Opdrachtnemer kan aantonen dat deze afwijking redelijkerwijs veroorzaakt wordt door factoren buiten de invloed van Opdrachtnemer. Dit geldt alleen als dit expliciet wordt aangetoond door Opdrachtnemer, waarbij te allen tijde een schriftelijke, deugdelijke onderbouwing wordt opgeleverd.

Opdrachtgever is gerechtigd deze onderbouwing door een (externe) specialist te laten toetsen.

4.3 Afwijking van afspraken

Wanneer uit de rapportages blijkt dat de beschikbaarheid of performance eisen niet zijn gehaald, komt Opdrachtnemer met een verbeterplan. Dit verbeterplan, de acties daaruit volgend en de voortgang van deze acties worden in het periodieke Service Level overleg besproken. De frequentie, inhoud en deelnemers van dit overleg staan verder beschreven in het Dossier van Afspraken en Procedures (DAP). Opdrachtgever hanteert voor de afgesproken SLA's het volgende escalatiemodel:

Stap 1: Bij het niet behalen van een afgesproken SLA, zal Opdrachtgever dit samen met Opdrachtnemer bespreken en hier afspraken over maken en hier een redelijke hersteltermijn voor afspreken (bovengenoemde verbeterplan).

Stap 2: Na het verstrijken van deze termijn, zal samen bekeken worden of de gestelde doelen inmiddels gerealiseerd zijn. Mocht dit niet zo zijn, dan wordt wederom de mogelijkheid geboden dit op orde te brengen binnen een redelijk gestelde termijn.

Stap 3: Mochten na de tweede gestelde termijn de doelen wederom niet gehaald worden, dan zal Opdrachtnemer in gebreke gesteld worden. Eventuele kosten welke voortvloeien uit deze ingebrekestelling kunnen door Opdrachtgever doorberekend worden aan Opdrachtnemer.

Stap 4: Wanneer de gestelde doelen niet verbeteren, dan kan Opdrachtgever besluiten om verdere stappen te ondernemen, waaronder het niet verlengen van de overeenkomst.



5. Processen

Dit hoofdstuk omschrijft de prestatie indicatoren van processen gerelateerd aan het beheer van de Applicatie en bijbehorende dienstverlening van Opdrachtnemer. Specifieke afspraken over zowel de samenwerking als deze processen staan beschreven in het DAP.

5.1 Rapportages

De rapportages over onderstaande processen waarover Opdrachtnemer periodiek rapporteert aan Opdrachtgever bevatten minimaal:

- Uniek meldingsnummer
- Datum en tijd van melding
- Naam van de melder
- Prioriteit
- Impact en urgentie
- Naam van de behandelaar
- Reactietijd gehaald binnen de gestelde norm?
- Levertijd gehaald binnen de gestelde norm?
- Hersteltijd gehaald binnen de gestelde norm?
- Datum en tijd van de oplossing
- Totale doorlooptijd van de melding tot en met oplossing
- Gerealiseerde beschikbaarheid van de Applicatie en bijbehorende dienstverlening
- Totale downtime (indien van toepassing)
- Aantallen meldingen per soort melding, per periode
- Aantallen nog openstaande meldingen, per soort melding per periode
- De oorzaak van verstoringen en de genomen verbetermaatregelen
- Trends of structurele thema's
- Kansen voor optimalisatie of verbeteringen

Waarbij een melding betrekking kan hebben op een incident, wijziging, probleem, vraag of advies. Voor de communicatie en rapportage over prioriteit 1 meldingen worden in het DAP de afspraken verder uitgewerkt. Net als over de frequentie van de rapportages en wanneer de rapportages beschikbaar moeten zijn.

Indien in de rapportageperiode een restoretest is uitgevoerd, bevat de periodieke rapportage ten minste de datum van uitvoering, het resultaat van de test, geconstateerde afwijkingen en de getroffen of geplande verbetermaatregelen.

