

<Plaats hier logo opdrachtnemer>

STANDAARD SERVICE LEVEL AGREEMENT SAAS-APPLICATIES

<NAAM OPDRACHTNEMER>

-

PROVINCIE NOORD-BRABANT

MET BETREKKING TOT **<NAAM SAAS DIENST>**

Publicatiedatum 16 juli 2026

Versie 3.01

Status Definitief

Colofon

Naam document

Standaard Service Level Agreement SaaS-applicaties

Datum

16 juli 2026

I Bijlagen

- Bijlage A: PNB informatiebeveiliging

III Disclaimer

Gebruik

Dit document bevat een standaard SLA voor SaaS-applicaties. Het definitieve SLA dat wordt overeengekomen met de SaaS-leverancier is afhankelijk van diverse factoren en kan afwijken van dit standaard SLA. Er is geen “one size fits all” oplossing; voor bedrijfskritische software wordt bijvoorbeeld een uitgebreider SLA opgesteld dan voor standaardapplicaties.

Indien een leverancier een eigen SLA aanbiedt kan dit worden getoetst aan het standaard SLA. Indien de leverancier geen eigen SLA heeft kan dit standaard SLA als input worden gebruikt.

Rechten en vrijwaring

Provincie Noord-Brabant (PNB) kan geen aansprakelijkheid aanvaarden voor eventueel in deze uitgave voorkomende onjuistheden, onvolledigheden of nalatigheden. Provincie Noord-Brabant aanvaardt ook geen aansprakelijkheid voor enig gebruik van voorliggende uitgave of schade ontstaan door de inhoud van de uitgave of door de toepassing ervan.

IV Ondertekening

Op **<Datum>** getekend door

<Naam, functie>

Provincie Noord-Brabant

<Naam, functie>

<Opdrachtnemer>

Inhoudsopgave

COLOFON	3
1. DOEL VAN HET SLA.....	6
2. DIENSTVERLENING, PROCESSEN.....	7
2.1 SUPPORT EN ONDERHOUD	7
2.2 SERVICEDESK.....	7
2.3 INCIDENT MANAGEMENT	7
2.4 PROBLEM MANAGEMENT	9
2.5 AVAILABILITY MANAGEMENT	10
2.6 PRESTATIE OPLOSSING	10
2.7 CHANGE MANAGEMENT	10
2.8 ASSET EN CONFIGURATIE MANAGEMENT	11
2.9 PATCH- EN RELEASEMANAGEMENT.....	12
2.10 INFORMATIEBEVEILIGING	13
2.11 DATABEHEER, BACK-UP EN RESTORE SERVICES	13
2.12 PRIVACY EN GEGEVENSBESCHERMING- MELDPlicht	14
2.13 SERVICE LEVEL RAPPORTAGE	14
2.14 DOCUMENTATIE EN EXIT	14
3. COMMUNICATIE PROVINCIE NOORD-BRABANT EN OPDRACHTNEMER	15
3.1. DIENSTRAPPORTAGES	16
3.2. KLACHTEN.....	16
3.3. CONTACTGEGEVENS PROVINCIE NOORD-BRABANT	16
4. DEFINITIES.....	17
BIJLAGE A: PNB INFORMATIEBEVEILIGING	19

1. Doel van het SLA

Doel van het SLA is het op een heldere en eenduidige wijze beschrijven van wederzijdse, kwalitatieve en kwantitatieve, verwachtingen en verantwoordelijkheden tussen de provincie en opdrachtnemer over het minimaal te realiseren dienstenniveau en de rapportage daarover. Op basis van deze normstelling kan de kwaliteit en uitvoering van de dienstverlening worden gemonitord en indien noodzakelijk worden verbeterd zodat de 'goede' relatie/samenwerking tussen beide partijen optimaal wordt gehouden. Opdrachtnemer voorziet in de beheersdiensten, in overeenstemming met de beschreven dienstenniveaus en overige afspraken. De diensten hebben betrekking op instandhouding van de applicatie, systemen of diensten en de aanpassingen hieraan ten gevolge van wijzigende omstandigheden en behoeften binnen de provincie.

De provincie beoogt door de relatie met de opdrachtnemer het volgende te realiseren:

- Het leveren van (toegevoegde) waarde aan de provinciale organisatie, interne belanghebbenden en de maatschappelijke taken van de provincie;
- Het voldoen aan de contractdoelstellingen;
- Het waarborgen van de continuïteit van de bedrijfsprocessen;
- Het borgen van de betrouwbaarheid, integriteit en vertrouwelijkheid van de kennis in de vorm van data die wordt verwerkt in de processen, systemen en geboden dienstverlening van en voor de provincie.

Normatief kader Informatiebeveiliging

De eisen in dit SLA zijn gebaseerd op het normenkader voor informatiebeveiliging en data privacy dat van toepassing is op de Provincie Noord-Brabant als overheidsorganisatie. Zie Bijlage A

Opdrachtnemer committeert zich aan naleving van bovengenoemd normenkader voor zover van toepassing op de geleverde SaaS-dienst.

Wijzigingsbeheer

Wijzigingen op de in het SLA vastgelegde regelingen, prestaties en rapportages kunnen zowel een incidenteel als een blijvend (structureel) karakter hebben:

- Incidenteel: Bij deze wijzigingen gaat het om een eenmalige, kortstondige afwijking van de inhoud van het SLA, waarbij het SLA als zodanig niet wijzigt.
- Structureel: Een wijziging is structureel wanneer ten gevolge van deze wijziging de inhoud van het SLA verandert.

