Service Level Agreement
Managed Security Services Provider (MSSP)

GGD GHOR Nederland

Inhoudsopgave

1. Inleiding

1.1 Document informatie

Deze SLA beschrijft de overeengekomen servicelevels tussen GGD GHOR Nederland en de Managed Security Services Provider (MSSP) voor het leveren van integrale beveiligingsdiensten. Een MSSP is een gespecialiseerde externe partij die continu toezicht houdt op de digitale omgeving, dreigingen detecteert en passende beveiligingsmaatregelen adviseert en uitvoert. Het doel van deze samenwerking is het waarborgen van een veilige, betrouwbare en compliant digitale werkomgeving voor GGD GHOR Nederland en haar ketenpartners.

- **Versie:** 0.9 – *Concept voor afstemming met SLM en Inkoop en Contractmanagement (IC&M)*
- **Datum:** [in te vullen]
- **Opdrachtgever:** GGD GHOR Nederland
- **Opdrachtnemer:** [in te vullen]

1.2 Documentatiebeheer

De Opdrachtnemer (MSSP) draagt er gedurende de gehele contractperiode zorg voor dat GGD GHOR Nederland te allen tijde beschikt over actuele, volledige en juiste documentatie met betrekking tot alle door de MSSP geleverde beveiligingsdiensten, gebruikte technologieën, processen, detectieregels en procedures.

De documentatie vormt een essentieel onderdeel van het beheer, toezicht en de governance van de securitydienstverlening en wordt gebruikt door GGD GHOR Nederland, het Governance Security Operations Center (G-SOC) en overige betrokken rollen.

De documentatie omvat ten minste:

- **Functionele securitydocumentatie:** Beschrijvingen van securityprocessen, escalatieprocedures, runbooks, SOC-use cases, detectieregels, workflows, rapportageformats en operationele werkinstructies.
- **Technische securitydocumentatie:** Architectuurdocumentatie van securityoplossingen, sensor-/agentconfiguraties, logging- en monitoringflows, correlatieregels, integraties met SIEM/SOAR, netwerksegmentaties, toegangsmodellen, hardening-standaarden en back-up/herstelprocedures van securitysystemen.
- **Wijzigings-, versie- en releasehistorie:** Wijzigingen in detectieregels, nieuwe of aangepaste securityoplossingen, updates, patches, configuratie-aanpassingen en verbeteringen in beveiligingsprocessen.
- **Documentatie over risico's, incidenten en kwetsbaarheden:** Overzichten van bekende risico's, gedetecteerde afwijkingen, incidentrapportages, root cause analyses, aanbevelingen en mitigerende maatregelen.
- **Contact- en escalatiepunten binnen de MSSP:** Escalatieladders, SPOC's, SOC-analisten, security engineers en 24/7 bereikbaarheid.

De Opdrachtnemer werkt de documentatie tijdig en aantoonbaar bij na elke wijziging, release, configuratieaanpassing of relevant security-event. De documentatie wordt digitaal en veilig beschikbaar gesteld via een door de Opdrachtgever goedgekeurd documentatieportaal of beveiligd platform.

De specifieke werkafspraken over het aanleveren, actualiseren, beoordelen en accorderen van documentatie worden verder uitgewerkt in het Dossier Afspraken en Procedures (DAP), dat integraal onderdeel vormt van deze SLA.

1.2 Opdrachtgever en opdrachtnemer

Deze Service Level Agreement (SLA) bevat de Service Level afspraken tussen Opdrachtgever en Opdrachtnemer (MSSP) inzake de levering, het beheer en de ondersteuning van beveiligingsdiensten. Deze SLA wordt overeengekomen door:

GGD GHOR Nederland, gevestigd en kantoorhoudende te Zwarte Woud 2, 3524 SJ Utrecht, rechtsgeldig vertegenwoordigd door [naam vertegenwoordiger], hierna te noemen: 'Opdrachtgever';

En

[Naam MSSP], gevestigd te [adres], rechtsgeldig vertegenwoordigd door [naam vertegenwoordiger], hierna te noemen: 'Opdrachtnemer';

Overwegende dat:

Deze SLA maakt onlosmakelijk deel uit van de Overeenkomst tussen Opdrachtgever en Opdrachtnemer en bevat aanvullende afspraken over de geleverde diensten.

De definities uit de Overeenkomst zullen op gelijke wijze in deze SLA worden gebruikt.

In deze SLA worden de kwalitatieve en kwantitatieve afspraken, met betrekking tot het beheer en onderhoud van de beveiligingsdiensten (MSSP) van GGD GHOR Nederland, vastgelegd.

De praktische aspecten van afstemming tussen Opdrachtgever en Opdrachtnemer met betrekking tot de overeengekomen dienstverlening zijn opgenomen in het Dossier Afspraken en Procedures (DAP). In het DAP zijn de werkafspraken en procedures op het koppelvlak tussen Opdrachtgever en Opdrachtnemer vastgelegd. Het DAP maakt integraal deel uit van deze SLA.

1.3 Doel van deze SLA

Het doel van deze SLA is het vastleggen van duidelijke afspraken over de levering van managed security services, zodat GGD GHOR Nederland verzekerd is van een proactieve, schaalbare en transparante beveiligingsdienstverlening. Deze SLA ondersteunt het functioneren van het Governance Security Operations Center (G-SOC), borgt compliance met relevante normen en wetgeving, en stelt kaders voor samenwerking, rapportage en continue verbetering.

1.4 Context en achtergrond

GGD GHOR Nederland is de landelijke koepelorganisatie van 25 GGD'en en GHOR's en ondersteunt de publieke gezondheid en veiligheid. Na de COVID-19-pandemie heeft de organisatie gekozen voor een strategische ICT-transitie: het uitfaseren van eigen infrastructuur en het omschakelen naar managed services. Deze transitie stelt GGD GHOR Nederland in staat om:

- Schaalbaar en flexibel op te schalen van circa 300 FTE naar maximaal 1.000 FTE in crisissituaties.
- Gestandaardiseerd en efficiënt te werken volgens ITIL v4-principes en moderne IT-servicemanagement (ITSM)-processen.
- Compliance en informatiebeveiliging te borgen conform BIO, AVG, NEN-ISO 27001/27002 en de GIBIT 2025-richtlijnen.
- Continuïteit en voorspelbaarheid te realiseren door duidelijke afspraken met de MSSP over prestaties, beschikbaarheid en kwaliteit van dienstverlening.