Naast procesrapportages kan Opdrachtgever aanvullende dienstgerichte rapportages verlangen, waarin de prestaties en kwaliteit van de afzonderlijke ICT-diensten inzichtelijk worden gemaakt.

5.2 Incidentenbeheer

Incidentenbeheer is het proces waarin verstoringen in de geleverde dienst(en) worden hersteld. De term Incident wordt in dit document gebruikt om aan te geven dat de werking van een geleverde dienst afwijkt van hetgeen verwacht mag worden, op basis van Aanbestedingsdocumenten waarbij deze afwijking niet van tevoren is aangemeld in het kader van preventief onderhoud.

- Elk incident dat bij de servicedesk van Opdrachtnemer wordt gemeld, krijgt een bepaalde prioriteitsstelling. Prioriteitsstelling vindt plaats op grond van impact en urgentie, zoals aangegeven in tabel 1.1. De prioriteit van een incident wordt vastgesteld in samenspraak met de contactpersoon van Opdrachtnemer. Indien er geen overeenstemming is, stelt Opdrachtgever de prioriteit, en in geval van meerdere incidenten, de volgorde van afwikkeling van de incidenten vast.
- In tabel 1.2 zijn de reactie- en hersteltijden opgenomen.
- Er geldt geen beperking voor wat betreft het aantal gemelde incidenten.



- De afhandeling van incidenten dient in de aangeboden tarieven te zijn inbegrepen.

		Urgentie		
		Hoog	Middel	Laag
Impact	Hoog	P1	P1	P2
	Middel	P1	P2	P3
	Laag	P2	P3	P3

Tabel 1.1 - Prioriteitenmatrix

Impact

- Hoog – het betreft meer dan de helft van de eindgebruikers van een applicatie (of grotere impact).
- Middel – het betreft een minderheid van de eindgebruikers van een applicatie.
- Laag – het betreft één of enkele eindgebruikers.

Urgentie

- Hoog – het betreft een kritisch bedrijfsvoeringsproces of de doorgang/voortgang van de bedrijfsvoering dan wel de uitvoering van de publieke taken is/wordt ernstig verhinderd.
- Middel – het betreft een bedrijfsvoeringsproces dat met enige hinder nog wel doorgang vindt.
- Laag – Medewerker(s) kan/kunnen nog werken

Prio	Reactietijd	Hersteltijd	PI	Terugkoppeling	Servicevenster
P1	15 min	2 uur	90%	Ieder uur	ma tm vr 08:00-17:00
P2	1 uur	1 werkdag	90%	Oplostijd overschreden	ma tm vr 08:00-17:00
P3	4 uur	5 werkdagen	90%	Oplostijd overschreden	ma tm vr 08:00-17:00

Tabel 1.2 – Afspraken incidentenbeheer

Reactietijd - Betreft de termijn waarbinnen een (eerste) inhoudelijke reactie op een melding plaatsvindt, inclusief een kennisgeving van welke medewerkers van Opdrachtnemer de melding opgepakt hebben, de gestelde prioriteit en beoogde hersteltijd.

Hersteltijd – Betreft de termijn waarbinnen de dienstverlening is hersteld.

Performance indicator (PI) – Opdrachtnemer dient in 90% van de gevallen te voldoen aan de opgegeven maximale reactie- en hersteltijd, welke per kwartaal worden gemeten en gerapporteerd.

Terugkoppeling – Betreft de frequentie of het moment waarop, ten minste, een inhoudelijke reactie op een melding plaatsvindt.

5.3 Wijzigingsbeheer

Het proces wijzigingsbeheer richt zich op het beheerst (volgens gestandaardiseerde methoden en procedures) uitvoeren van wijzigingen, zodat incidenten ten gevolge van wijzigingen tot een minimum worden beperkt en tegelijkertijd de gewenste snelheid van verandering wordt bereikt.

