Bijlage 7 - Service Level Agreement (SLA)
Thesaurusbeheersysteem

KB, nationale bibliotheek

oktober, 2026

Versie: v0.1
Status: Template t.b.v. aanbesteding
Eigenaar: Servicemanagement KB

Inhoudsopgave

1	Algemeen	4
1.1	Doel	4
1.2	Relatie met andere documenten	4
1.3	Begrippen	4
1.4	Documentbeheer	5
1.5	Looptijd	5
2	Beschrijving van de dienstverlening	5
2.1	De Oplossing en de gebruikers	5
2.2	Servicecatalogus	5
2.3	Uitgangspunten	6
3	Serviceniveaus (KPI's)	6
3.1	Prioriteiten	7
3.2	Reactie-, update- en oplostijden	7
4	Meten en bewaken	7
4.1	Meting	7
4.2	Monitoring	8
4.3	Afwijkingen	8
5	Informatiebeveiliging en continuïteit	8
5.1	Security governance	8
5.2	Assurance	8
5.3	Beveiligingstesten en kwetsbaarheden	9
5.4	Hardening	9
5.5	Patch- en lifecyclemanagement	10
5.6	Security monitoring en beveiligingsincidenten	10
5.7	Back-up, herstel en disaster recovery	10
5.8	Keten van toeleveranciers	11
5.9	Toegang	12
5.10	Privacy en digitale toegankelijkheid	12
6	Rapportage en evaluatie	12
6.1	Servicerapportage	12
6.2	Overige rapportages	12
6.3	Verbeterplan	13
6.4	Serviceoverleg en evaluatie	13
7	Exit	13
8	Bijlagen	14
8.1	Bijlage A. Minimale inhoud van het DAP	14
9	Ondertekening	19

Toelichting bij dit template

- Deze SLA is een template bij de Europese aanbesteding Thesaurusbeheersysteem van de KB, naast het Programma van Eisen (PvE).
- Inschrijver gaat bij de Inschrijving akkoord met dit template.
- De voorlopig winnende Inschrijver werkt op basis van dit template een eerste versie uit. Deze toelichting vervalt in die versie.
- De tekst buiten de haken ligt vast.
- [PvE]: de norm, termijn of frequentie staat in het PvE en wordt daaruit overgenomen. Die ligt vast en staat niet ter discussie.
- [ ]: de voorlopig winnende Inschrijver vult dit in met een voorstel. De invulling behoeft goedkeuring van de KB.
- Een invulling past binnen het PvE en dit template. Deze beperkt geen norm, termijn of verplichting, voegt geen uitzonderingen of voorwaarden toe en verwijst niet naar eigen voorwaarden van de Inschrijver.
- [kenmerk Overeenkomst] vult de KB in.
- Het PvE gaat voor.

Versiebeheer

Versie	Datum	Auteur	Status	Wijzigingen
0.1	21-10-2026	KB Servicemanagement	Template	Template bij de aanbestedingsstukken
[ ]	[ ]	[ ]	[ ]	[ ]

1 Algemeen

1.1 Doel

Deze SLA legt de serviceniveaus vast voor de dienstverlening van Opdrachtnemer aan de KB voor de Oplossing. De SLA vormt samen met het DAP de basis voor rapportage, evaluatie en bijsturing van de dienstverlening. Het DAP beschrijft de procedures en afspraken waarmee de serviceniveaus worden uitgevoerd. Wat het DAP ten minste beschrijft, staat in bijlage A.

1.2 Relatie met andere documenten

Deze SLA hoort bij de Overeenkomst [kenmerk Overeenkomst]. Het PvE gaat voor; de SLA, het DAP en het Exitplan doen geen afbreuk aan het PvE. Bij strijdigheid geldt de rangorde uit de Overeenkomst.

Waar deze SLA naar het DAP verwijst, beschrijft het DAP alleen hoe een verplichting wordt uitgevoerd. Het DAP verlengt geen termijn, verlaagt geen norm en voegt geen voorwaarden toe. Wat het DAP ten minste beschrijft, staat in bijlage A.

1.3 Begrippen

Begrippen met een hoofdletter hebben de betekenis uit het Beschrijvend Document. Daarnaast hebben de begrippen hieronder in dit document de volgende betekenis, ook als deze met een kleine letter worden geschreven:

- Inbeheername: het einde van de implementatiefase, nadat de KB heeft vastgesteld dat aan de voorwaarden voor inbeheername uit het PvE is voldaan;
- Incident: een verstoring van de dienstverlening;
- Reactie, update en opgelost: zoals beschreven in het PvE;
- Materieel of relevant: met mogelijke gevolgen voor de beschikbaarheid, integriteit of vertrouwelijkheid van de dienstverlening aan de KB;
- Workaround: een tijdelijke oplossing voor een incident, zoals bedoeld in het PvE;
- Standaard serviceverzoek: een verzoek uit de lijst met standaard serviceverzoeken in het DAP (bijlage A);
- Wijzigingsverzoek: een verzoek van de KB om een wijziging, waaronder doorontwikkeling zoals een nieuwe koppeling of een nieuwe thesaurus (non-standard change), zoals bedoeld in het PvE;
- Dienst: een afzonderlijk onderdeel van de dienstverlening dat de KB van Opdrachtnemer afneemt (paragraaf 2.2);
- Servicecatalogus: het overzicht van de diensten in paragraaf 2.2;
- Transitieperiode: de periode na het einde van de Overeenkomst waarin Opdrachtnemer op verzoek van de KB de dienstverlening doorlevert tot de overdracht is afgerond, zoals bedoeld in het PvE.