1.5 Contractperiode

1.6 Scope van de dienstverlening

De scope van de MSSP betreft ten minste:

- Het volledige GGD GHOR Nederland domein en alle daarbinnen actieve kantoor- en bedrijfsvoeringapplicaties, oplossingen en voorzieningen;
- Idealiter ook het gedeelde domein met GGD'en en GHOR's en alle daarbinnen actieve standaard-, hybride- en maatwerkapplicaties, oplossingen en voorzieningen;
- Idealiter ook de Data Intelligence-voorzieningen.

De MSSP levert en beheert de volgende beveiligingsdiensten:

Domein	Omschrijving
Prevention & Detection	24/7 monitoring van systemen, SIEM-integratie, threat intelligence, honeypots, anomaliedetectie en perimeter security.
Incident Response & Risk Management	Incidentrespons binnen afgesproken tijdslijnen, forensisch onderzoek, herstelservices, penetratietesten
Netwerk & Dataprotectie	Monitoring van Firewallbeheer, VPN, Data-encryptie, DLP en endpoint protection via SIEM. Analyse van afwijkingen, correlatie van logdata en rapportage naar aanleiding van gedetecteerde risico's.
Security Governance & Compliance	Periodieke securityrapportages, KPI/KRI-monitoring, ondersteuning bij BIO, AVG, ISO 27001/2 en NEN 7510, risk assessments, maturity-beoordelingen en strategisch security-advies.
Security Awareness & Human Risk Management	Phishingtests, risicogedrag-analyses, gerichte awareness-campagnes, trainingsprogramma's en periodieke evaluaties van bewustzijnsniveaus.
Integratie met G-SOC	Volledige koppeling met Governance Security Operations Center (G-SOC) van GGD GHOR Nederland
Security Assessments & Testing	Veiligheidsassessments, risicoanalyses, kwetsbaarhedenscans, red teaming en penetratietesten (webapps, infrastructuur, API's, mobile,

Domein	Omschrijving
	cloud). Rapportage inclusief bevindingen, risico-classificatie en mitigerende adviezen.
Security Consultancy & Expert Services	Advies en begeleiding op threat hunting, incident investigation, incident response planning, herstelservices, security roadmap-ontwikkeling, optimalisatie van detectiecapaciteiten en begeleiding bij security-verbeterprogramma's.

1.7 Uitgangspunten

Deze SLA is gebaseerd op de principes van ITIL v4 en de governance-kaders van GGD GHOR Nederland. De volgende uitgangspunten zijn leidend:

- Transparantie, samenwerking en vertrouwen tussen Opdrachtgever, MSSP en G-SOC;
- Naleving van wet- en regelgeving (BIO, AVG, NEN-ISO 27001/27002, NEN 7510, GIBIT 2025);
- Eén gezamenlijk servicemanagementproces voor incident-, probleem-, change- en releasemanagement;
- Continu verbeteren via Continual Service Improvement (CSI);
- Gebruik van de centrale ServiceNow-omgeving voor registratie, rapportage en communicatie;
- Data-soevereiniteit: alle data blijven binnen de Europese Economische Ruimte (EER)

1.8 Begrippen en definities

Begrip	Definitie
Opdrachtgever GGD GHOR Nederland	Partij die de overeenkomst sluit en governance voert.
Opdrachtnemer (MSSP)	Externe Managed Security Services Provider die 24/7 securitydiensten levert (monitoring, detectie, respons, rapportage).
SLA (Service Level Agreement)	Contractueel document met serviceniveaus, KPI's, processen, escalaties, rapportages en verantwoordelijkheden.
DAP (Dossier Afspraken en Procedures)	Detailafspraken, procedures en runbooks op het koppelvlak opdrachtgever–MSSP; integraal onderdeel van de SLA.
Servicevenster	Afgesproken tijdvakken voor beschikbaarheid en onderhoud (o.a. 24/7 monitoring; maandelijks onderhoud buiten kantooruren).
Beschikbaarheid	Mate waarin een dienst/platform operationeel is binnen de afgesproken periode (gerapporteerd als percentage).
Incident	Ongeplande verstoring of security-event met impact op beschikbaarheid, integriteit of vertrouwelijkheid (BIV).
Major Incident	Kritiek incident dat primaire processen significant verstoort of stillegt; vereist versnelde escalatie/communicatie.
Problem (Problem Management)	Onderliggende, onbekende oorzaak van één of meer incidenten; gericht op structurele oplossing en voorkomen van herhaling.
Change (Change Management)	Geautoriseerde, gecontroleerde wijziging aan diensten/infrastructuur/securitycomponenten (standaard, normaal, spoed).
Release (Release Management)	Gecontroleerde uitrol van nieuwe/gewijzigde software of configuraties met testen, rollback en post-evaluatie.