Opdrachtgever heeft de mogelijkheid om wijzigingsverzoeken (RfC's) in te dienen bij Opdrachtnemer. Per RfC volgt een adequate terugkoppeling van Opdrachtnemer over het besluit om de wijziging wel of niet op te pakken, inclusief onderbouwing en verwachte tijdslijn. Er geldt geen beperking voor wat betreft het aantal ingediende RfC's. Het in behandeling nemen van RfC's is bij de aangeboden tarieven inbegrepen. Indien het gaat om maatwerk op verzoek van Opdrachtgever, dat niet is opgenomen in het betreffende Programma van Eisen, dan zal Opdrachtnemer bij de terugkoppeling ook een opgave



van de kosten op basis van een marktconform tarief en een planning opnemen. De realisatie van een maatwerk RfC start pas na goedkeuring door Opdrachtgever. Nadat de wijziging succesvol in productie is genomen kunnen kosten in rekening worden gebracht.

Reactietijd – Dit betreft de termijn (4 werkdagen) waarbinnen een (eerste) inhoudelijke reactie op een wijzigingsaanvraag plaatsvindt, inclusief een kennisgeving van welke medewerker van Opdrachtnemer de aanvraag opgepakt heeft en een beoogde planning voor de vervolgstappen.

Levertijd conform planning – Dit betreft de afgesproken termijn waarbinnen de wijziging is opgeleverd en in productie is genomen.

Performance indicator (PI) – Opdrachtnemer dient in 90% van de gevallen te voldoen aan de opgegeven maximale reactie- en levertijd, welke per kwartaal worden gemeten en gerapporteerd.

5.4 Problem management

Problem management is het proces gericht op het structureel identificeren, analyseren en oplossen van de onderliggende oorzaken van terugkerende incidenten, om herhaling te voorkomen en de kwaliteit en continuïteit van de Applicatie en bijbehorende dienstverlening te waarborgen.

Terugkerende incidenten worden door Opdrachtnemer geclassificeerd als problem op basis van één of meer van de volgende criteria:

- wanneer eenzelfde type incident zich drie (3) keer of vaker voordoet binnen een periode van zes (6) maanden;
- of als er sprake is van een duidelijke trend (bijv. wekelijks/maandelijks patroon).

Opdrachtnemer registreert elk problem en voert een gestructureerde analyse uit naar de onderliggende oorzaak (root cause analyse). Daarbij wordt, waar relevant, onderscheid gemaakt tussen technische, organisatorische en procesmatige oorzaken. Indien zich een problem voordoet binnen het ICT-landschap van Opdrachtgever dat niet direct is toe te rekenen aan de dienstverlening van Opdrachtnemer, maar daarmee mogelijk samenhang vertoont, verleent Opdrachtnemer binnen redelijke grenzen ondersteuning bij de diagnose en analyse van dit problem. Na analyse levert Opdrachtnemer een verbeterplan op dat tenminste bevat:

- een beschrijving van de oorzaak van het problem;
- de voorgenomen maatregelen om herhaling te voorkomen;
- een concrete planning, inclusief onderzoeksperiode, inzet van mensen en middelen en beoogde resultaten;
- een overzicht van risico's en afhankelijkheden.

De voortgang van het verbeterplan, de uitvoering van de maatregelen en de behaalde resultaten worden periodiek door Opdrachtnemer gerapporteerd aan Opdrachtgever en op verzoek nader toegelicht. Indien een verbeteractie leidt tot een wijziging, dan is het Wijzigingsbeheer van toepassing zoals hierboven beschreven.

Reactietijd – Dit betreft de termijn (4 werkdagen) waarbinnen een (eerste) inhoudelijke reactie na classificatie van het problem plaatsvindt, inclusief een kennisgeving van welke medewerker van Opdrachtnemer het problem in behandeling heeft en een beoogde planning voor de vervolgstappen.

