

## DEEL: I DOCUMENTENCLASSIFICATIE

Voor dit document hanteren wij classificatie: **TLP: AMBER**

SIVON maakt gebruik van de volgende classificaties en coderingen:

| Classificatie     | Toelichting                                                                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>TLP: RED</b>   | Strikte toegangscontrole. Opslag op beveiligde servers met encryptie. Distributie alleen via beveiligde kanalen.                                    |
| <b>TLP: AMBER</b> | Dit document mag gedeeld worden binnen SIVON en (externe) toegewezen belanghebbenden. Ontvanger mag niet verder delen zonder toestemming van SIVON. |
| <b>TLP: GREEN</b> | Geen restricties op toegang of distributie. Mag vrijelijk gedeeld worden binnen en buiten SIVON, maar niet via publieke kanalen.                    |
| <b>TLP: CLEAR</b> | Geen restricties op toegang of distributie. Mag vrijelijk gedeeld worden, ook via publieke kanalen binnen en buiten SIVON.                          |

## Bijlage Service Level Agreement

Inschrijver dient de Service Level Agreement (SLA) van inschrijver bij te voegen. De SLA van inschrijver moet uit de volgende vijf (5) onderdelen bestaan:

1. **Informatiebeveiliging en privacy**
2. **Beschikbaarheid en continuïteit**
3. **Performance en gebruikerservaring**
4. **Incidenten en helpdesk**
5. **Service Level Rapportage**

Per onderdeel is vermeld welke onderwerpen in de SLA van inschrijver moeten zijn opgenomen en toegelicht.

Vervolgens zijn de minimumeisen vermeld die van toepassing zijn op het onderdeel en die in de onderwerpen moeten zijn opgenomen. Ook als inschrijver een minimumeis niet/ niet volledig/ niet juist opneemt in de onderwerpen van het betreffende onderdeel, dan geldt de minimumeis zoals gesteld.

| 1. Informatiebeveiliging en privacy                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <p><b>In de SLA van inschrijver moeten ten aanzien van “Informatiebeveiliging en privacy” de onderstaande onderwerpen opgenomen en toegelicht zijn.</b></p> <ol style="list-style-type: none"> <li>1. Versiebeheer applicatie, database en besturingssystemen</li> <li>2. Autorisatie en logging van toegang tot persoonsgegevens door beheerders opdrachtnemer</li> <li>3. Vergroten van IBP bewustzijn bij medewerkers</li> <li>4. Inrichting IDS/IPS of SOC/SIEM</li> <li>5. Inrichting ontwikkelstraat (denk aan OTAP, SDLC, CI/CD)</li> <li>6. Audits, pentests, DPIA's</li> <li>7. Tests van AI-modellen op privacy, bias en beveiliging</li> <li>8. Beheer van fysieke toegang</li> <li>9. Beveiliging van back-ups</li> <li>10. Versleuteling en cryptografie</li> <li>11. Vernietiging / verwijdering afgeschreven media</li> <li>12. Overige beveiligingsmaatregelen</li> </ol> <p><b>Bij bovenstaande onderwerpen gelden de volgende minimumeisen waaraan de SLA ten aanzien van Informatiebeveiliging en privacy moet voldoen:</b></p> <ol style="list-style-type: none"> <li>a. Het LAS van inschrijver voldoet aan alle onderdelen van het gestelde in de bijlage Informatiebeveiliging en privacy.</li> </ol> |

## 2. Beschikbaarheid en continuïteit

**In de SLA van inschrijver moeten ten aanzien van Beschikbaarheid en continuïteit de onderstaande onderwerpen opgenomen en toegelicht zijn.**

1. Beschikbaarheidspercentage van het LAS
2. Service-window voor gepland onderhoud
3. Communicatie over geplande onderbrekingen
4. Beheersing van majeure incidenten (crisisscenario's)
5. Recovery Point Objective (RPO) en Recovery Time Objective (RTO)
6. Back-up en restoreprocedure
7. Nood- en uitwijkprocedures
8. Fysieke beveiliging datacenters en back-up locaties
9. Wijze waarop procedures worden getest en geoefend.
10. Beschikbaarheid broncode via Escrow-regeling