1.4 Documentbeheer

Vaststelling, ondertekening en actualisatie van de SLA volgen het PvE:

- de voorlopig winnende Inschrijver werkt op basis van dit template een eerste versie van de SLA uit;
- de KB en Opdrachtnemer stellen de SLA na gunning en vóór ondertekening van de Overeenkomst vast en ondertekenen deze (hoofdstuk 9, Ondertekening);
- de KB en Opdrachtnemer voeren een review uit van de SLA, samen met het DAP en het Exitplan, met de frequentie [PvE] en daarnaast bij relevante wijzigingen in de dienstverlening;
- een wijziging geldt pas na schriftelijke goedkeuring door de KB en Opdrachtnemer en wordt opgenomen in het versiebeheer;
- bij elke nieuwe versie stellen de KB en Opdrachtnemer vast dat beide over dezelfde versie beschikken.

1.5 Looptijd

De SLA geldt vanaf inbeheername gedurende de looptijd van de Overeenkomst. Levert Opdrachtnemer op verzoek van de KB de dienstverlening door in de transitieperiode, dan blijft de SLA in die periode gelden. Het Exitplan beschrijft de transitieperiode.

2 Beschrijving van de dienstverlening

2.1 De Oplossing en de gebruikers

De Oplossing wordt gebruikt door de KB en de netwerkpartners, elk met eigen processen en koppelingen. De serviceniveaus gelden voor alle onderdelen van de Oplossing, inclusief de beheerinterface, de publieksinterface en alle koppelvlakken.

2.2 Servicecatalogus

De servicecatalogus beschrijft per dienst wat Opdrachtnemer levert. Een dienst is een afzonderlijk onderdeel van de dienstverlening dat de KB van Opdrachtnemer afneemt, bijvoorbeeld de beheerinterface, de publieksinterface, de API en de overige koppelvlakken, de servicedesk en de test- of acceptatieomgeving. Opdrachtnemer neemt elke dienst die de KB afneemt op als aparte regel en houdt de catalogus actueel; een wijziging verloopt via het versiebeheer van deze SLA.

Dienst	Beschrijving	Gebruikers	Servicevenster	Afhankelijkheden
[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]

Het servicevenster per dienst is ten minste het venster [PvE]. Een afhankelijkheid in deze tabel doet geen afbreuk aan de verantwoordelijkheid van Opdrachtnemer voor de gehele Oplossing en aan de serviceniveaus.

2.3 Uitgangspunten

〉 De normen in het PvE vormen de ondergrens voor deze SLA.
〉 Alle serviceniveaus zijn resultaatverplichtingen.
〉 Een wijziging in de dienstverlening doet geen afbreuk aan de serviceniveaus.

3 Serviceniveaus (KPI's)

De tabel geeft per serviceniveau (KPI) de norm en de meetmethode. De norm wordt overgenomen uit het PvE ([PvE]). De meetmethode ([ ]) beschrijft per serviceniveau ten minste het meetpunt, het meetinstrument, de berekening en, bij beschikbaarheid, de registratie van downtime. De meetmethode volgt de definities uit het PvE en de meetperiode [PvE]; uitsluitingen gelden alleen als het PvE deze toestaat.

Serviceniveau	Norm	Meetmethode
Beschikbaarheid	[PvE]	[ ]
Performance API	[PvE]	[ ]
Responstijd user-interface	[PvE]	[ ]
Ondersteuningstijden servicedesk	[PvE]	[ ]
Statusinformatie over de dienstverlening	[PvE]	[ ]
Reactie-, update- en oplostijden incidenten	zie paragraaf 3.2	[ ]
Afhandeling standaard serviceverzoeken	[PvE]	[ ]
Impactanalyse wijzigingsverzoek	[PvE]	[ ]
Voorstel bij verzoek om advies of ondersteuning	[PvE]	[ ]
Voortgangsupdate openstaande verzoeken	[PvE]	[ ]
Oorzaakanalyse	[PvE]	[ ]
Hersteltijd (RTO) en maximaal dataverlies (RPO)	[PvE]	[ ]
Aankondiging van wijzigingen, per soort wijziging	[PvE]	[ ]
Aankondiging van vervallen of verminderde functionaliteit	[PvE]	[ ]
Roadmap	[PvE]	[ ]
Release-informatie	[PvE]	[ ]
Beschikbaarheid testomgeving vóór livegang	[PvE]	[ ]

Serviceniveau	Norm	Meetmethode
Aankondiging en overgangsperiode API-wijzigingen	[PvE]	[ ]
Onderhoud zonder downtime	[PvE]	[ ]
Gepland onderhoud met downtime	[PvE]	[ ]
Spoedonderhoud	[PvE]	[ ]

3.1 Prioriteiten

Incidenten worden ingedeeld in vier prioriteiten op basis van impact en urgentie, volgens het PvE. De KB stelt bij de melding de prioriteit vast. Incidenten die Opdrachtnemer zelf vaststelt, meldt Opdrachtnemer met een voorlopige prioriteit; de KB kan deze prioriteit wijzigen. Het DAP beschrijft de meldroute (bijlage A).