Een tussentijdse aanpassing van het SLA verkrijgt rechtskracht na overeenstemming en ondertekening door de daartoe bevoegde vertegenwoordigers van beide partijen.

Uitbreiding en inkrimping van (de scope van de) dienstverlening geschiedt in overleg en wordt gecoördineerd door de Contractmanager van de provincie Noord-Brabant. Deze wijzigingen worden schriftelijk vastgelegd in een Addendum op de Overeenkomst, welke slechts na ondertekening door beide partijen van kracht wordt.

Delen SLA

Opdrachtgever is gerechtigd deze SLA te delen met andere ICT-leveranciers van de provincie indien deze dienstverlening onderdeel uitmaakt van een totale keten aan ICT-diensten. Dit om de totale continuïteit van deze keten ICT-dienst te garanderen. In dat geval informeert Opdrachtgever vooraf Opdrachtnemer hierover. Opdrachtgever zal enkel service afspraken delen en geen financiële afspraken delen.

2. Dienstverlening, processen

Provincie Noord-Brabant maakt gebruik van het ITIL-framework voor service management. Processen, dienstverleningstijden, prioriteitsniveaus etc. zijn dan ook in die termen beschreven. Het gaat in het SLA om afspraken over de dienstverlening. Zie hoofdstuk 3 voor algemene bepalingen met betrekking tot communicatie, rapportages, klachtafhandeling e.d. De specifieke procedures met betrekking tot de werkprocessen kunnen worden ondergebracht in een Dossier met Afspraken en Procedures (DAP).

2.1 Support en onderhoud

Uitgangspunt is dat de SaaS-toepassing 24/7 beschikbaar is en dat onderhoud in de vorm van updates (releases en patches) of upgrades geen verstoring geeft in de dienstverlening.

Onderhoud dient plaats te vinden binnen een onderhoudswindow:

- op maandag tot en met vrijdag van 22:00 uur tot 07:00 uur de volgende ochtend.
- op zaterdag en zondag en feestdagen, in alle gevallen mits er een goedgekeurde change is.

Opdrachtnemer kondigt onderhoud aan de aangeboden oplossing minimaal 10 werkdagen van tevoren aan middels een nog vast te stellen procedure (deze kan worden uitgewerkt in een DAP).

2.2 Servicedesk

- De servicedesk van de Opdrachtnemer is het single point of contact voor Provincie Noord-Brabant m.b.t. service aanvragen en de afhandeling daarvan, ook wanneer Opdrachtnemer voor bepaalde dienstverlening werkt met onderaannemers.
- De servicedesk communiceert met Provincie Noord-Brabant in de Nederlandse taal en is gevestigd in Nederland.
- De servicedesk van Opdrachtnemer is telefonisch beschikbaar op maandag t/m donderdag van 08:00 tot 16:30 uur en op vrijdag van 08:00 tot 16:00 uur. In geval van telefonische communicatie dient de servicedesk bereikbaar te zijn op telefoonnummers tegen binnenlands- of gratis tarief (geen internationale nummers, geen betaalnummers).
- De servicedesk van Opdrachtnemer is 24/7 beschikbaar middels een webportaal of soortgelijke applicatie, waarin geselecteerde medewerkers van Opdrachtgever hun verzoeken en incidenten kunnen melden en de voortgang van openstaande verzoeken/incidenten/changes kunnen zien.

2.3 Incident Management

Opdrachtnemer maakt onderscheid in 3 verschillende prioriteringen voor incidenten. In onderstaande tabel zijn deze prioriteiten uitgewerkt met vermelding van de geldende servicetijden en KPI-afspraken. De meetperiode voor de opgestelde KPI's betreft één kalendermaand. Opdrachtnemer garandeert maandelijks inzicht te zullen geven in incident statussen en prioritering, problemen, serviceverzoeken en standaard changes.

Opdrachtnemer stelt Provincie Noord-Brabant in de gelegenheid om tussentijds prioritering en status van incidenten en ondersteuningsaanvragen te kunnen volgen via het webportaal en/of telefonisch.

Prioriteit	Scope	Maximale Reactietijd	Maximale Hersteltijd	Percentage Gehaald (KPI)
Prioriteit 1	• De SaaS-applicatie is volledig onbereikbaar. • Kritieke processen liggen stil. • Beveiligingsincident zoals een datalek, ongeautoriseerde toegang of kwetsbaarheden CVSS ≥ 9.0 • Data-integriteitsproblemen zoals verlies of corruptie.	15 minuten	4 klokuren	98% van de Incidenten binnen de norm opgelost

Prioriteit 2	- Kernfunctionaliteit werkt niet of is beperkt beschikbaar. - Prestatieproblemen zoals trage respons of veel time-outs. - API's of integraties met bedrijfskritische systemen werken niet. - Kwetsbaarheid met CVSS 7.0–8.9.	30 minuten	8 klokuren	90% van de Incidenten binnen de norm opgelost
Prioriteit 3	- Niet-kritieke functionaliteit werkt niet naar behoren. - Kleine bugs of cosmetische fouten zonder functionele impact.	4 klokuren	2 werkdagen	90% van de Incidenten binnen de norm opgelost
Prioriteit 4	- Kleine verstoringen zonder impact op productiviteit - Informatieaanvraag	1 werkdag	10 werkdagen	90% van de Incidenten binnen de norm opgelost

Afspraken inzake uitvoering incidentmanagement proces:

- Zodra het Incident verholpen is (structureel of met een tijdelijke oplossing), dient de Opdrachtnemer de Provincie Noord-Brabant direct te informeren.
- Bij de prioriteitstelling van een Incident wordt tevens gekeken naar impact van het Incident. Dit betekent dat Incidenten bij Provinciale Staten, Gedeputeerde Staten en de Commissaris van de Koning een hogere prioriteit kunnen krijgen.
- De meetperiode voor de opgestelde KPI's betreft één kalendermaand.
- Opdrachtnemer bewaakt proactief de dienst en meldt kritieke verstoringen conform overeengekomen reactietijd bij de functioneel beheerder.
- De reactietijd is de periode tussen de melding van een incident en de eerste daadwerkelijke (menselijke) reactie. Deze reactie bevestigt dat het incident bekend is en dat de opdrachtnemer ermee aan de slag gaat.
- De hersteltijd is de periode tussen de melding van een incident en het gereed melden van het incident na overleg met de aanmelder van het incident.
- In geval de melding een Prioriteit 1 incident betreft, dan zal de melding altijd gevolgd worden door een telefonisch overleg tussen de functioneel beheerder van opdrachtgever en de service-coördinator van opdrachtnemer.

Prioriteitenbepalingsmatrix

Impact/ urgentie	Hoog	Midden	Laag
Hoog	Prioriteit 1	Prioriteit 1	Prioriteit 2
Midden	Prioriteit 1	Prioriteit 2	Prioriteit 3
Laag	Prioriteit 2	Prioriteit 3	Prioriteit 4

Hoe werkt deze matrix?

- Impact = Hoeveel gebruikers en processen worden beïnvloed?
 - Hoog = Volledige applicatie-uitval of bedrijfskritische processen geraakt.
 - Midden = Grote verstoring, maar workaround mogelijk.
 - Laag = Kleine verstoring zonder serieuze impact.
- Urgentie = Hoe snel moet dit worden opgelost?
 - Hoog = Onmiddellijke actie vereist (bijv. datalek, volledige onbeschikbaarheid).
 - Midden = Probleem heeft aanzienlijke impact, maar directe oplossing is niet noodzakelijk.
 - Laag = Kan zonder directe gevolgen later worden opgepakt.

2.4 Problem Management

Het doel van Problem Management is het minimaliseren van de impact van incidenten door de oorzaken ervan te achterhalen, herhaling te voorkomen en de algehele beschikbaarheid van de dienstverlening te verhogen.

Classificatie: De classificatie van het Problem gebeurt door de Opdrachtgever en is afhankelijk van:

- Ernst van het Problem;
- Urgentie vanuit het perspectief van de opdrachtgever;
- Beschikbaarheid van een tijdelijke oplossing (workaround);
- Wetgeving
- Imagoschade
- Complexiteit van een aangeboden workaround

Prioriteit	Status melding	Doorlooptijd achterhalen oorzaak	Doorlooptijd structurele oplossing	Percentage Gehaald (KPI)
Hoog	Dagelijks	3 werkdagen	2 werkweken	95% van de problems binnen de norm doorlooptijd structurele oplossing opgelost
Midden	Wekelijks	2 werkweken	4 werkweken	90% van de problems binnen de norm doorlooptijd structurele oplossing opgelost
Laag	Wekelijks	4 werkweken	8 werkweken	90% van de problems binnen de norm doorlooptijd structurele oplossing opgelost

Afspraken inzake uitvoering problem management proces:

- De meetperiode voor de opgestelde KPI's betreft één kalenderkwartaal.
- In geval van een hoogste Prioriteit incident welke verder als Problem wordt behandeld dient binnen 5 werkdagen een Root Cause Analyse (RCA) rapportage voor worden opgesteld.
- Verbetervoorstellen dienen in een Service Improvement Plan (SIP) te worden opgenomen en middels een problem te worden geïmplementeerd.
- Afspraken over het melden en afhandelen van problemen kunnen worden opgenomen in een DAP.

Onderstaande matrix bepaalt of een probleem "Hoog", "Midden" of "Laag" prioriteit krijgt:

Impact/urgentie	Hoog	Midden	Laag
Hoog	Prioriteit 1	Prioriteit 1	Prioriteit 2
Midden	Prioriteit 1	Prioriteit 2	Prioriteit 3
Laag	Prioriteit 2	Prioriteit 3	Prioriteit 3

Toelichting:

- Impact = hoe groot de gevolgen van het probleem zijn voor de organisatie en gebruikers.
 - Hoog: Repeterende incidenten of "Workarounds" raken kritieke diensten of $\geq 50\%$ van de gebruikers.
 - Midden: Repeterende problemen beïnvloeden een belangrijke, maar niet bedrijfskritische dienst.
 - Laag: Enkel een paar gebruikers of niet-kritieke functionaliteit zijn geraakt
- Urgentie = hoe snel er een structurele oplossing nodig is.
 - Hoog: Geen werkende workaround, of workaround veroorzaakt te hoge operationele kosten.
 - Midden: Workaround is afdoende voor de korte termijn, maar extra lasten voor de operatie.
 - Laag: Workaround is goed genoeg en direct ingrijpen niet nodig.