Begrip	Definitie
Request (Request Management)	Gestandaardiseerde afhandeling van serviceverzoeken (standaard en niet-standaard) via ITSM.
Prioriteit P1/P2/P3/P4	Classificatie op impact/urgentie: P1 = kritiek; P2 = hoog; P3 = normaal; P4 = laag/informatie/advies.
Reactietijd	Tijd tussen melding/registratie en eerste actie/acknowledgement door de MSSP.
Oplostijd	Tijd tot herstel of containment binnen de afgesproken norm per prioriteit.
KPI (Key Performance Indicator)	Prestatie-indicator, zoals beschikbaarheid, incidentrespons, patch compliance, logretentie, klanttevredenheid.
MTTD / MTTA / MTTI / Time to Notify	Metrics: Detect (MTTD), Acknowledge (MTTA), Investigate (MTTI) en meldtijd na bevestiging van een incident.
SIEM	Security Information and Event Management: centrale logverzameling, correlatie en alerting.
SOAR	Security Orchestration, Automation & Response: orkestratie/automatisering van playbooks en respons.
EDR / NDR / XDR	Detectie & respons op endpoint (EDR), netwerk (NDR) en geïntegreerd over domeinen (XDR).
UEBA	User & Entity Behavior Analytics: anomaliedetectie op basis van gedrag van gebruikers/entiteiten.
MXDR	Door MSSP beheerde XDR-dienst (24/7 detectie & respons).
Threat Intelligence	Interne/externe dreigingsinformatie (feeds) ter verbetering van detectie en correlatie.
Patchmanagement	Identificeren, beoordelen, plannen, implementeren en rapporteren van software-updates/patches.
CVSS-score	Standaard 0–10 schaal voor kwetsbaarheids-ernst; stuurt urgentie/implementatietermijn.
Disaster Recovery (DR)	Herstel van kritieke IT-diensten na verstoring conform plan en testregime.
RPO / RTO	Recovery Point Objective (max. dataverlies) / Recovery Time Objective (max. hersteltijd).
Logretentie	Afgesproken bewaartermijn van security/operationele logs (minimaal 180 dagen).
BIV-classificatie	Classificatie van informatie op Beschikbaarheid, Integriteit, Vertrouwelijkheid.
BIO / AVG / NEN-ISO 27001/27002 / NEN 7510 / GIBIT	Normenkaders/wetgeving die de MSSP-dienstverlening moet naleven.
Data-soevereiniteit (EER)	Data blijft binnen de Europese Economische Ruimte en is beschermd tegen toegang door niet-EU overheden.
Toegangsbeheer (MFA, JIT/JEA)	Authenticatie en autorisatie met Multi-Factor Authentication en Just-In-Time/Just-Enough-Access.
Runbook	Gestandaardiseerde stappen/werkinstructies voor detectie, triage en respons (SOC).
RCA (Root Cause Analysis)	Analyseverslag van oorzaak, tijdlijn, impact, mitigaties en verbeteracties na (major) incident.

Begrip	Definitie
PIR (Post-Implementation Review)	Evaluatie na release/change om resultaten en verbeterpunten vast te leggen.
SLR (Service Level Rapportage)	Maandrapportage met prestaties, incidenten, changes, beschikbaarheid, vulnerabilities en compliance.
TSO / SSOT	Tactisch (kwartaal) en Strategisch (halfjaar) serviceoverleg voor voortgang en alignment.
Escalatieproces	Gelaagde opvolging bij (dreigende) SLA-overschrijding of kritieke impact; niveaus, rollen en reactietijden vastgelegd.
Exitplan	Afspraken voor overdracht van documentatie/data en ondersteuning bij transitie naar nieuwe leverancier of intern.
ServiceNow	ITSM-platform van GGD GHOR NL voor registratie, workflow, rapportage en KPI-meting.

1.9 Rollen en verantwoordelijkheden

Nader in te vullen

2. Servicevensters en beschikbaarheid

Dit hoofdstuk beschrijft de tijdsvensters waarin de MSSP-diensten beschikbaar dienen te zijn en de bijbehorende serviceniveaus. Het doel is om de continuïteit van de dienstverlening te waarborgen en duidelijke normen vast te leggen voor beschikbaarheid, reactietijden en escalatie.

2.1 Servicevensters

De MSSP levert diensten die zijn afgestemd op de kritieke aard van informatiebeveiliging. Daarom gelden voor verschillende typen dienstverlening verschillende servicevensters:

- **Monitoring & detectie:** 24/7 beschikbaar. De MSSP monitort continu op afwijkingen, dreigingen en anomalieën.
- **Incidentrespons:** 24/7 bereikbaar voor P1-incidenten via directe lijn met GGD GHOR Nederland. Voor overige incidenten geldt een reactievenster binnen kantooruren.
- **Rapportage & communicatie**: Tijdens kantooruren (Ma–Vr 08:00–18:00). Periodieke rapportages worden afgestemd met GGD GHOR Nederland.

2.2 Reactietijden en oplostijden (MSSP-minimum)

Prioriteit	Definitie	Reactietijd	Oplostijd
P1 – Kritiek	Incidenten met directe impact op de organisatie of dataveiligheid	≤ 30 minuten	≤ 4 uur (containment)
P2 – Hoog	Incidenten met ernstige impact op afdelingen of processen	≤ 30 minuten	≤ 8 uur
P3 – Normaal	Incidenten met beperkte impact	≤ 2 uur	≤ 1 week
P4 – Laag	Informatieverzoeken of kleine verstoringen	≤ 4 uur	≤ 2 weken

Deze serviceniveaus worden gemonitord via ServiceNow en gerapporteerd in de maandelijkse SLA-rapportages.

2.3 Key Performance Indicators (KPI's)

KPI*	Norm	Frequentie	Onderhoudsvenster	Max. downtime kwartaal
Beschikbaarheid SIEM/SOC	≥ 99,9%	Maandelijks	Buiten kantooruren	≤ 2,19 uur
Security platforms	≥ 99,8%		Buiten kantooruren	≤ 5,46 uur
Incidentrespons P1	≥ 95% binnen norm	Maandelijks		
Patch compliance	≥ 98%	Maandelijks		
Logretentie	≥ 180 dagen	Continu		
CSAT (Security tickets)	3.5/5	Maandelijks		

RPO: Maximaal 2 uur
RTO: Maximaal 4 uur
Disaster Recovery Test: Minimaal jaarlijks
*Meetmethode: timestamps in ServiceNow.

3. Monitoring & Threat Detection

De Opdrachtnemer (MSSP) voert 24/7 monitoring uit op alle beveiligingscomponenten (SIEM, firewalls, endpoints, cloud). Doelen:

- Detectie van dreigingen en anomalieën via correlatie, threat intelligence en honeypots;
- Meldingen van P1/P2-incidenten aan het G-SOC;
- Trendanalyse en structurele risicorapportage;
- Onderhoud van logging-infrastructuur en dashboards;
- Integratie met ServiceNow voor event-registratie.

4. Incident management

Dit hoofdstuk beschrijft de wijze waarop incidenten worden geclassificeerd, opgevolgd en opgelost binnen de dienstverlening van de MSSP. Er wordt onderscheid gemaakt tussen:

- **Reguliere incidenten:** verstoringen in IT-diensten zoals werkplekken, netwerk en applicaties.
- **Security incidenten:** incidenten die direct betrekking hebben op informatiebeveiliging en de Beschikbaarheid, Integriteit en Vertrouwelijkheid (BIV) van gegevens. Deze vereisen een versnelde en strengere aanpak vanwege mogelijke impact op privacy, compliance en bedrijfscontinuïteit.