Levertijd conform planning – Opdrachtnemer realiseert de uitvoering van het goedgekeurde verbeterplan conform de overeengekomen planning.

Performance indicator (PI) – Minimaal 90% van de in het verbeterplan opgenomen acties wordt gerealiseerd binnen de afgesproken planning. Afwijkingen van de planning worden tijdig, gemotiveerd en voorafgaand aan de overschrijding gemeld aan Opdrachtgever, inclusief een bijgestelde planning en mitigerende maatregelen.



5.5 Vraag- en adviesproces

Het Vraag- en adviesproces is bedoeld om Opdrachtgever de mogelijkheid te bieden inhoudelijke vragen te stellen en advies te verkrijgen over het gebruik, beheer en de inrichting van de Applicatie en bijbehorende dienstverlening, zonder dat direct een wijziging noodzakelijk is.

- Opdrachtgever kan onbeperkt vragen en adviesverzoeken indienen via het reguliere servicekanaal.
- Het stellen van vragen of het opvragen van advies brengt geen aanvullende kosten met zich mee.
- Vragen kunnen betrekking hebben op functionaliteit, beheer, inrichting, best practices of impact op bedrijfsprocessen.
- Indien een vraag leidt tot een verzoek voor een aanpassing, wordt deze in overleg met Opdrachtgever omgezet in een RfC en valt deze onder het wijzigingsbeheerproces.

Reactietijd - Opdrachtnemer geeft binnen 4 werkdagen een inhoudelijke reactie op vragen of adviesverzoeken. De reactie bevat, indien van toepassing:

- Een toelichting of antwoord.
- Een inschatting of het verzoek leidt tot een wijziging (RfC).
- Verwijzingen naar documentatie of instructies.

Levertijd – Betreft de termijn waarbinnen een inhoudelijke reactie komt op vragen of verzoeken tot advies.

Performance indicator (PI) – Opdrachtnemer dient in 90% van de gevallen te voldoen aan de opgegeven maximale reactie- en levertijd, welke per kwartaal worden gemeten en gerapporteerd.

Vragen met hoge urgentie bijvoorbeeld over de continuïteit of veiligheid van de Applicatie en bijbehorende dienstverlening worden door Opdrachtgever in lijn met een prioriteit 1 melding telefonisch doorgegeven aan de Helpdesk van Opdrachtnemer. Opdrachtnemer zorgt ervoor dat deze vragen uiterlijk dezelfde werkdag worden voorgelegd aan de daarvoor aangewezen specialistische kennishouder, die verantwoordelijk is voor het bepalen van de benodigde vervolgstappen, het bewaken van de voortgang, het verzorgen van de terugkoppeling aan Opdrachtgever en de uiteindelijke beantwoording van de vraag.

5.6 Klachtenmanagement

Opdrachtgever en Opdrachtnemer komen een klachtenregeling overeen, gedetailleerd uitgewerkt in het DAP, waarvoor het volgende geldt:

- Opdrachtnemer reageert binnen twee werkdagen op klachten over de dienstverlening.
- Binnen twee werkdagen na de melding komt Opdrachtnemer tot een voorstel voor de afhandeling van de klacht.
- De klacht kan pas afgesloten worden na goedkeuring van Opdrachtgever.

De escalatie van een klacht wordt uitgevoerd conform de escalatieregeling in het DAP. In de periodieke rapportage is een aparte paragraaf voor klachtrapportage opgenomen.



6. Softwareonderhoud en Releasebeheer

Dit hoofdstuk beschrijft de afspraken ten aanzien van softwareonderhoud, releases, Upgrades, Updates en de bijbehorende serviceprocessen die van toepassing zijn op de Applicatie en bijbehorende dienstverlening die Opdrachtnemer aan Opdrachtgever levert.