2.5 Availability Management

Availability Management is erop gericht om de beschikbaarheid van de dienstverlening gedurende de looptijd van het contract te kunnen waarborgen. Onder Availability Management wordt verstaan:

- Schaalbaarheid van de geboden dienst: Opdrachtnemer garandeert dat er geen limieten bestaan ten aanzien van de opslagcapaciteit of het aantal gebruikersprofielen binnen de geboden dienst. M.a.w. is de dienst schaalbaar en zijn er ruime mogelijkheden t.a.v. groei en/of krimp.
- Performance gelijktijdig gebruik: Opdrachtnemer garandeert een optimale werking van het systeem bij een gelijktijdig gebruik van alle gebruikers/x-aantal gebruikers
- Uitwijkmogelijkheid van de dienst: De aangeboden dienst is dusdanig ingericht dat bij calamiteiten in het datacenter de dienst naadloos kan worden aangeboden/gecontinueerd vanaf een tweede of derde locatie

Opdrachtnemer garandeert onderstaande beschikbaarheid van de onderstaande diensten:

Tijdvak	Minimale beschikbaarheid	Meetperiode
Gedurende Servicewindow (07:00-22:00 uur)	Minimale beschikbaarheid SaaS-dienst 99,8% Minimale beschikbaarheid API's en integraties 99,8%	Per kalendermaand
Gedurende Onderhoudswindow	Minimale beschikbaarheid SaaS-dienst 99,5% Minimale beschikbaarheid API's en integraties 99,5%	Per kalendermaand

Business Continuïteit en Disaster Recovery

Opdrachtnemer committeert zich aan de volgende continuïteitseisen:

Kenmerk	Eis	Meetwijze
Recovery Time Objective (RTO)	≤ 4 uur voor Prioriteit 1	Per incident
Recovery Point Objective (RPO)	≤ 24 uur (maximaal dataverlies)	Per incident
DR-test	Minimaal jaarlijks een volledige DR-test	Testrapport beschikbaar voor opdrachtgever
Geografische redundantie	Minimaal 2 fysiek gescheiden datacenters binnen EU/EER	Architectuurdocumentatie

2.6 Prestatie oplossing

Prestatiecriterium	Maximale responstijd	KPI
Openen volledige (web)applicatie	≤ 10 sec	≥ 95%
API-response tijd	≤ 1 sec	≥ 95%
Opslaan registratie/aanpassingen in systeem	≤ 5 sec	≥ 95%
Keystroke registratie	≤ 200 ms	≥ 95%
Bulkacties verwerken tbv rapportages (>10.000 records)	≤ 60 sec	≥ 95%

- De meetperiode voor de opgestelde KPI's betreft één kalendermaand.

2.7 Change Management

Change Management moet ervoor zorgdragen dat gewenste aanpassingen aan geleverde oplossing (software, omgeving) / dienstverlening een gestructureerde, overzichtelijke en gecontroleerde manier een weg vinden naar het productiesysteem.

PNB maakt onderscheid tussen service requests, standaard-, niet-standaard- en speedwijzigingen.

- Service Request: Een lijst met overeengekomen Service Request kunnen in een DAP worden vastgelegd.
- Standaard wijzigingen: zijn onderdeel van de standaard dienstverlening en worden daarom niet apart door opdrachtnemer in rekening gebracht.

- Niet standaard wijzigingen: voor niet-standaard wijzigingen zullen Opdrachtnemer en Opdrachtgever een Request for Change proces doorlopen.
- Spoed wijzigingen: Een spoedwijziging (Emergency Change) is een wijziging die zo snel mogelijk moet worden geïmplementeerd om een onverwacht prioriteit 1 incident op te lossen, een grote verstoring van de dienstverlening te voorkomen of een beveiligingsrisico te mitigeren.

Type wijziging	Norm	Tijdigheid	Juistheid	Volledigheid
Service request	Reactietijd: 1 werkdag Doorlooptijd: per Service Request vastgelegd in DAP		100% in één keer correct doorgevoerd	• ≥ 90% binnen de norm afgesloten • 100% binnen 2 * de norm afgesloten
Standaard wijziging	Reactietijd: 1 werkdag Doorlooptijd: per wijziging vastgelegd in DAP		100% in één keer correct doorgevoerd.	
Niet standaard wijziging	Reactietijd: 2 werkdagen Doorlooptijd: conform geplande datum, na akkoord van CAB Indien van toepassing: een offerte binnen 5 Werkdagen	Minimaal 5 Werkdagen voor het beoogde Change-window aangekondigd bij het CAB	• In maximaal 2 keer goedgekeurd door het CAB (tijdig, volledig, juist aangeleverd) • 90% in één keer correct doorgevoerd, in het geplande Change-window	
Spoed wijziging	Reactietijd: Zsm Doorlooptijd: Zie prio 1 incident management.			

Afspraken inzake uitvoering Changemanagement proces:

- De meetperiode voor de opgestelde KPI's betreft één kalendermaand.
- Een wijziging met impact op de Opdrachtgever, dient minimaal 10 werkdagen voorafgaand aan het doorvoeren van de wijziging te zijn gemeld.
- Opdrachtnemer voorziet in een roll-back plan bij een niet-standaard wijziging.
- Procedures in relatie tot het Change Proces kunnen worden vastgelegd in een DAP.
- In de DAP is vastgelegd welke wijzigingen als standaard wijzigingen zijn gedefinieerd en welke doorlooptijden ten behoeve van uitvoer zijn voorzien

2.8 Asset en Configuratie management

De doelstelling van configuratiebeheer is het beschikbaar stellen van informatie over applicatieobjecten waarvoor opdrachtnemer verantwoordelijk is. Deze informatie dient ter ondersteuning van andere applicatie georiënteerde processen (Release management, Problem management) waarbij de exacte samenstelling en identificatie van de applicatieobjecten relevant is.