De Opdrachtnemer (MSSP) rapporteert maandelijks over dit domein conform de vereisten in hoofdstuk 11 – Service Level Rapportages. De MSSP werkt nauw samen met het G-SOC bij de afhandeling van kritieke incidenten. Alle incidenten worden gemeten en gemonitord via de volgende MT-metrics:

- **MTTD (Time to Detect):** tijd tot detectie van een incident;
- **MTTA (Time to Acknowledge):** tijd tot erkenning van een incident;
- **MTTI (Time to Investigate):** tijd tot eerste onderzoek of analyse;
- **Time to Notify:** tijd tot notificatie aan relevante stakeholders.

4.1 Incident prioriteiten en metrics

De onderstaande tabel combineert reguliere en security-incidenten met hun prioriteit, voorbeelden en meetbare responstijden:

Tier	MTTD	MTTA	MTTI	Time to Notify
Premium	≤ 30 min	≤ 15 min	2–4 uur	≤ 1 uur
Advanced	≤ 1 uur	≤ 30 min	≤ 8 uur	≤ 2 uur
Basic	≤ 4 uur	≤ 1 uur	≤ 24 uur	≤ 4 uur

4.2 Security incident prioriteiten

Security-incidenten hebben een versterkte focus op BIV:

Prioriteit	Omschrijving
P1	Integriteit en/of vertrouwelijkheid van informatie of processen direct in gevaar.
P2	Beschikbaarheid van informatie of processen direct in gevaar.
P3	Observaties die mogelijk tot P1/P2 leiden, rekening houdend met tijd.
P4	Vraag of advies.

MT-metrics zijn afgestemd op de tiers zoals weergegeven in sectie 4.1.

4.3 Doorlooptijd en reactietijd GGD GHOR Nederland

De onderstaande tabel geeft de normen voor doorlooptijd en reactietijd GGD GHOR Nederland bij security incidenten:

Prioriteit	Doorlooptijd	Reactietijd
P1/Major	≤ 4 uur	≤ 30 minuten
P2	≤ 1 dag	≤ 30 minuten
P3	≤ 1 week	≤ 2 uur
P4	≤ 2 weken	≤ 4 uur

5. Major incident management

Major-incidenten zijn incidenten die kritieke bedrijfsprocessen en primaire applicaties van GGD GHOR Nederland ernstig verstoren of volledig stilleggen. Het doel van het major-incidentmanagementproces is:

- Continuïteit waarborgen van essentiële diensten tijdens een crisis.
- Impact minimaliseren door mitigerende maatregelen en tijdelijke oplossingen.
- Herstel realiseren van de dienstverlening binnen afgesproken termijnen.
- Preventie van herhaling door structurele verbetermaatregelen.

Dit proces is van toepassing op alle diensten die onder de MSP-overeenkomst vallen en wordt uitgevoerd conform ITIL v4-principes en de afspraken in deze SLA.

5.1 Procedure en afspraken bij major incidenten

Communicatie
De contactpersoon van GGD GHOR Nederland op escalatieniveau 1 wordt elke 30 minuten geïnformeerd over de status van het incident. Afwijking van deze frequentie kan alleen in overleg en wordt vastgelegd in het incidentticket.

Meldingsplicht
Major-incidenten en P1-incidenten worden zowel telefonisch als via de ITSM-koppeling gemeld.

Root Cause Analysis (RCA)
Na het oplossen van een major incident dat door de leverancier is veroorzaakt, ontvangt GGD GHOR Nederland binnen 5 werkdagen een RCA-rapport. Indien noodzakelijk worden maatregelen direct geïnitieerd conform het Change Management-proces. De inhoud van dit rapport wordt toegelicht tijdens een overleg met:

- Procesmanagement
- Service Level Management
- Product Owner Security

Het **RCA-rapport** bevat minimaal de volgende onderdelen:

- Probleembeschrijving:
    - Aanleiding of trigger van het incident
    - Duur van het incident
    - Impact op bedrijfsprocessen
    - Mitigerende of tijdelijke maatregelen
- Tijdslijn van gebeurtenissen
- Preventieve maatregelen:
    - Bevindingen en aanbevelingen (methode: *5x Waarom*)

6. Problem management

Een probleem is de onderliggende, onbekende oorzaak van één of meer incidenten. Een incident kan worden opgelost door een definitieve oplossing of door een tijdelijke workaround. Indien een incident niet direct kan worden opgelost, start het Problem Management-proces. Het probleem wordt onderzocht om een definitieve oplossing te vinden en herhaling te voorkomen.

Het doel van Problem Management is het voorkomen van herhaalde incidenten en het minimaliseren van de impact van verstoringen op de dienstverlening.

- **Root Cause Analysis (RCA);**
    - KPI: binnen 5 werkdagen na P1/P2-incident
    - Meetmethode: RCA-document in ServiceNow
- **Structurele verbeteracties vastgelegd in ServiceNow;**
    - KPI: 100% van geïdentificeerde verbeteracties vastgelegd in ServiceNow
    - KPI: Minimaal 80% van verbeteracties geïmplementeerd binnen afgesproken termijn
- Evaluatie van openstaande problemen in het **Tactisch Service Overleg (TSO);**
- Documentatie van lessons learned in het **Dossier Afspraken en Procedures (DAP).**

7. Change & Release management

7.1 Change management

Het Change Management-proces waarborgt dat alle wijzigingen aan beveiligingsdiensten gecontroleerd, geautoriseerd en gedocumenteerd worden om risico's te minimaliseren en continuïteit te garanderen. Dit proces is van toepassing op alle wijzigingen die impact hebben op IT-services, infrastructuur en beveiligingscomponenten.