**Bij bovenstaande onderwerpen gelden de volgende minimeisen waaraan de SLA ten aanzien van Beschikbaarheid en continuïteit moet voldoen:**

- a. Het LAS is 24 uur per dag, 7 dagen per week beschikbaar voor gebruik door opdrachtgever, met uitzondering van het gestelde onder c.
- b. Het LAS kent een beschikbaarheidspercentage voor de gebruiker van minimaal 99,5% per maand, op basis van bovengenoemde beschikbaarheidseis.
- c. Regulier onderhoud (vervangen van hardware, plaatsen van nieuwe versies van de software) zal plaatsvinden in een service-window dat minimaal 24 uur voordien aangekondigd wordt aan de opdrachtgever.
- d. Na een verstoring in de beschikbaarheid van het LAS, maakt de opdrachtnemer een (korte) rapportage met daarin opgenomen minimaal: de oorzaak, het LAS en welke maatregelen opdrachtnemer heeft getroffen om een dergelijke verstoring in de toekomst te voorkomen.
- e. Het RPO (Recovery Point Objective, hoeveelheid maximaal te missen data) is maximaal 24 uur en het RTO (Recovery Time Objective, maximale duur na probleem of ramp voor hernieuwde beschikbaarheid) is maximaal 48 uur.
- f. De data- en applicatieservers zijn uitgerust met een adequate back-up- en restorevoorziening om de RPO te garanderen.
- g. De back-up-voorziening staat in een beveiligde ruimte, welke zich op een andere locatie bevindt dan de serverlocatie. De locatie beschikt over voorzieningen om brand te voorkomen en middelen om vroegtijdig in te grijpen bij brand.
- h. Opdrachtnemer beschrijft, in overleg met de opdrachtgever, een duidelijke restoreprocedure. Deze procedure wordt bekend gemaakt bij de verantwoordelijke personen bij de opdrachtgever. Voor restoreverzoeken door opdrachtgever geldt eveneens een maximale RPO van 24 uur.
- i. Om de continuïteit van het LAS te kunnen garanderen heeft de opdrachtnemer de broncode van het LAS, op basis van een actieve Escrow-overeenkomst, in bewaring gegeven bij een onafhankelijke Escrow-agent. De Escrow-overeenkomst wordt getekend door de opdrachtnemer van het LAS, de Escrow-agent en opdrachtgever. De opdrachtnemer geeft bij de opdrachtgever aan in welke programmeertaal en versie van de programmeertaal de broncode is ontwikkeld.

### 3. Performance en gebruikerservaring

**In de SLA van inschrijver moeten ten aanzien van Performance en gebruikerservaring de onderstaande onderwerpen opgenomen en toegelicht zijn.**

1. Responsetijd van de applicatie en database
2. Webbrowserondersteuning

**Bij bovenstaande onderwerpen gelden de volgende minimeisen waaraan de SLA ten aanzien van Performance en gebruikerservaring moet voldoen:**

- a. De responstijd van de applicatie is in 95% van de gevallen maximaal 2 seconden en voor de overige 5%, maximaal 5 seconden. Dit geldt niet voor het genereren van rapportages.
- b. De scherm-lay-out is binnen alle gangbare browsers gelijk. Gangbare browsers zijn bijvoorbeeld, maar niet uitsluitend, Microsoft Edge, Mozilla Firefox, Apple Safari en Google Chrome.

### 4. Incidenten en helpdesk

**In de SLA van inschrijver moeten ten aanzien van Incidenten en helpdesk de onderstaande onderwerpen opgenomen en toegelicht zijn.**

1. Kanalen en bereikbaarheid
2. Prioriteitenmatrix
3. Response- en oplostijden
4. Escalatieprocedures

**Bij bovenstaande onderwerpen gelden de volgende minimeisen waaraan de SLA ten aanzien van Incidenten en helpdesk moet voldoen:**