3.2 Reactie-, update- en oplostijden

Voor incidenten gelden de termijnen [PvE], met de definities van reactie, update en opgelost en de tijden waarbinnen de termijnen lopen uit het PvE. De termijnen in de tabel ([PvE]) worden uit het PvE overgenomen.

Prioriteit	Reactie	Update	Opgelost
1	[PvE]	[PvE]	[PvE]
2	[PvE]	[PvE]	[PvE]
3	[PvE]	[PvE]	[PvE]
4	[PvE]	[PvE]	[PvE]

Een workaround stopt de oplostijd alleen als de KB daarmee instemt.

4 Meten en bewaken

4.1 Meting

- Opdrachtnemer meet de serviceniveaus per meetperiode volgens het PvE, met de meetmethode uit hoofdstuk 3.
- Voor de meting van de beschikbaarheid registreert Opdrachtnemer geplande en ongeplande downtime, met begin- en eindtijd en de oorzaak.
- Opdrachtnemer geeft de KB op verzoek inzage in de onderliggende meetgegevens, binnen de termijn [PvE].

4.2 Monitoring

- Opdrachtnemer monitort gedurende de looptijd de beschikbaarheid en de performance van de Oplossing en reageert op afwijkingen die gevolgen kunnen hebben voor de dienstverlening.
- Uitval, performanceproblemen, (Distributed) Denial of Service-aanvallen, onverklaarbaar hoog netwerkverkeer en vergelijkbare gebeurtenissen meldt Opdrachtnemer onmiddellijk aan de KB, volgens het DAP (bijlage A).
- Opdrachtnemer bewaakt de naleving van alle serviceniveaus.

4.3 Afwijkingen

- Uitval en performanceproblemen meldt Opdrachtnemer als incident.
- Afwijkingen van de overige serviceniveaus meldt Opdrachtnemer binnen de termijn [PvE], met de verwachte hersteltijd en de herstelmaatregelen.
- Het DAP beschrijft de meldroute (bijlage A).

5 Informatiebeveiliging en continuïteit

Dit hoofdstuk beschrijft de verplichtingen die voortkomen uit de security-eisen in het PvE. Wat het DAP voor de uitvoering ten minste beschrijft, staat in bijlage A. Waar een frequentie of termijn geldt, staat bij het punt [PvE].

5.1 Security governance

- Opdrachtnemer beschikt gedurende de looptijd over één centraal aanspreekpunt voor informatiebeveiliging en borgt dat de bij de KB bekende contactgegevens van dit aanspreekpunt actueel zijn. Een wijziging van deze contactgegevens geeft Opdrachtnemer tijdig en vooraf door aan de KB.
- Vragen, meldingen en afstemming over informatiebeveiliging lopen via dit aanspreekpunt en worden binnen de organisatie van Opdrachtnemer opgevolgd.
- Opdrachtnemer borgt een gestructureerde aanpak voor informatiebeveiliging, ingericht vergelijkbaar met een ISMS volgens ISO 27001:2022, die aantoonbaar is ingebed in de organisatie en de dagelijkse dienstverlening.
- Opdrachtnemer beoordeelt periodiek de werking en actualiteit van deze aanpak en volgt geconstateerde tekortkomingen en verbetermaatregelen aantoonbaar op.
- Materiële wijzigingen, risico's of tekortkomingen in de informatiebeveiliging die gevolgen kunnen hebben voor de dienstverlening aan de KB, deelt Opdrachtnemer met de KB, volgens het DAP (bijlage A).

5.2 Assurance

- Opdrachtnemer beschikt over de assurance-rapportage of -verklaring uit het PvE, binnen de termijn [PvE], en zorgt voor tijdige vernieuwing daarvan.

- Opdrachtnemer stelt de actuele rapportage of verklaring beschikbaar aan de KB, met de frequentie [PvE]. De scope omvat de aan de KB geleverde dienstverlening en de daarvoor relevante toeleveringsketen.
- Bevindingen, uitzonderingen of beperkingen in de assurance die gevolgen kunnen hebben voor de dienstverlening aan de KB, maakt Opdrachtnemer inzichtelijk en volgt Opdrachtnemer op, volgens het DAP (bijlage A).