6.1 Continuïteit van functionaliteit

1. Nieuwe releases, inclusief Updates en Upgrades, waarborgen te allen tijde dat de functionaliteit zoals beschreven in de Aanbestedingsdocumenten behouden blijft.
2. Nieuwe releases mogen niet leiden tot verminderde functionaliteit, het vervallen van functionaliteit of het niet meer kunnen voldoen aan de eerder gestelde eisen en wensen zoals opgenomen in de aanbesteding.
3. Wanneer functionaliteit wordt gewijzigd, uitgebreid of vervangen door gelijkwaardige of betere functionaliteit, wordt dit tijdig en duidelijk aan Opdrachtgever gemeld.

6.2 Uitfasering en doorontwikkeling

1. Indien de geleverde Applicatie en bijbehorende dienstverlening wordt uitgefaseerd of doorontwikkeld waardoor de overeengekomen functionaliteit overgaat in een opvolgende productlijn, geldt dat Opdrachtgever gedurende de looptijd van de Overeenkomst:
 - o onverminderd wordt voorzien in de overeengekomen functionaliteit, en
 - o geen additionele kosten of transitiekosten in rekening worden gebracht.
2. De netto overeengekomen prijs voor de Applicatie en bijbehorende dienstverlening blijft ongewijzigd tijdens deze overgang.

6.3 Releasekalender en aankondigingen

1. Opdrachtnemer publiceert minimaal jaarlijks een releasekalender waarin geplande releases, onderhoudsmomenten en belangrijke productwijzigingen worden aangekondigd.
2. Wijzigingen in de releasekalender worden tijdig gecommuniceerd aan Opdrachtgever.
3. Een nieuwe release wordt altijd minimaal 2 werkdagen van tevoren aangekondigd.

6.4 Releasenotes

1. Elke release wordt standaard voorzien van Nederlandstalige releasenotes.
2. De releasenotes worden uiterlijk op het moment van oplevering beschikbaar gesteld aan Opdrachtgever.
3. De releasenotes bevatten ten minste:
 - o Een beschrijving van gewijzigde, vervallen en nieuwe functionaliteit.
 - o Instructiemateriaal voor beheerders en/of gebruikers.
 - o Informatie over mogelijke impact op koppelingen en integraties.
 - o Informatie over mogelijke impact op certificaten.
 - o Bekende beperkingen of bijzonderheden.

6.5 Patch- en kwetsbaarhedenbeheer

Opdrachtnemer beschikt over een gedocumenteerd en aantoonbaar patch- en updatebeleid voor de Applicatie, de mobiele app en alle door Opdrachtnemer beheerde componenten die onderdeel uitmaken van de dienstverlening. Dit beleid bevat ten minste de classificatiecriteria, responstijden, hersteltermijnen en procedures voor het testen en uitrollen van patches en updates. Opdrachtnemer stelt dit beleid op verzoek beschikbaar aan Opdrachtgever.



Opdrachtnemer monitort actief op beveiligingskwetsbaarheden en classificeert deze op basis van risico. Daarbij wordt ten minste rekening gehouden met de ernst en impact van de kwetsbaarheid, de kans op misbruik, de beschikbaarheid van een exploit en de blootstelling van de getroffen component. Voor de afhandeling worden beveiligingskwetsbaarheden gekoppeld aan de prioriteiten zoals opgenomen in paragraaf 5.2.

De reactie- en hersteltijd vangen aan zodra de kwetsbaarheid door Opdrachtnemer is vastgesteld of redelijkerwijs had behoren te zijn vastgesteld.

Kritieke kwetsbaarheden worden onverwijld in behandeling genomen.

Indien een kwetsbaarheid niet binnen de toepasselijke hersteltijd definitief kan worden verholpen, treft Opdrachtnemer binnen die termijn passende mitigerende maatregelen. Opdrachtnemer informeert Opdrachtgever over de risico's, de getroffen maatregelen en de planning voor definitief herstel.