Deze afspraken zijn van toepassing op het beheer van assets en configuratie-items binnen de dienstverlening door de Opdrachtnemer. Denk hierbij aan licenties, API-koppelingen en specifieke configuraties.

Bij SaaS-dienstverlening beheert de opdrachtnemer de onderliggende infrastructuur. De Provincie Noord-Brabant registreert de SaaS-applicatie als configuratie-item (CI) in de eigen CMDB. De opdrachtnemer is verantwoordelijk voor het tijdig aanleveren van configuratie-informatie die de opdrachtgever nodig heeft voor het eigen CMDB.

Informatieverstrekking door opdrachtnemer:

Informatie-element	Omschrijving	Frequentie/norm
Applicatieversie	Actuele versienummers van de SaaS-applicatie	Uiterlijk 2 werkdagen vóór release
API-specificaties	Actuele API-documentatie en endpoints	Bij wijziging, uiterlijk 5 werkdagen vooraf
Integratiedetails	Koppelingen met PNB-systemen, protocollen, authenticatie	Uiterlijk 30 dagen vóór wijziging
Licentie-informatie	Actueel aantal licenties, type, looptijd	Kwartaalrapportage
Architectuuroverzicht	Logische architectuur, datastromen, locaties	Jaarlijks en bij significante wijzigingen

- De meetperiode voor de opgestelde KPI's betreft één kalenderkwartaal.

2.9 Patch- en Releasemanagement

2.9.1 Releasemanagement

Onder releasemanagement wordt verstaan het coördineren, reguleren en bewaken van de implementatie van een nieuwe versie van de aangeboden oplossing. Releasemanagement is onderdeel van de overeengekomen dienstverlening. Opdrachtnemer heeft een methodiek voor het beoordelen, prioriteren en implementeren van nieuwe gewenste functionaliteit/verbeteringen in de applicatie / SaaS dienst. Opdrachtnemer brengt jaarlijks minimaal één release uit waarin bovenstaande verbeteringen zijn opgenomen.

- Opdrachtnemer zal de coördinatie voeren over de gehele release cyclus.
- Opdrachtnemer informeert Opdrachtgever minimaal 10 werkdagen voor het uitvoeren van een nieuwe release per email. Hiervan kan afgeweken worden indien er security risico's kunnen optreden.
- Naast de resultaatverplichting voor een geaccepteerde nieuwe release, verzorgt de opdrachtnemer de coördinatie over de gehele release cyclus, beginnend vanaf het moment dat een verzoek om een wijziging is aangemeld tot en met het moment dat de nieuwe release operationeel is gebracht. Opdrachtnemer heeft daarbij een initiërende, organiserende en signalerende rol.
- Opdrachtnemer voert releasemanagement uit waardoor de SaaS dienst steeds veilig is, aan wettelijke eisen voldoet en op versie N of N-1 is (N-1 alleen na voorafgaande toestemming van provincie Noord-Brabant). De kosten hiervoor maken onderdeel uit van de overeengekomen dienstverlening en worden niet separaat doorbelast.

2.9.2 Security Patches

Security patches volgen een risico gebaseerde benadering op basis van CVSS-score en worden altijd geïmplementeerd ongeacht het releaseproces.

Opdrachtnemer monitort actief op bekende kwetsbaarheden in de SaaS-dienst en onderliggende componenten. De volgende hersteltermijnen zijn van toepassing, conform de NCSC VM Toolbox v1.1:

CVSS-score	Classificatie	Maximale implementatietijd	KPI
9.0 – 10.0	Critical	48 uur (noodpatch)	100%
7.0 – 8.9	High	1 werkweek	98%
4.0 – 6.9	Medium	4 werkweken	95%
0.1 – 3.9	Low	Volgende reguliere release	90%

- Bij actief geëxploiteerde kwetsbaarheden (opgenomen in CISA KEV Catalogue of NCSC-waarschuwing) geldt ongeacht CVSS-score de Critical-termijn van 48 uur.
- Opdrachtnemer meldt geïdentificeerde kwetsbaarheden met CVSS ≥ 7.0 binnen 24 uur aan de Security Officer van opdrachtgever, inclusief impactanalyse en verwachte implementatiedatum.
- Het verkort aankondigingsregime voor noodpatches (Critical/High) wijkt af van de standaard 10 werkdagen: opdrachtnemer informeert opdrachtgever zo spoedig mogelijk, maar de patch mag niet worden vertraagd door het aankondigingsproces.

2.9.3 Overzicht per type wijziging

Type wijziging	Ondersteund binnen SLA?	Extra kosten?	Change-proces PNB vereist?
Patch	Ja	Nee	Nee
Security patch	Ja	Nee	Ja, achteraf
Release	Ja	Nee	Ja
Upgrade	Ja	Conform nadere afspraak	Ja
Specifieke klantwijziging	Nee	Ja (meerwerk)	Ja
Aangepaste configuratie	Nee	Ja (meerwerk)	Ja

2.10 Informatiebeveiliging

De opdrachtnemer waarborgt informatiebeveiliging als integraal onderdeel van de SaaS-dienstverlening conform de wet- en regelgeving en het normenkader dat van toepassing is op de Provincie Noord-Brabant. De eisen in deze paragraaf zijn afgeleid van BIO2 v1.3, ISO 27002:2022 en NIS2.