- **Standaard Change:** Vooraf goedgekeurd, laag risico (bijvoorbeeld signature-updates).
- **Normale Change:** Risicobeoordeling en goedkeuring door de Change Authority Board (CAB). Een normale change is een toevoeging, aanpassing of verwijdering van (een gedeelte van) hetgeen dat effect heeft op de bestaande IT-services en infrastructuur, zoals:
    - Periodieke wijzigingen
    - Functionele wijzigingen
    - Technische wijzigingen

  Wijzigingen worden niet uitgevoerd zonder goedkeuring van de Change Authority Board van GGD GHOR Nederland. Goedgekeurde changes worden uitgevoerd op het overeengekomen tijdstip conform het opgeleverde draaiboek. Indien een change onverhoopt mislukt, wordt het rollback-plan ingezet en geëvalueerd met de changecoördinator. De leverancier informeert de changecoördinator over de status van de change of rollback na uitvoering.
- **Spoedchange**: Spoedchanges die noodzakelijk zijn ter voorkoming of oplossing van P1- en P2-incidenten. Worden gecoördineerd door de changecoördinator van GGD GHOR Nederland. De leverancier voert de change uit en levert achteraf alle benodigde informatie voor evaluatie.

De Opdrachtnemer (MSSP) rapporteert maandelijks over dit domein conform de vereisten in hoofdstuk 11 – Service Level Rapportages.

7.2 Geautoriseerde personen

- Alle change-aanvragen verlopen via het selfserviceportaal of de servicedesk van GGD GHOR Nederland.
- Na indiening wordt de change beoordeeld en goedgekeurd door de changemanager tijdens een CAB-vergadering.
- Na goedkeuring begeleidt de changecoördinator het verdere proces en monitort de uitvoering.
- Indien een change niet verloopt zoals verwacht, wordt het escalatiemodel toegepast om communicatie en opvolging te waarborgen.

7.3 Communicatie afspraken

- De leverancier verwijst niet-geautoriseerde personen naar de GGD GHOR Nederland servicedesk.
- Alle communicatie over voorbereiding en implementatie verloopt via changecoördinatie of change management van GGD GHOR Nederland.
- Voor technische of functionele afstemming kan de leverancier schakelen met de Product Owner Security en kennishouders.
- Wijzigingen worden tijdig gemeld via de ITSM-koppeling om registratie en coördinatie conform procedures te waarborgen.

7.4 Verantwoordelijkheden MSSP

De opdrachtnemer (MSSP) is verantwoordelijk voor:

- Aanlevering van change-verzoeken in ServiceNow.
- Uitvoering van impactanalyse en rollback-plan voor iedere change.
- Communicatie met GGD GHOR Nederland en betrokken teams tijdens voorbereiding en uitvoering.
- Vastlegging van alle changes in de changelog en releasekalender.

7.5 KPI's

KPI	Norm	Frequentie
% changes uitgevoerd conform CAB-goedkeuring	≥ 95%	Maandelijks
% spoedchanges geëvalueerd binnen 5 werkdagen	100%	Maandelijks
% changes met rollback-plan beschikbaar	100%	Maandelijks

7.6 Release management

Het releaseproces waarborgt dat nieuwe software-, configuratie- of securitycomponenten gecontroleerd en getest worden ingevoerd. Releases plaatsvinden buiten kantooruren:

- Acceptatietest (UAT) en rollback-plan verplicht;
- Release-notities beschikbaar voor GGD GHOR Nederland;
- Post-Implementation Review (PIR) na elke major release

Type	Frequentie	Omschrijving
Minor	Maandelijks	Bug-fixes, definities, signatures
Major	Per kwartaal	Nieuwe functionaliteit / updates
Emergency	Ad-hoc	Spoedupdates bij dreiging

8. Request management

Het Request Management-proces is een gestandaardiseerde werkwijze voor het behandelen van serviceverzoeken. Het proces zorgt ervoor dat verzoeken van gebruikers, zoals: toegang tot systemen, configuratie-aanpassingen, informatieaanvragen of andere ondersteuningsverzoeken binnen de MSSP-dienstverlening snel, veilig en efficiënt worden afgehandeld.

Het doel is een gestroomlijnde en voorspelbare afhandeling, zodat de gebruikerstevredenheid gewaarborgd blijft en de bedrijfscontinuïteit van GGD GHOR Nederland wordt ondersteund.

Binnen het Request Management-proces wordt onderscheid gemaakt tussen twee hoofdtypen verzoeken Standaard Service Requests en Niet-Standaard Service Requests.

8.1 Standaard Service Requests

Een Standaard Service Request betreft het verzoek voor het leveren van een vooraf gedefinieerde dienst. Deze verzoeken worden:

- Volgens vastgestelde werkinstructies en autorisaties uitgevoerd;
- Binnen vooraf gedefinieerde doorlooptijden afgehandeld;
- Uitgevoerd tegen vooraf bekende kosten;
- Volledig geregistreerd en gecommuniceerd via ServiceNow.

Standaardverzoeken zijn laag-risico, voorspelbaar en herhaalbaar en kunnen zonder aanvullende impactanalyse worden uitgevoerd.

8.2 Niet-Standaard Service Requests

Een Niet-Standaard Service Request betreft een verzoek dat afwijkt van de standaard dienstverlening of aanvullende beoordeling vereist. Na intake via ServiceNow bepaalt de leverancier, in afstemming met GGD GHOR Nederland, welke vervolgroute passend is.

Een niet-standaard verzoek kan worden:

- **Gehonoreerd en uitgevoerd:** Het verzoek is uitvoerbaar binnen de overeengekomen dienstverlening.
- **Gestandaardiseerd:** Het verzoek blijkt structureel of veelvoorkomend en wordt omgezet naar een Standaard Service Request.
- **Omgezet naar een Backlog Request:** Aanvullende analyse, ontwikkeling of integratie is nodig; het verzoek wordt opgenomen in de Backlog of roadmap.
- **Omgezet naar een Project Request:** Het verzoek heeft significante operationele of security-impact en moet via project-governance worden behandeld.
- **Niet gehonoreerd**: Het verzoek valt buiten scope, is niet uitvoerbaar of voldoet niet aan beveiligings- en compliance-eisen.

9. Security- en Patch management

Security- en patchmanagement betreft het door de leverancier identificeren, verkrijgen, beoordelen, implementeren en controleren van software-updates (patches). Patches zijn noodzakelijk voor het herstellen van fouten, het mitigeren van kwetsbaarheden en het waarborgen van de beveiliging en functionaliteit van de door de Opdrachtnemer beheerde systemen en diensten.