Opdrachtnemer informeert Opdrachtgever onverwijld over P1-kwetsbaarheden en verstrekt daarbij ten minste informatie over:

- de aard en impact van de kwetsbaarheid;
- de getroffen componenten;
- de getroffen of voorgenomen maatregelen;
- het verwachte moment van definitief herstel.

In de periodieke rapportage wordt ten minste gerapporteerd over:

- geconstateerde beveiligingskwetsbaarheden;
- de toegepaste classificatie;
- gerealiseerde hersteltermijnen;
- getroffen maatregelen;
- eventuele overschrijdingen;
- openstaande risico's en verbetermaatregelen.

Indien een beveiligingskwetsbaarheid leidt tot een incident, wordt deze tevens afgehandeld conform paragraaf 5.2 Incidentenbeheer.

6.6 Beveiligings- en compliancerapportage

Opdrachtnemer verstrekt ten minste halfjaarlijks en daarnaast op verzoek van Opdrachtgever een rapportage over de wijze waarop de veiligheid, integriteit en privacy van de Applicatie, de mobiele app en de bijbehorende dienstverlening worden gewaarborgd.

De rapportage bevat ten minste:

- de actuele status van de ISO 27001-certificering en de Verklaring van Toepasselijkheid;
- de wijze waarop wordt voldaan aan de toepasselijke maatregelen uit de BIO2;
- relevante afwijkingen, auditbevindingen, restrisico's en verbetermaatregelen;
- relevante ontwikkelingen op het gebied van informatiebeveiliging, privacy, technologie en wet- en regelgeving en de naar aanleiding daarvan getroffen maatregelen;
- aanvullende maatregelen die specifiek voor Opdrachtgever zijn getroffen;
- relevante wijzigingen in de beveiligingsorganisatie, hostingomgeving, gegevensverwerking of inzet van subverwerkers;
- de status van identiteits- en toegangsbeheer, waaronder Microsoft Entra ID, MFA, Single Sign On en toepassing van het least-privilegebeginsel;
- de status van de beveiliging van de mobiele app en mobiele apparatuur;
- de status van privacy by design, privacy by default, encryptie en verwerking van persoonsgegevens binnen de Europese Economische Ruimte;



- de status van logging en audittrail, waaronder integriteit, beschikbaarheid en bewaartermijnen;
- relevante beveiligingsincidenten en de getroffen maatregelen;
- relevante audits, penetratietests, kwetsbaarheidsscans en de opvolging van bevindingen.

Per relevante bevinding of verbetermaatregel bevat de rapportage ten minste:

- de risico-inschatting;
- de getroffen of geplande maatregel;
- de planning en status;
- het restrisico.

Opdrachtgever heeft het recht tussentijds aanvullende informatie en bewijsstukken op te vragen om de naleving en effectiviteit van de maatregelen te controleren. Opdrachtnemer verstrekt deze binnen een redelijke termijn.



7. Back-up & Herstel

7.1 Back-upvoorzieningen

Opdrachtnemer verzorgt volledige en betrouwbare back-ups van alle data, configuraties en systeeminstellingen die onderdeel uitmaken van de Applicatie en bijbehorende dienstverlening. Back-upprocessen worden continu gemonitord. Fouten worden automatisch gedetecteerd en door Opdrachtnemer proactief gecorrigeerd.

- De volledige herstelprocedure is gedocumenteerd, actueel en inzichtelijk voor Opdrachtgever.
- Restore-verzoeken worden door Opdrachtnemer afgehandeld conform deze SLA en tijdig gecommuniceerd.

7.2 Testen en validatie

- Opdrachtnemer voert ieder kwartaal een volledige testrestore uit.
- Van iedere test wordt een schriftelijk verslag opgeleverd met resultaten, bevindingen en eventuele verbetermaatregelen.

7.3 Rapportage en inzicht

- Opdrachtnemer rapporteert periodiek over back-upstatus.
- Opdrachtgever heeft inzicht in de back-upstatus en kan restores aanvragen via de overeengekomen servicekanalen.