- a. Opdrachtnemer beschikt over een helpdesk voor incidenten, vragen en serviceverzoeken. Deze is voor opdrachtgever ten minste telefonisch, per e-mail en online (via een webbased klantomgeving) beschikbaar.
- b. De gebruikers die daartoe geautoriseerd zijn door opdrachtgever kunnen per e-mail en online 24 uur per dag, 7 dagen per week incidenten melden en serviceverzoeken indienen via deze helpdesk.
- c. De telefonische helpdesk is ten minste beschikbaar op werkdagen tussen 8:00 en 17:00 uur.
- d. De wachttijd voor de telefonische helpdesk is in 90% van de gevallen niet meer dan 5 minuten.
- e. Opdrachtnemer maakt aan de hand van een prioriteitenmatrix inzichtelijk:
  - a. Welke meldingstypen en prioriteiten onderkend worden
  - b. Welke criteria gelden per prioriteit, i.e. hoe prioriteiten worden bepaald
  - c. Welke reactietijden en oplostijden hiermee corresponderen.
  - d. Welke escalatieprocedures gelden als reactie- en oplostijden niet gehaald worden.
  - e. Welke prestatie-indicatoren worden gehanteerd om de eigen serviceverlening te beoordelen
- f. Incidenten, vragen en serviceverzoeken krijgen een datum-tijdstempel en uniek kenmerk welke per e-mail aan de melder wordt teruggekoppeld voor verdere correspondentie.
- g. Door opdrachtgever geautoriseerde medewerkers kunnen in de webbased klantomgeving inzicht krijgen in – en rapportages genereren over - de totale incident- en meldingshistorie van opdrachtgever.
- h. Opdrachtnemer communiceert proactief over zelf geconstateerde incidenten, bugs en andere knelpunten, naar door opdrachtgever aangewezen applicatiebeheerders.
- i. Opdrachtnemer vermeld welke escalatieprocedure geldt en stemt deze af met opdrachtgever, zodat bij aanvang van de overeenkomst over en weer de rollen / functionarissen bekend zijn.

## 5. Service Level Rapportage

**In de SLA van inschrijver moeten ten aanzien van Service Level Rapportage de onderstaande rapportages zijn opgenomen en toegelicht.**

1. Informatiebeveiliging en privacy
  - a. De wijze waarop aan IBP-bewustzijn van medewerkers wordt gewerkt.
  - b. Resultaten van audits t.a.v. fysieke toegangsbeveiliging
  - c. Logging, bescherming tegen manipulatie.
  - d. De wijze van beveiliging van back-up.
  - e. Borging van toegang tot persoonsgegevens medewerkers.
  - f. Versiebeheer: Zijn er patches uitgevoerd en hoe is dit uitgevoerd, zonder dataverlies?
  - g. Versleuteling en cryptografie
  - h. Eventuele manipulatie van logging
  - i. Verwijdering/vernietiging afgeschreven media en gegevensdragers
  - j. Processen voor fysieke toegang, sleutelbeheer.
  - k. Toegepaste AI modellen en aspecten als privacy, bias en beveiliging
2. Beschikbaarheid en continuïteit
  - a. Beschikbaarheidspercentage van het LAS.
  - b. Overzicht van majeure incidenten, oplostijden, gevolgen en maatregelen.
  - c. Eventuele maatregelen ter voorkoming van (majeure) incidenten en om beschikbaarheid te verbeteren.
  - d. Resultaten van tests en oefening van o.a. back-up en herstelprocedures, beheersing van majeure incidenten, RTO en RPO.
3. Performance en gebruikerservaring
  - a. Prestaties t.a.v. de responsetijden van de applicatie en database
  - b. De wijze waarop deze responsetijden worden gemeten.
  - c. Eventuele wijzigingen in browserondersteuning
4. Incidenten en helpdesk
  - a. Overzicht van geregistreerde incidenten, vragen en serviceverzoeken
  - b. Scores op de reactie- en oplostijden uit de prioriteitenmatrix
  - c. Score op de gemiddelde wachttijd voor de telefonische helpdesk
  - d. Eventuele maatregelen om incidentafhandeling en serviceverlening te verbeteren

**Ten aanzien van het Service Level Rapport (SLR) gelden de volgende minimumeisen:**

- a. Inschrijver rapporteert ten minste één keer per jaar aan opdrachtgever over de prestaties ten aanzien van de SLA aan de hand van bovengenoemde rapportages.