Opdrachtnemer (MSSP):

- Voert patchmanagement uit conform deze SLA;
- Monitort advisories;
- Voert impactanalyses uit;
- Rapporteert periodiek over status en afwijkingen.

Opdrachtgever (GGD GHOR Nederland):

- Autoriseert impactvolle patches;
- Faciliteert toegang tot systemen;
- Stemt onderhoudsvensters af;
- Ontvangt en beoordeelt rapportages.

9.1 Categorisering van patches

De Opdrachtnemer integreert patchmanagement als een doorlopend onderdeel van de dienstverlening. Er wordt onderscheid gemaakt tussen:

- **Standaard security patches:** updates die zonder functionele impact automatisch kunnen worden toegepast binnen reguliere onderhoudsvensters. Deze patches doorlopen geen changeproces.
- **Specifieke of impactvolle patches:** updates waarbij functionele of technische impact niet kan worden uitgesloten. Deze doorlopen verplicht het change managementproces. Voor impactvolle patches voert de leverancier een gedetailleerde impactbeoordeling uit, inclusief risicoanalyse en rollback-scenario. Implementatie vindt uitsluitend plaats conform het afgesproken changeproces en na goedkeuring door GGD GHOR Nederland.

Let op: Urgentie (CVSS-score) staat los van impact. Beide worden parallel beoordeeld en bepalen gezamenlijk de implementatieroute.

9.2 Monitoring en classificatie

De Opdrachtnemer monitort actief security-advisories die door leveranciers en relevante nationale instanties worden gepubliceerd. Alle patches worden geclassificeerd op basis van de CVSS-score en relevantie voor de omgeving van GGD GHOR Nederland.

9.3 Implementatietermijnen

De volgende implementatietermijnen zijn van toepassing:

Categorie	CVSS-score	Implementatietermijn	Afstemming met GGD GHOR Nederland
Kritische security-updates/patches	9.0+	Binnen 24 uur na publicatie	Vereist
Hoge security-updates	7.0+	Binnen 5 werkdagen na publicatie	Vereist
Overige updates	<7.0	Binnen 30 dagen/ regulier onderhoudsvenster	In overleg

10. Onderhoud en continuïteit

10.1 Standaard onderhoudsvenster

De opdrachtnemer (MSSP) hanteert een standaard maandelijks onderhoudsvenster buiten reguliere kantooruren om impact op de bedrijfsvoering van GGD GHOR Nederland te minimaliseren.

- **Tijdstip:** een avond van een werkdag, start om 18:00 uur.
- **Frequentie:** derde dinsdag of derde donderdag van elke maand.
- **Planning:** deze momenten worden vooraf opgenomen in de jaarlijkse onderhoudskalender.

Communicatie:

- Het definitieve onderhoudsschema wordt elk nieuw kalenderjaar gecommuniceerd aan GGD GHOR Nederland.
- De communicatie vindt plaats via e-mail naar:
    - vm.algemeen@ggdghor.nl
    - De contactpersonen bij Change Management.

Verplichtingen opdrachtnemer:

- Voert onderhoud uit conform planning;
- Meldt afwijkingen tijdig en stemt deze af met GGD GHOR Nederland;
- Documenteert uitgevoerde werkzaamheden voor audit en rapportage.

Het onderhoudsvenster kan worden gebruikt voor geplande patch-deployments, systeemupdates en kleine releases, mits tijdig gecommuniceerd. Uitzonderingen buiten het onderhoudsvenster vereisen expliciete goedkeuring van GGD GHOR Nederland.

10.2 Onderhoudsvenster bij pandemie of opschaling

In uitzonderlijke omstandigheden, zoals pandemieën of organisatorische opschaling, dient het standaard onderhoudsvenster door de opdrachtnemer (MSSP) te worden aangepast:

- **Starttijd:** na 23:00 uur, tenzij anders overeengekomen;
- **Afstemming:** wijziging vindt altijd plaats in overleg met GGD GHOR Nederland;
- **Communicatie:** wijzigingen worden direct gecommuniceerd naar de reguliere contactpersonen.

Het doel hiervan is het minimaliseren van impact op kritische bedrijfsprocessen, terwijl onderhoud en updates veilig kunnen worden uitgevoerd.

11.Service Level Rapportages (SLR's)

11.1 Frequentie en oplevering

De opdrachtnemer (MSSP) levert een Service Level Rapportage (SLR) maandelijks aan GGD GHOR Nederland. De SLR vormt de basis voor evaluatie van prestaties, trends, risico's en verbeteracties.

- **Oplevertermijn:** binnen 10 werkdagen na afloop van de rapportageperiode.
- **Distributie:** opgenomen in het Dossier Afspraken en Procedures (DAP).
- **KPI's:** prestaties worden beoordeeld aan de hand van de KPI's zoals beschreven in Hoofdstuk 2 – Servicevensters en beschikbaarheid.

11.2 Inhoud van de rapportages

De SLR's bevatten minimaal de volgende onderwerpen:

1. Service Level Performance

- Overzicht van prestaties ten opzichte van SLA-afspraken.
- KPI's zoals beschikbaarheid, responstijd en incidentenbeheer.
- Percentages en grafieken ter illustratie van prestaties.

2. Incidenten en Problemen

- Overzicht van alle open en gesloten incidenten en problemen.
- Classificatie op ernst (bijv. P1, P2, P3).
- Hersteltijden en genomen maatregelen om herhaling te voorkomen.

3. Wijzigingen (Change Management)

- Aantal en aard van aangebrachte wijzigingen in systemen en diensten.
- Impact van wijzigingen op de dienstverlening.

4. Beschikbaarheid (Availability Management) en Onderhoud

- Uptime van systemen en diensten gedurende de rapportageperiode.
- Geplande en ongeplande onderhoudsactiviteiten, inclusief impact op dienstverlening.

5. Capaciteitsbeheer

- Analyse van resourcegebruik (bijv. CPU, schijfruimte, netwerkbandbreedte).
- Eventuele capaciteitsproblemen en voorgestelde oplossingen.

6. Security Management

- **Kwetsbaarheidsbeheer:** overzicht van gedetecteerde kwetsbaarheden, risicoanalyse, status van maatregelen en trends.