2.10.1 Beveiligingsincidenten en meldplicht

Service Level	Omschrijving	Norm/KPI	Meetfrequentie
Detectie van beveiligingsincidenten	Leverancier monitort proactief beveiligingsincidenten binnen de SaaS-dienst.	95% van incidenten met impact binnen 1 uur na constatering.	Maandelijks rapporteren van incidentoverzicht.
Meldplicht incidenten	Security incidenten met impact op vertrouwelijkheid, integriteit of beschikbaarheid worden binnen overeengekomen tijd gemeld.	Melding binnen 4 uur na constatering aan de Security Officer van de opdrachtgever.	Per incident gemonitord.
NIS2/Cbw-meldplicht	Opdrachtnemer stelt opdrachtgever in staat om binnen 24 uur een vroege waarschuwing en binnen 72 uur een formele melding te doen aan het CSIRT.	Volledige incidentinformatie binnen 4 uur beschikbaar voor opdrachtgever	Per incident
Forensische ondersteuning	Bij een beveiligingsincident levert opdrachtnemer logbestanden en forensische gegevens aan opdrachtgever.	Binnen 24 uur na verzoek	Per incident

- De meetperiode voor de opgestelde KPI's betreft één kalendermaand

2.10.2 Logging en monitoring: aanlevering leverancier

Opdrachtnemer biedt de mogelijkheid om bovengenoemde logdata geautomatiseerd aan te leveren aan het SIEM van de opdrachtgever, zodat de opdrachtgever zelf kan correleren, detecteren en monitoren over de gehele ICT-keten.

Kenmerk	Eis	Norm
Latency	De vertraging tussen het optreden van een gebeurtenis en de beschikbaarheid in het SIEM van de opdrachtgever is maximaal 5 minuten (near-realtime).	≤ 5 minuten
Beschikbaarheid	De log-aanlevering heeft dezelfde beschikbaarheidsnorm als de SaaS-dienst zelf (99,8% tijdens servicewindow).	99,8%
Wijzigingsbeheer	Opdrachtnemer informeert de opdrachtgever minimaal 10 werkdagen vooraf bij wijzigingen in logformaat, beschikbare logtypen of API-specificaties.	10 werkdagen vooraf
Forensic analyse	Logbestanden zijn op verzoek binnen 24 uur beschikbaar voor opdrachtgever ten behoeve van incidentonderzoek of forensische analyse	≤ 24 uur

2.11 Databeheer, Back-up en Restore services

Middels de back-up en restore services worden preventief kopieën gemaakt van de aanwezige data, en waar nodig/van toepassing infrastructuur en applicatie.

Hierdoor worden deze gegevens veiliggesteld voor het geval de gegevens op de originele locatie verloren gaan of beschadigd raken. Indien nodig kan een back-up weer op de oorspronkelijke locatie teruggeplaatst worden.

De volgende eisen worden gesteld:

Omgeving	RPO	Onsite bewaartermijn	Offsite bewaartermijn
Productie	24 uur	1 maand	1 jaar
Acceptatie	24 uur	1 maand	1 maand
Test	48 uur	2 weken	n.v.t.

Restoreverzoeken worden aangevraagd middels een (standaard) wijziging. Doorlooptijden worden vastgelegd in (standaard) wijzigingsverzoeken.

2.12 Privacy en gegevensbescherming- meldplicht

Opdrachtnemer treedt op als verwerker in de zin van AVG art. 28. Een verwerkersovereenkomst wordt als separaat document bij het SLA gevoegd.

Opdrachtnemer meldt datalekken (inbreuken op persoonsgegevens) binnen 4 uur aan de Security Officer van opdrachtgever, zodat opdrachtgever binnen 72 uur kan melden bij de Autoriteit Persoonsgegevens (AVG art. 33).

2.13 Service Level Rapportage

Opdrachtnemer stelt binnen 10 werkdagen na afloop van elke maand de Service Level Rapportage (SLR) beschikbaar aan de afdeling Service Delivery Management (SDM) van Opdrachtgever.

Eisen ten aanzien van de inhoud van de rapportage dienen tenminste het volgende te bevatten:

- Alle meldingen aangemeld en afgerond (aantal, prioriteit, soort melding).
- Prestatieoverzichten van afhandeling meldingen (duur openstaande melding, reactietijd, hersteltijd, per categorie) inclusief percentage KPI-realiserende.
- Aantal, soort en beschrijving van incidenten.
- Beschikbaarheidsrapportage over overeengekomen en afgenomen services en componenten, inclusief behaalde en afgesproken niveaus en de identificatie waar verbetering kan plaatsvinden.
- Wijzigingenbeheer: overzicht openstaande en uitgevoerde wijzigingen inclusief KPI-realiserende.
- Trendanalyse over laatste 6 maanden van overeengekomen KPI-afspraken.
- CMDB-rapportage.
- Verbetermaatregelen van service levels indien deze beneden het vereiste niveau zijn of dreigen te raken.

2.14 Documentatie en Exit

Specifieke voorwaarden ten aanzien van documentatie en exit-plan worden opgenomen in de overeenkomst; eventuele extra SLA afspraken kunnen hier worden opgenomen

Detailafspraken inzake data-overdracht worden vastgelegd in een Exit- / Retransitieplan, welke als bijlage bij de overeenkomst wordt opgenomen.