5.3 Beveiligingstesten en kwetsbaarheden

- Opdrachtnemer laat alle webapplicaties en API's in scope van de dienstverlening penetratietesten door een gekwalificeerde externe partij, met de frequentie [PvE]. De rapportage stelt Opdrachtnemer op verzoek van de KB beschikbaar.
- Opdrachtnemer voert vulnerability scans uit op de digitale infrastructuur van de dienstverlening, met de frequentie [PvE]. De rapportage stelt Opdrachtnemer op verzoek van de KB beschikbaar.
- Opdrachtnemer beoordeelt de bevindingen van elke test en scan op gevolgen voor de dienstverlening aan de KB, en classificeert, registreert en volgt geconstateerde kwetsbaarheden aantoonbaar op.
- Bevindingen en kwetsbaarheden die een materieel beveiligingsrisico vormen of gevolgen kunnen hebben voor de beveiliging of continuïteit van de dienstverlening, meldt Opdrachtnemer volgens het DAP (bijlage A) en volgt Opdrachtnemer op.
- Opdrachtnemer beoordeelt geïdentificeerde kwetsbaarheden tijdig en verhelpt deze, of mitigeert deze voldoende als direct herstel niet mogelijk is. Kwetsbaarheden waarvoor aanvullende herstelmaatregelen nodig zijn, worden opgenomen in een door de KB geaccordeerd verbeterplan. Opdrachtnemer brengt voor het oplossen van kwetsbaarheden geen aanvullende kosten in rekening en bewaakt de voortgang tot de kwetsbaarheid aantoonbaar is verholpen of voldoende is beheerst.
- Kwetsbaarheden met een hoge prioriteit volgens het PvE behandelt Opdrachtnemer met voorrang. Opdrachtnemer treft onmiddellijk maatregelen om het beveiligingsrisico te beperken, verhelpt de kwetsbaarheid binnen de termijn [PvE] volgens het beveiligingsadvies dat het PvE noemt, en bewaakt de voortgang tot de kwetsbaarheid aantoonbaar is opgelost of voldoende is gemitigeerd. Kan de kwetsbaarheid gevolgen hebben voor de dienstverlening aan de KB, dan meldt Opdrachtnemer deze volgens het DAP (bijlage A).
- Opdrachtnemer rapporteert over de actuele staat en opvolging van kwetsbaarheden als onderdeel van de servicerapportage, met de frequentie [PvE] en de inhoud uit het PvE. De rapportage geeft de KB inzicht in openstaande kwetsbaarheden, de voortgang van herstel- en mitigerende maatregelen en relevante ontwikkelingen in het kwetsbaarheidsbeeld.

5.4 Hardening

- Opdrachtnemer rapporteert over de staat van compliance op hardening als onderdeel van de servicerapportage, met de frequentie [PvE].

5.5 Patch- en lifecyclemanagement

- Opdrachtnemer borgt gedurende de looptijd dat alle voor de Oplossing gebruikte ICT-componenten worden beheerd volgens een gedocumenteerd patchmanagementbeleid en -proces.
- Opdrachtnemer beoordeelt beschikbare patches en updates op beveiligingsrisico, urgentie, impact en toepasbaarheid, beoordeelt vooraf de implementatierisico's en test patches en updates eerst in een niet-productieomgeving.
- Security patches en hotfixes voor kwetsbaarheden met een hoge prioriteit volgens het PvE past Opdrachtnemer met voorrang toe, binnen de termijn [PvE] en volgens het beveiligingsadvies dat het PvE noemt.
- Is er geen geschikte patch of update beschikbaar, dan treft Opdrachtnemer mitigerende maatregelen en bewaakt Opdrachtnemer het restrisico tot een structurele oplossing beschikbaar en geïmplementeerd is.
- Opdrachtnemer borgt een gedocumenteerd lifecyclemanagementproces voor alle componenten van de Oplossing, bewaakt actief de lifecycle- en ondersteuningsstatus en neemt tijdig maatregelen om te voorkomen dat verouderde of niet langer ondersteunde componenten leiden tot risico's voor de beveiliging, continuïteit of juiste werking van de dienstverlening.
- Relevante lifecyclewijzigingen die gevolgen kunnen hebben voor de dienstverlening aan de KB, meldt Opdrachtnemer volgens het DAP (bijlage A) en volgt Opdrachtnemer op.
- Opdrachtnemer gebruikt uitsluitend hard- en softwarecomponenten die actief worden ondersteund door de leverancier of fabrikant, en neemt tijdig maatregelen om te voorkomen dat een component tijdens de dienstverlening out of support of end of life raakt.
- Opdrachtnemer rapporteert over het patchniveau en de lifecyclestatus van de componenten, met de frequentie [PvE]. Nadert een component de status end of support of end of life, dan informeert Opdrachtnemer de KB tijdig en maakt Opdrachtnemer de gevolgen en de voorgenomen maatregelen inzichtelijk.

5.6 Security monitoring en beveiligingsincidenten

- Opdrachtnemer borgt gedurende de looptijd continue security monitoring van alle onderdelen van de Oplossing door een gekwalificeerd Security Operations Centre.
- Securitygebeurtenissen die een risico kunnen vormen voor de beschikbaarheid, integriteit of vertrouwelijkheid van de gegevens in de Oplossing, worden beoordeeld en opgevolgd. Gebeurtenissen die gevolgen kunnen hebben voor de dienstverlening aan de KB meldt Opdrachtnemer onmiddellijk aan de KB, volgens het DAP (bijlage A).
- Een potentieel informatiebeveiligingsincident met impact op data, systemen of medewerkers van de KB meldt Opdrachtnemer onverwijld aan de KB via CSIRT-KB.
- Opdrachtnemer zorgt dat zulke incidenten intern tijdig worden herkend, geclassificeerd en geëscaleerd, en houdt de KB tijdens de afhandeling op de hoogte van relevante ontwikkelingen.