- **Bedrijfsmiddelen:** rapportage van onbekende of ongeautoriseerde bedrijfsmiddelen binnen de dienstverlening.
- **Beveiligingsincidenten:** overzicht van incidenten zoals inbreuken, DDoS-aanvallen, malware, en gesignaleerde dreigingen.
- **Risicoanalyse:** impactanalyse van beveiligingsincidenten en blootgestelde kwetsbaarheden.
- **Maatregelen:** correctieve en preventieve acties ter mitigatie van risico's.
- **Compliance:** naleving van beveiligingsstandaarden, ISO27001 en relevante wet- en regelgeving.
- **Patchmanagement:** overzicht van uitgevoerde beveiligingsupdates en patches op systemen, software en infrastructuur.
- **Audit- en monitoringactiviteiten:** uitgevoerde audits, penetratietesten, afwijkingen en monitoring.
- **Medewerkers:** overzicht van geautoriseerde medewerkers met toegang tot systemen/informatie van GGD GHOR Nederland, inclusief VOG-status, autorisatieniveau en bewustzijn van autorisatie.

7. Patch Management

- Geïmplementeerde patches.
- Openstaande patches inclusief geplande implementatiedatum.
- Afwijkingen van de termijnen met onderbouwing.
- Risico's voor de securitypositie.
- Impactanalyse van specifieke of impactvolle patches.

8. Afwijkingen en Verbeteracties

- Overzicht van eventuele SLA-afwijkingen.
- Verbeter- en preventieve maatregelen die zijn genomen of worden voorgesteld.

9. Toekomstige acties en planning

- Vooruitblik op geplande verbeteringen, wijzigingen of uitbreidingen.
- Eventuele risico's die de serviceverlening in de komende maand kunnen beïnvloeden.

10. Conclusie en aanbevelingen

- Algemeen oordeel over de prestaties van de afgelopen maand.
- Aanbevelingen voor verbeteringen of wijzigingen om de service op het gewenste niveau te houden of te verbeteren.

11.3 Service Level gesprekken

De opdrachtnemer (MSSP) neemt deel aan een maandelijks Service Level gesprek met GGD GHOR Nederland. Tijdens dit gesprek worden de geleverde diensten besproken aan de hand van de SLR. Resultaten en afspraken worden vastgelegd in een leveranciersgesprekverslag.

11.4 Leveranciersgesprekverslag

Na elk Service Level gesprek verzorgt de opdrachtnemer (MSSP) de verslaglegging. Het verslag is toegankelijk voor GGD GHOR Nederland en dient als input voor procesverbetering en borging van de dienstverlening.

11.5 Overlegstructuur

De opdrachtnemer (MSSP)* en GGD GHOR Nederland hebben periodieke overlegmomenten ter borging van de dienstverlening en afstemming over operationele en strategische zaken:

Frequentie	Type overleg	Doel / Inhoud
Maandelijks	Service Level overleg	Bespreking van prestaties, KPI-trends en incidenten; identificatie van verbeterpunten.
Kwartaal	Tactisch Service Overleg (TSO)	Evaluatie van operationele prestaties, incidenten, trends en voortgang verbeteracties.
Halfjaarlijks	Strategisch Service Overleg (SSO)	Beoordeling van strategische doelstellingen, structurele verbeteringen en alignment met organisatiebeleid.

***Integratie met ServiceNow:** De MSSP gebruikt de bestaande ServiceNow-omgeving van GGD GHOR Nederland voor registratie van incidenten, changes en requests, zodat het overleg gebaseerd is op actuele, uniforme gegevens.*

11.6 Continu Service Improvement (CSI)

- De MSSP voert minimaal per kwartaal een evaluatie uit van prestaties, incidenten, trends en verbeteracties.
- Verbeteracties worden vastgelegd in het DAP en besproken in het Tactisch Service Overleg (TSO).
- Het doel hiervan is structurele verhoging van kwaliteit en effectiviteit van dienstverlening.

12. Compliance en Security-eisen

Dit hoofdstuk beschrijft de minimale eisen die worden gesteld aan de MSSP op het gebied van informatiebeveiliging, wet- en regelgeving en certificering.

Onderwerp	Minimumeis
Toegangsbeheer	MFA verplicht, JIT/JEA voor beheerders
Patching	Critical ≤ 7 dagen, High ≤ 14 dagen
Logging & monitoring	24/7, logretentie ≥ 180 dagen; logomgeving gescheiden van andere diensten
Security-incidenten	Classificatie P1/P2, melding binnen 24 uur; afstemming met G-SOC
Audits	Jaarlijks, conform BIO/AVG/ISO/NEN; MSSP levert auditrapportages en bewijslast
Data-soevereiniteit	Alle data blijven binnen de EER en zijn beschermd tegen toegang door niet-EU overheden