Richtlijnen voor een Exit- / Retransitieplan:

Onderwerp	Eis	Termijn
Transitieperiode	Opdrachtnemer verleent volledige medewerking aan transitie naar opvolgende leverancier of in-house oplossing.	Minimaal 6 maanden na opzegging
Data-export	Alle data wordt geëxporteerd in een open, machine-leesbaar formaat (CSV, JSON, XML of SQL-dump).	Binnen 5 werkdagen na verzoek
Datadeletie	Na bevestiging van succesvolle overdracht worden alle data (inclusief back-ups) aantoonbaar verwijderd.	Binnen 90 dagen na overdracht, met bewijs van deletie
Documentatie	Actuele technische documentatie, API-specificaties, configuratiedocumentatie en beheerdocumentatie.	Beschikbaar bij start transitie
Kennisoverdracht	Opdrachtnemer ondersteunt kennisoverdracht aan opdrachtgever of opvolgende partij.	Binnen transitieperiode

3. Communicatie provincie Noord-Brabant en Opdrachtnemer

Voor het bewaken van de afgesproken kwaliteit, het realiseren van de afgesproken dienstenniveaus en het doorvoeren van veranderingen en verbeteringen (bijvoorbeeld vastgelegd in verbeterplannen) is regelmatig overleg op diverse organisatieniveaus noodzakelijk.

In onderstaande tabel is vastgelegd wanneer gestructureerd overleg plaatsvindt, wie er aan dit overleg deelnemen en wie bij beide partijen verantwoordelijk is voor de onderlinge relatie. Neem tevens een overzicht op van alle contactpersonen en verantwoordelijken bij escalatie of calamiteiten.

Een nadere concretisering van deze overlegvormen kan worden opgenomen in een DAP. Denk hierbij aan tijdstippen of aanleidingen voor overleg en de betrokken personen bij overleg.

Overlegniveau	Frequentie	Participanten (=bevoegden)	Agenda/doel
Operationeel	1x per maand	<u>Opdrachtgever</u> • Servicemanager • Functioneel beheerder • (ISO) • (Contractmanager) <u>Opdrachtnemer</u> • Servicemanager • Operationeel manager • (Contractmanager)	• Stand van zaken lopende zaken • Updates van werkafspraken • Extra facturabele activiteiten • Inhoudelijke bespreking van lopende incidenten / problemen / escalaties • Kwaliteit van de services / leveringen • Actuele risico's • Verbetering in de communicatie onderling • Roadmap (o.a. input wensen van klanten) van leverancier en nieuwe ontwikkelingen ,evt. aanstaande projecten / grote aanpassingen)
Tactisch	1x per kwartaal	<u>Opdrachtgever</u> • Servicemanager • Contractmanager • (Functioneel beheerder) • (Proces Manager) • (ISO) <u>Opdrachtnemer</u> • Servicemanager • Contractmanager • Product owner	• Bespreken highlights van de kwaliteit van de dienstverlening op basis van de SLA rapportages incl. operationele issues en escalaties • Bespreking van de ingekomen grote projecten • Verbetervoorstellen en goedkeuring daarvan (Changemanagement) • Actuele risico's • Klant tevredenheid • Status realisatie contractdoelstellingen • Proces evaluatie • Facturatie • Actualiteit Technische- en Beheerdocumentatie • Wijze van uitvoering van het contract, SLA en DFA en evt. voorstellen voor aanpassing (als input voor Strategisch overleg) • Wijzigingen op het DAP • Roadmap en nieuwe ontwikkelingen
Strategisch	1x per jaar	<u>Opdrachtgever</u> • Contractmanager • Contracteigenaar • (CISO) <u>Opdrachtnemer</u> • Contractmanager • Directie of • Account manager	• Evaluatie van de belangrijkste escalaties, dienstverlening en samenwerking • Contractdoelstellingen • Voortgang en vaststellen/bijstellen gezamenlijke toekomstvisie • Verbetervoorstellen en goedkeuring daarvan • Accorderen wijzigingen op het Contract / SLA en /of Dossier Financiële Afspraken (DFA) (indien van toepassing)

3.1. Dienstrapportages

Zie paragraaf 2.13 voor specifieke rapportages voor een bepaald proces.

Als provincie moeten we zicht hebben, krijgen en houden op alles wat te maken heeft met de afgenomen dienstverlening. Daarnaast kan ook afgesproken worden dat de opdrachtnemer periodiek een onderzoek naar de kwaliteit van de beveiliging laat doen door een onafhankelijke derde. Dergelijke afspraken worden in de klantleveranciersovereenkomst vastgelegd, waarbij bepaald wordt dat jaarlijks een externe auditor de opdracht krijgt een zogenaamde Third Party-Mededeling (TPM) op te stellen. De TPM bevat een oordeel over de kwaliteit van het stelsel van maatregelen van interne controle en beveiliging bij de opdrachtnemer en biedt de provincie de garantie dat de opdrachtnemer zijn contractuele beveiligingsafspraken is nagekomen.

3.2. Klachten

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

- Binnen twee werkdagen na de melding komt de opdrachtnemer tot een voorstel voor de afhandeling van de klacht.
- De klacht kan pas afgesloten worden na goedkeuring van de opdrachtgever.