5.7 Back-up, herstel en disaster recovery

- Opdrachtnemer beschikt gedurende de looptijd over een werkende back-up- en herstelvoorziening die voldoet aan de RPO en RTO [PvE].

- Opdrachtnemer controleert de bruikbaarheid, correctheid en volledigheid van de back-ups met de frequentie [PvE], registreert de controles en volgt geconstateerde afwijkingen tijdig op.
- Afwijkingen die de herstelbaarheid of het halen van de RPO of RTO kunnen beïnvloeden, meldt Opdrachtnemer volgens het DAP (bijlage A).
- Opdrachtnemer voert een hersteltest uit met de frequentie [PvE] en stelt daarmee representatief vast of back-ups kunnen worden hersteld binnen de RPO en RTO. Opdrachtnemer documenteert de uitvoering, de resultaten, de afwijkingen en de verbetermaatregelen, en stelt de documentatie op verzoek van de KB beschikbaar.
- Opdrachtnemer stelt in afstemming met de KB een Disaster Recovery Plan op en houdt het actueel. Opdrachtnemer actualiseert het plan bij relevante wijzigingen in de dienstverlening, infrastructuur, keten, herstelvoorzieningen of organisatie.
- Opdrachtnemer test de werking van het Disaster Recovery Plan met de frequentie [PvE]. Neemt de KB deel aan de test, dan wordt de test vooraf met de KB afgestemd. Opdrachtnemer documenteert de test, de resultaten, de tekortkomingen en de verbetermaatregelen, en deelt een gedocumenteerde evaluatie van elke test met de KB.
- De back-upvoorziening voldoet aan de 3-2-1-1-0 regel uit het PvE, inclusief een offline kopie en 0 fouten in geverifieerde back-ups.
- Afwijkingen op deze norm rapporteert Opdrachtnemer als afwijking van een serviceniveau (paragraaf 4.3). Opdrachtnemer herstelt de herstelbaarheid van de betreffende back-up met voorrang en meldt afwijkingen met mogelijke gevolgen voor de RPO of RTO afzonderlijk aan de KB, volgens het DAP (bijlage A).

5.8 Keten van toeleveranciers

- Opdrachtnemer houdt een overzicht bij van de keten van toeleveranciers en deelt dit overzicht met de KB voorafgaand aan de start van de opdracht.
- Opdrachtnemer informeert de KB zodra een wijziging optreedt in de keten van toeleveranciers, volgens het DAP (bijlage A).
- Opdrachtnemer borgt gedurende de looptijd dat de voor de dienstverlening relevante informatiebeveiligingseisen worden doorgelegd aan de betrokken toeleveranciers.
- Verklaart Opdrachtnemer een informatiebeveiligingseis niet van toepassing op een toeleverancier, dan legt Opdrachtnemer de uitsluiting en de onderbouwing aantoonbaar vast en beoordeelt Opdrachtnemer de uitsluiting opnieuw als de dienstverlening, de inzet van de toeleverancier of de risico's wijzigen. Afwijkingen met gevolgen voor de informatiebeveiliging van de dienstverlening deelt Opdrachtnemer met de KB, volgens het DAP (bijlage A).
- Opdrachtnemer bewaakt gedurende de looptijd veranderingen en informatiebeveiligingsrisico's in de keten die gevolgen kunnen hebben voor de dienstverlening aan de KB.
- Relevante wijzigingen, kwetsbaarheden en informatiebeveiligingsincidenten in de keten beoordeelt Opdrachtnemer tijdig op impact voor de dienstverlening aan de KB, en meldt en volgt Opdrachtnemer op volgens het DAP (bijlage A).

5.9 Toegang

〉 Opdrachtnemer houdt bij welke personen namens Opdrachtnemer toegang hebben tot de Oplossing en verstrekt de KB op verzoek een overzicht.
〉 Toegang blijft alleen bestaan zolang die nodig is voor de werkzaamheden.

5.10 Privacy en digitale toegankelijkheid

〉 Voor de verwerking van persoonsgegevens gelden de privacy-eisen uit het PvE en, als die is gesloten, de Verwerkersovereenkomst.
〉 Voor digitale toegankelijkheid gelden de eisen voor digitale toegankelijkheid uit het PvE, inclusief de frequentie van het auditrapport en de rapportage over de verbeterpunten.

6 Rapportage en evaluatie

6.1 Servicerapportage

Opdrachtnemer levert een servicerapportage met de inhoud uit het PvE, de frequentie [PvE] en de termijn [PvE]. Het format van de rapportage leggen de KB en Opdrachtnemer vast in het DAP (bijlage A).

6.2 Overige rapportages

Naast de servicerapportage levert Opdrachtnemer de rapportages in de tabel. De KB bepaalt welke van deze rapportages in de servicerapportage worden opgenomen.

Rapportage	Frequentie
Assurance-rapportage of -verklaring	[PvE]
Rapportage penetratietests en vulnerability scans	op verzoek van de KB
Staat van kwetsbaarheden (onderdeel van de servicerapportage)	[PvE]
Hardening (onderdeel van de servicerapportage)	[PvE]
Patchniveau	[PvE]
Documentatie back-upcontroles en hersteltests	op verzoek van de KB
Evaluatie test Disaster Recovery Plan	[PvE]
Digitale toegankelijkheid: auditrapport	[PvE]
Digitale toegankelijkheid: rapportage verbeterpunten	[PvE]

6.3 Verbeterplan

Haalt Opdrachtnemer een serviceniveau niet, dan levert Opdrachtnemer een verbeterplan volgens het PvE. Het verbeterplan behoeft goedkeuring van de KB. Opdrachtnemer rapporteert over de voortgang in de servicerapportage.