13. Escalaties en exit-strategie

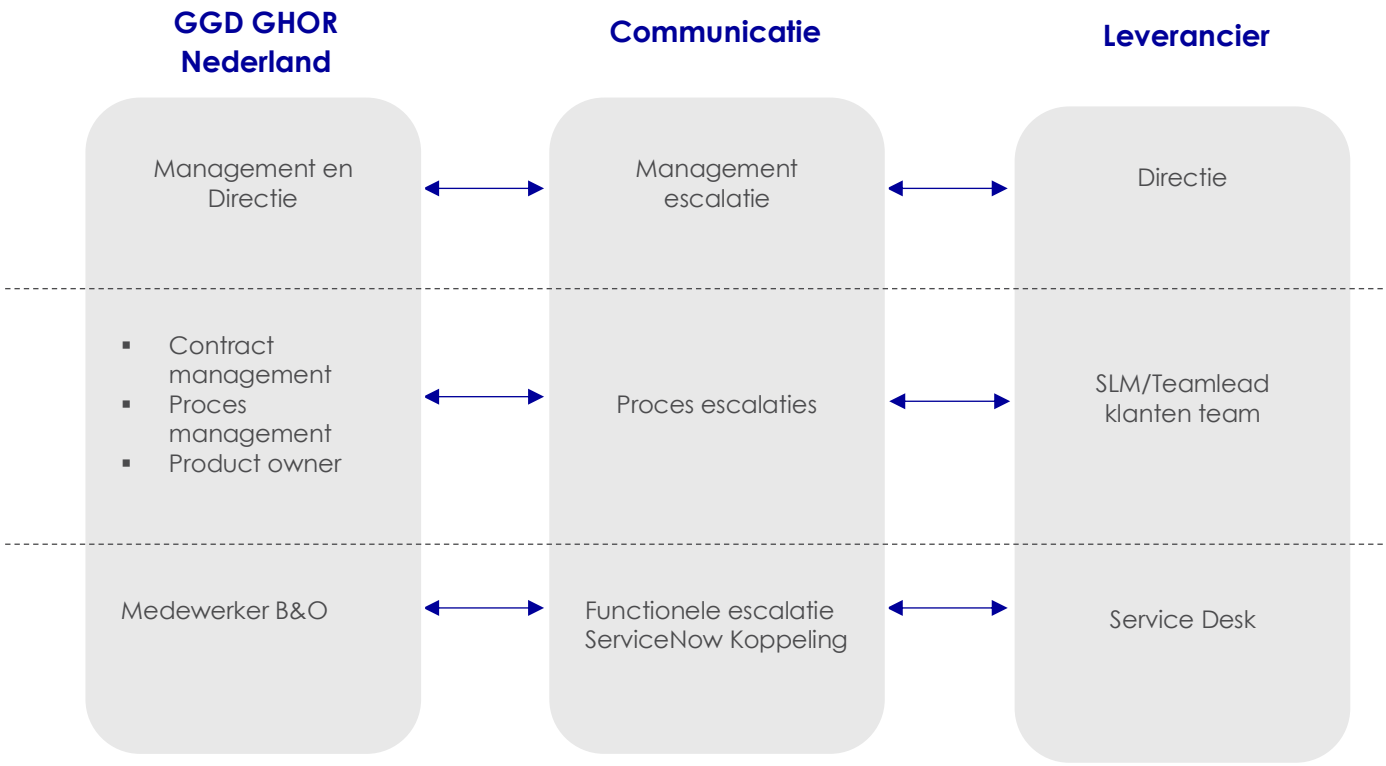
Het escalatieproces beschrijft de hiërarchische lijn waarlangs incidenten, afwijkingen of kritieke situaties worden opgevolgd indien ze niet binnen afgesproken termijnen of normen kunnen worden opgelost. Escalatie vindt plaats op basis van urgentie, impact en het type incident.

Escalatie niveau	Functie	Rol / Verantwoordelijkheid
1	Roulerend	**Medewerker Beheer & Ondersteunen (B&O)** – eerste aanspreekpunt voor operationele problemen en verzoeken. Verantwoordelijk voor registratie, initiële analyse en eerste oplossingspogingen.
2	Dienstenverantwoordelijke	**Product Owner** – verantwoordelijk voor prioritering en afstemming bij incidenten die niet op niveau 1 kunnen worden opgelost of impact hebben op dienstverlening.
3	Procesmanagement	**Procesmanager** – coördineert bij herhaalde of complexe incidenten, bewaakt procesconformiteit en ondersteunt bij structurele oplossingen.
4	(Relatie) Service Level Management	**(Relatie) Service Level Manager** – treedt op bij incidenten die SLA's raken of herhaaldelijk optreden; bewaakt contractuele afspraken en rapporteert aan management.
5	Management & Directie	**Directie** – verantwoordelijk voor strategische besluitvorming, communicatie naar stakeholders en escalatie naar externe partijen indien nodig.

13.1 Toelichting escalatieproces

1. **Startpunt:** Incidenten of afwijkingen worden altijd eerst op niveau 1 afgehandeld.
2. **Escalatiecriteria:** Escalatie vindt plaats indien:
    - Oplossing binnen afgesproken reactietijden niet mogelijk is;
    - SLA-afspraken in gevaar komen;
    - Impact op bedrijfsvoering groot is;
    - Herhaalde of kritieke incidenten optreden.
3. **Communicatie:** Iedere escalatie wordt gedocumenteerd in ServiceNow en direct gecommuniceerd naar het volgende niveau.
4. **Tijdlijnen:** Voor elk escalatieniveau gelden interne reactietijden, vastgelegd in het SLA, zodat tijdige opvolging wordt gewaarborgd.
5. **Terugkoppeling:** Na afhandeling vindt een evaluatie plaats en worden lessons learned en verbeteracties vastgelegd in het DAP of procesverbeterplan.

13.2 Communicatielijnen



13.3 Exit-plan

Bij beëindiging van de dienstverlening, om welke reden dan ook, gelden de volgende afspraken:

- **Overdracht van documentatie:** Alle relevante handleidingen, procesbeschrijvingen, configuraties, logbestanden en rapportages worden overgedragen aan GGD GHOR Nederland.
- **Export van data:** Data wordt geleverd in vooraf overeengekomen, standaardformaten zodat continuïteit en integratie met bestaande systemen gewaarborgd zijn.
- **Medewerking aan transitie:** De MSSP ondersteunt actief bij de overgang naar een nieuwe leverancier of interne uitvoering, inclusief kennisoverdracht aan medewerkers van GGD GHOR Nederland.

14. Juridisch Addendum

Looptijd en herziening:

- Deze SLA treedt in werking op [datum] en heeft een looptijd van [x jaar].
- Jaarlijkse herziening in overleg tussen GGD GHOR Nederland en MSSP.

Aansprakelijkheid:

- MSSP is aansprakelijk voor directe schade veroorzaakt door nalatigheid tot een maximum van [bedrag].
- Uitsluiting van aansprakelijkheid voor indirecte schade, tenzij sprake is van grove nalatigheid.

Vertrouwelijkheid:

- Beide partijen verplichten zich tot geheimhouding van vertrouwelijke informatie.
- NDA wordt separaat ondertekend en maakt integraal deel uit van de SLA.

15. Akkoordverklaring

Aldus overeengekomen en in tweevoud ondertekend:

GGD GHOR Nederland	[Naam MSSP]
Plaats: Utrecht	Plaats: [in te vullen]
Datum:	Datum:
_____	_____
Handtekening	Handtekening
Naam:	Naam:
Functie:	Functie:

Zwarte Woud 2
3524 SJ Utrecht
ggdghor.nl