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

3.3. Contactgegevens provincie Noord-Brabant

- E-mail onsloket@brabant.nl
- Telefoon 073 680 88 88

4. Definities

Term	Definitie
API	Application Programming Interface; een set definities en protocollen waarmee softwarecomponenten met elkaar communiceren.
Asset en Configuratie management	Het proces dat zorgt voor het identificeren, registreren en beheren van assets en configuratie-items binnen de IT-dienstverlening.
Auditor	Onafhankelijke partij die controleert of aan vooraf vastgelegde eisen is voldaan, zoals de naleving van beveiligingsmaatregelen in de SLA.
Bedrijfskritische systemen	Systemen die essentieel zijn voor het primaire proces van de organisatie; uitval ervan heeft directe impact op de continuïteit van de dienstverlening.
Bugfix	Een kleine correctie in de software die bedoeld is om fouten te herstellen of beveiligingslekken te dichten.
Bugs	Fouten of gebreken in software die leiden tot verstoringen, onjuist of ongewenst gedrag van een applicatie of systeem.
Configuration Management Database (CMDB)	Een centrale database met informatie over alle configuratie-items en hun onderlinge relaties binnen de dienstverlening.
Doorlooptijd	De tijd tussen de ontvangst van een verzoek of incident en de volledige afhandeling, inclusief terugkoppeling.
Dossier Afspraken en Procedures (DAP)	Document dat de operationele, dagelijkse werkwijze beschrijft (hoe, door wie, met welke middelen).
Dossier Financiële Afspraken (DFA)	Document waarin de financiële afspraken tussen opdrachtgever en opdrachtnemer zijn vastgelegd, als onderdeel van de dienstverleningsovereenkomst.
Exit- / Retransitieplan	Een plan dat beschrijft hoe data, diensten, hardware en verantwoordelijkheden worden overgedragen bij beëindiging of wijziging van de samenwerking met de leverancier.
Incidentmanagement	Het ITIL-proces gericht op het zo snel mogelijk herstellen van normale dienstverlening na een verstoring.
IT Infrastructure Library (ITIL)	Een wereldwijd erkend best-practice-raamwerk voor IT-servicemanagement (ITSM). Het beschrijft generieke processen, rollen en principes om IT-diensten te plannen, leveren, beheren en continu te verbeteren, zodat deze aansluiten op de behoeften van de organisatie.
Keystroke registratie	Toetsaanslagregistratie, is het proces waarbij elke toetsaanslag op een apparaat wordt vastgelegd.
Security patch	Een essentiële beveiligingsgerelateerde software-update, die met spoed en volgens afgesproken procedures moet worden geïmplementeerd.
Key Performance Indicator (KPI)	Specifiek, meetbaar, acceptabel, realistisch en tijdsgebonden beschreven prestatie-eenheid waarmee de kwaliteit van dienstverlening wordt beoordeeld.
Niet-kritieke functionaliteit	Functionaliteit waarvan het uitvallen geen directe impact heeft op bedrijfsprocessen of kernfunctionaliteit.
Niet standaard wijzigingen	Wijzigingen die buiten de standaard dienstverlening vallen en via het formele changeproces worden behandeld.
Patch	Een softwarecorrectie die functionele of beveiligingsproblemen oplost, of nieuwe functionaliteiten toevoegt.
Reactietijd	De tijd tussen het melden van een incident of verzoek en de eerste inhoudelijke reactie van de opdrachtnemer.
Release	Het vervangen van bestaande programmatuur door een nieuwere, betere of uitgebreidere versie
Root Cause Analyse (RCA)	Een gestructureerde analyse om de dieperliggende oorzaak van een incident of probleem te achterhalen.
Software as a Service (SaaS)-applicatie	Een via internet aangeboden applicatie die door de leverancier technisch wordt beheerd en onderhouden.
Service Improvement Plan (SIP)	Een plan met acties en doelstellingen gericht op structurele verbetering van de IT-dienstverlening.
Service Level	Het afgesproken kwaliteitsniveau van een dienst, zoals beschikbaarheid, reactietijd of doorlooptijd. Vastgelegd middels KPI's.
Service Request	Een standaardaanvraag van een gebruiker, bijvoorbeeld voor informatie, advies of toegang tot een dienst.

Term	Definitie
Spoed wijzigingen	Wijzigingen die per direct moeten worden uitgevoerd vanwege kritieke incidenten of beveiligingsrisico's.
Standaard wijzigingen	Veelvoorkomende, vooraf goedgekeurde wijzigingen binnen de reguliere dienstverlening, zonder extra kosten.
Upgrade	Het vervangen of uitbreiden van bestaande programmatuur door een nieuwer, krachtiger of uitgebreider systeem.
Versie N of N-1	Het beleid dat systemen draaien op de meest actuele versie (N) of één versie daaronder (N-1) voor veiligheid en compatibiliteit. Dit betreft daarmee de meest actuele majeure versie (vb. van 1.3 naar 2.1)
Webportaal	Een online omgeving waar gebruikers incidenten en verzoeken kunnen melden en/of functioneel beheer meldingen kunnen indienen en de voortgang daarvan kunnen volgen.

Bijlage A: PNB Informatiebeveiliging

Normatieve verwijzingen

Verwijzing	Titel	Versie/Datum
ISO 27001	NEN-EN-ISO/IEC 27001:2023	2023
ISO 27002	NEN-EN-ISO/IEC 27002:2022	2022
BIO2	Baseline Informatiebeveiliging Overheid 2 v1.3	5 maart 2026
NIS2	EU Richtlijn 2022/2555	2022
Cbw	Cyberbeveiligingswet	augustus 2026
AVG	Algemene Verordening Gegevensbescherming (EU 2016/679)	2016
NCSC VM Toolbox	Kwetsbaarheidsbeheer — hersteltermijnen	v1.1 (dec 2024)