6.4 Serviceoverleg en evaluatie

De KB en Opdrachtnemer voeren serviceoverleg en evalueren de dienstverlening, inclusief de samenwerking met de netwerkpartners, met de frequentie [PvE]. De deelnemers en de werkwijze staan in het DAP (bijlage A). Opdrachtnemer legt de afspraken en verbeterpunten uit elk overleg vast en levert het verslag binnen de termijn [PvE].

7 Exit

De afspraken over beëindiging, overdracht, de transitieperiode en de verwijdering van gegevens staan in het Exitplan.

8 Bijlagen

8.1 Bijlage A. Minimale inhoud van het DAP

Opdrachtnemer levert het DAP aan zoals het PvE beschrijft. Het DAP beschrijft ten minste wat hieronder per onderdeel van deze SLA staat. De KB toetst elke versie van het DAP hieraan. Opdrachtnemer mag het DAP aanvullen, binnen paragraaf 1.2.

Algemeen

- de rollen van de KB en Opdrachtnemer; de contactgegevens per rol staan in een aparte contactenbijlage van het DAP;
- de verantwoordelijkheden, contactpunten, meldroutes en escalatieniveaus, met ten minste een operationeel niveau en een managementniveau;
- een RACI-matrix en de demarcatie van de verantwoordelijkheden van Opdrachtnemer, de KB en, waar van toepassing, de netwerkpartners, ten minste voor de koppelingen en koppelvlakken, de monitoring, het melden en oplossen van incidenten, en het doorvoeren van wijzigingen en releases;
- dat netwerkpartners incidenten en serviceverzoeken melden via het aanspreekpunt van de KB;
- het beheer van accounts en rollen;
- de afhankelijkheden van de koppelingen;
- de procedure bij calamiteiten: wie een calamiteit vaststelt en het herstel start, hoe en bij wie Opdrachtnemer meldt, hoe Opdrachtnemer de KB informeert tot het herstel is afgerond, en hoe Opdrachtnemer de uitkomsten van hersteltests met de KB deelt;
- de operationele uitwerking van de eisen over privacy en digitale toegankelijkheid.

Serviceverzoeken, incidenten en onderhoud (hoofdstuk 1 en 3)

- de lijst met standaard serviceverzoeken;
- de procedures voor incidenten, serviceverzoeken, wijzigingen, releases en onderhoud;
- de meldroute voor incidenten, ook voor incidenten die Opdrachtnemer zelf vaststelt;
- de procedure voor het aankondigen van onderhoud, met de contactpersonen en communicatiekanalen.

Meten, monitoring en afwijkingen (hoofdstuk 4)

- welke onderdelen en indicatoren worden gemonitord;
- de criteria voor signalering en escalatie, en hoe meldingen worden beoordeeld en opgevolgd;
- het communicatiekanaal en de contactpersonen voor meldingen;
- wat een melding ten minste bevat, voor zover op dat moment bekend: de aard en omvang van het incident, de getroffen onderdelen, de mogelijke impact, de getroffen maatregelen en de verwachte vervolgstappen;

- hoe voortgang en herstel worden bewaakt en hoe Opdrachtnemer de KB op de hoogte houdt tot de dienstverlening is hersteld;
- de registratie van geplande en ongeplande downtime voor de meting van de beschikbaarheid (paragraaf 4.1);
- de meldroute voor afwijkingen van de overige serviceniveaus.

Security governance (paragraaf 5.1)

- in de contactenbijlage: de contactgegevens van het centrale aanspreekpunt voor informatiebeveiliging: naam of functie, e-mailadres, telefoonnummer, bereikbaarheid en vervanging bij afwezigheid;
- hoe Opdrachtnemer een wijziging van deze contactgegevens tijdig en vooraf doorgeeft aan de KB en verwerkt in de contactenbijlage;
- hoe de security governance voor de dienstverlening aan de KB operationeel is ingericht: de rollen en verantwoordelijkheden voor informatiebeveiliging; hoe risico's worden geïdentificeerd, beoordeeld en opgevolgd; hoe beveiligingsmaatregelen periodiek worden beoordeeld; hoe tekortkomingen en verbetermaatregelen worden geregistreerd en opgevolgd; hoe wijzigingen in risico's, maatregelen of governance met de KB worden afgestemd; en welke rapportages, controles, audits of andere bewijsstukken de werking aantonen;
- hoe overeengekomen verbetermaatregelen met verantwoordelijken en streefdata worden geregistreerd en gevolgd tot afhandeling.

Assurance (paragraaf 5.2)

- wat Opdrachtnemer bij de assurance-rapportage of -verklaring vermeldt: de verslag- en geldigheidsperiode; de scope; de onderdelen van de dienstverlening buiten de scope; uitzonderingen, bevindingen of tekortkomingen en hun mogelijke impact op de dienstverlening aan de KB; corrigerende maatregelen met verantwoordelijken en geplande opleverdata; en afhankelijkheden van toeleveranciers die in de assurance zijn betrokken of daarvan zijn uitgesloten;
- in welk overleg de KB en Opdrachtnemer materiële bevindingen en de voortgang van corrigerende maatregelen bespreken;
- hoe Opdrachtnemer de KB informeert als de scope, geldigheid of uitkomst van de assurance wezenlijk wijzigt.

Beveiligingstesten en kwetsbaarheden (paragraaf 5.3)

- per penetratietest: de webapplicaties en API's in scope, de datum, de externe partij, de bevindingen en hun classificatie, de mogelijke impact op de dienstverlening aan de KB, de herstel- of mitigerende maatregelen, de verantwoordelijke en de geplande en werkelijke datum van afhandeling;

- per vulnerability scan: de datum, de scope, de gescande componenten, de kwetsbaarheden, de classificatie en waar beschikbaar de CVE-code en CVSS-score, de mogelijke impact en de status van opvolging;
- per kwetsbaarheid: de bron en datum van identificatie, de getroffen component, de classificatie, de mogelijke impact, de gekozen maatregel, de verantwoordelijke, de geplande hersteldatum, de actuele status en de datum waarop de kwetsbaarheid aantoonbaar is verholpen of voldoende gemitigeerd;
- bij een kwetsbaarheid met een hoge prioriteit daarnaast: de CVE-code en CVSS-score, het herstel- of mitigatieadvies, de onmiddellijk getroffen maatregelen en de geplande definitieve herstelmaatregel;
- wat een verbeterplan voor een kwetsbaarheid ten minste bevat: de oorzaak, het risico, de tijdelijke beheersmaatregelen, de definitieve oplossing en de geplande opleverdatum;
- hoe Opdrachtnemer na herstel controleert dat de kwetsbaarheid aantoonbaar is verholpen;
- wat de rapportage over kwetsbaarheden ten minste bevat: het aantal en type kwetsbaarheden, de getroffen componenten, waar beschikbaar de CVE-code, de CVSS-score of prioriteit, de status van de maatregelen, openstaande kwetsbaarheden met de geplande datum van afhandeling, kwetsbaarheden met mitigerende maatregelen of risicoacceptatie, en trends of terugkerende kwetsbaarheden;
- in welk overleg de rapportage en materiële openstaande risico's worden besproken, en hoe vervolgacties worden vastgelegd en gevolgd.

Patch- en lifecyclemanagement (paragraaf 5.5)

- het patchmanagementproces en, per relevante patch of update: de component, de patch, update of hotfix, de datum van beschikbaarheid, de kwetsbaarheid en waar beschikbaar de CVE-code en CVSS-score, de beoordeling van beveiligings- en implementatierisico's, de prioriteit, de test en het resultaat, de geplande en werkelijke implementatiedatum, de verantwoordelijke en eventuele afwijkingen of tijdelijke mitigerende maatregelen;
- wat Opdrachtnemer vastlegt als een patch of update niet binnen de geldende termijn kan worden toegepast: de reden, het restrisico, de mitigerende maatregelen en de vervolgstap;
- per component: de versie, de leverancier of fabrikant, de lifecycle- en ondersteuningsstatus, de bekende end-of-support- en end-of-life-data, opvolgende versies of vervangende componenten, de risico's, de geplande upgrade, migratie, vervanging of uitfasering, de verantwoordelijke en de geplande datum;
- hoe relevante lifecyclewijzigingen, risico's en voorgenomen maatregelen met de KB worden afgestemd voordat deze gevolgen hebben voor de dienstverlening;
- wat de rapportage over het patchniveau ten minste bevat: de componenten en versies, de patch- of updatestatus, openstaande patches en updates, de ondersteuningsstatus, de bekende end-of-support- en end-of-life-data, de componenten waarvoor een upgrade, migratie of vervanging nodig is, de risico's of afwijkingen, en de geplande maatregelen met verantwoordelijken en streefdata;
- in welk overleg deze rapportage wordt besproken.

Security monitoring en beveiligingsincidenten (paragraaf 5.6)

- de operationele inrichting van de security monitoring: welke onderdelen worden gemonitord, de verantwoordelijkheden van het Security Operations Centre, hoe signalen worden gedetecteerd, geanalyseerd en geclassificeerd, de criteria voor escalatie naar de KB, het communicatiekanaal en de contactpersonen, en hoe opvolging en afsluiting worden geregistreerd;
- wat een melding van een securitygebeurtenis ten minste bevat, voor zover op dat moment bekend: de aard, de getroffen onderdelen, de mogelijke impact, de getroffen maatregelen en de verwachte vervolgstappen;
- voor potentiële informatiebeveiligingsincidenten: de criteria voor classificatie, de interne escalatieroute, de contactgegevens en het communicatiekanaal van CSIRT-KB, hoe en hoe vaak vervolgupdates worden gegeven, en hoe maatregelen, besluiten, afsluiting en vervolgacties worden vastgelegd;
- wat de eerste melding van een potentieel informatiebeveiligingsincident ten minste bevat, voor zover op dat moment bekend: de aard en het moment, de betrokken systemen, gegevens of gebruikers, de (mogelijke) impact op de KB, de genomen beheersmaatregelen en de verwachte vervolgstappen.

Back-up, herstel en disaster recovery (paragraaf 5.7)

- welke gegevens, configuraties en overige onderdelen in de back-up zijn opgenomen, de frequentie van de back-ups, de bewaartermijnen, de procedure voor een herstelactie en de rollen en contactpersonen van Opdrachtnemer en de KB bij herstel;
- hoe wijzigingen in de back-upvoorziening die gevolgen kunnen hebben voor de RPO of RTO vóór ingebruikname met de KB worden afgestemd;
- per back-upcontrole: de datum, de gecontroleerde voorziening of set, het resultaat, fouten of afwijkingen, de impact op herstelbaarheid, RPO en RTO, de herstelmaatregelen en de datum waarop de afwijking is opgelost;
- hoe wordt gecontroleerd of aan de 3-2-1-1-0 regel en de norm van 0 fouten wordt voldaan, en per verificatie: het moment, de back-up of set, het resultaat, fouten, de gevolgen voor herstelbaarheid, RPO en RTO, de herstelmaatregel en het moment waarop de back-up weer aantoonbaar bruikbaar is;
- per hersteltest: de datum en scope, de back-up of set, de herstelhandeling, de hersteltijd, het resultaat, afwijkingen ten opzichte van de RPO en RTO, tekortkomingen of risico's, en verbetermaatregelen met verantwoordelijken en streefdata;
- wat het Disaster Recovery Plan ten minste bevat: de scope, wanneer het plan wordt geactiveerd, de rollen, verantwoordelijkheden en bevoegdheden, de escalatie- en communicatieprocedure, de contactpersonen, de herstelvolgorde van kritieke onderdelen, de technische en organisatorische afhankelijkheden, de relatie met de RPO en RTO, en de terugkeer naar de reguliere dienstverlening;
- wanneer het Disaster Recovery Plan wordt beoordeeld, en in welk overleg wijzigingen met gevolgen voor de dienstverlening aan de KB worden besproken;
- hoe de test van het Disaster Recovery Plan in de beheer- of testplanning staat, en wat de KB en Opdrachtnemer vooraf afstemmen als de KB deelneemt: de testmethode, de scope en

doelstelling, het scenario, de rollen en contactpersonen, de datum en duur, de gevolgen voor de dienstverlening en de evaluatie;
- wat de evaluatie van een test van het Disaster Recovery Plan ten minste bevat: de testscenario's, het resultaat, de gerealiseerde hersteltermijnen, afwijkingen of tekortkomingen, de impact op de dienstverlening, en verbetermaatregelen met verantwoordelijken en streefdata;
- hoe materiële tekortkomingen die het halen van de RPO of RTO kunnen beïnvloeden worden besproken en gevolgd tot deze zijn opgelost of door de KB zijn geaccepteerd.

Keten van toeleveranciers (paragraaf 5.8)

- waar het overzicht van de keten van toeleveranciers staat;
- wat een melding van een wijziging in de keten ten minste bevat: de naam van de nieuwe of gewijzigde toeleverancier, de reden, de dienst of functionaliteit, de ingangsdatum, een bevestiging dat de informatiebeveiligingseisen onverminderd van toepassing zijn, en de informatiebeveiligingsrisico's van de wijziging;
- dat Opdrachtnemer het overzicht gelijktijdig met de melding actualiseert;
- per relevante toeleverancier: welke informatiebeveiligingseisen van toepassing zijn, en bij een uitsluiting de eis, de toeleverancier, de reden, de risico's en eventuele compenserende maatregelen;
- bij een verandering, kwetsbaarheid of incident in de keten: de toeleverancier, de aard, de (mogelijke) impact op de dienstverlening aan de KB, de beheersmaatregelen, de vervolgacties en verantwoordelijken, en de status en verwachte datum van afhandeling;
- het communicatiekanaal voor meldingen over de keten, en hoe Opdrachtnemer de KB op de hoogte houdt tot het risico of incident voldoende is beheerst.

Toegang (paragraaf 5.9)

- per persoon met toegang tot de Oplossing: naam of unieke identificatie, organisatie en functie of rol, het toegangsniveau of de omgeving, de datum van toekenning en de datum van wijziging of intrekking;
- hoe Opdrachtnemer het overzicht actualiseert en toegang intrekt als die niet meer nodig is.

Rapportage en overleg (hoofdstuk 6)

- het format van de servicerapportage;
- de deelnemers en de werkwijze van het serviceoverleg en de evaluatie;
- welk overleg wordt gebruikt voor de onderwerpen in deze bijlage waarvoor een overleg wordt genoemd.

9 Ondertekening

De KB en Opdrachtnemer stellen deze SLA vast en ondertekenen deze. Met ondertekening bevestigen de KB en Opdrachtnemer ook dat beide over dezelfde versie beschikken.

Voor akkoord

Details	Akkoord KB	Akkoord Opdrachtnemer
Document status	[ ]	[ ]
Plaats	[ ]	[ ]
Naam	[ ]	[ ]
Functie	[ ]	[ ]
Datum van ondertekening	[ ]	[ ]
Handtekening		