Bijlage 8: Minimale eisen voor de SLA bij de aanbesteding SIS voor Rijn IJssel

Doel: contractueel toetsbare minimumeisen voor een bedrijfskritische SaaS-/SIS-dienst, inclusief beschikbaarheid, incidenten, continuïteit, beveiliging, privacy, integraties, releases en exit.

Document	Waarde
Versie	Def
Datum	30 oktober 2026
Opdrachtgever	Rijn IJssel
Classificatie SIS	Bedrijfskritisch/kritieke onderwijs- en bedrijfsvoering
Toepassing	Productieomgeving en alle voor productie noodzakelijke diensten, koppelingen en beheercomponenten

1. Doel, reikwijdte en uitgangspunten

Deze bijlage legt de minimale Service Level Agreements (SLA), serviceprocessen en continuïteitseisen vast die gelden voor de levering van het Studentinformatiesysteem (SIS) aan Rijn IJssel. De eisen zijn minimumeisen: een inschrijver mag een hoger serviceniveau aanbieden, maar niet lager.

- De SLA geldt voor de volledige end-to-end dienstverlening die nodig is om het SIS te gebruiken, inclusief hosting/cloud, databases, authenticatiecomponenten voor zover door leverancier geleverd, API's, batchverwerking, portalen, beheerfuncties en door leverancier beheerde integratiecomponenten.
- De leverancier blijft verantwoordelijk voor onderaannemers en subverwerkers alsof het eigen dienstverlening betreft.
- Gepland onderhoud telt alleen buiten de beschikbaarheidsberekening wanneer het vooraf is aangekondigd, binnen het afgesproken onderhoudsvenster valt en de maximale onderhoudsduur niet wordt overschreden.
- Een storing in een kritische ketenfunctie kan als P1 worden geclassificeerd, ook wanneer de SIS-interface zelf technisch bereikbaar is.
- Servicelevels worden per kalendermaand gemeten, tenzij bij een eis anders vermeld. Rapportage vindt minimaal per kwartaal plaats; P1/Major Incidents worden afzonderlijk gerapporteerd.

2. Serviceclassificatie en prioriteitsmodel

Voor het SIS geldt serviceklasse SL1: bedrijfskritisch. De prioriteit wordt bepaald op basis van impact én urgentie. Rijn IJssel heeft het recht de prioriteit gemotiveerd te verhogen wanneer onderwijscontinuïteit, wettelijke termijnen, examens, inschrijving, bekostiging of gegevensuitwisseling in het geding zijn.

Prioriteit	Definitie	Voorbeelden
P1 - Kritiek	Volledige uitval of ernstige verstoring van een kernproces; geen werkbare workaround; grote groep gebruikers of wettelijke/onderwijskritische deadline geraakt.	Inschrijving onmogelijk; centrale gegevensuitwisseling geblokkeerd; autorisatieprobleem met brede datatoegang; massale foutieve gegevensverwerking.
P2 - Hoog	Belangrijke functionaliteit of ketenfunctie uitgevallen; aanzienlijke groep gebruikers geraakt; tijdelijke workaround beperkt mogelijk.	Kritische koppeling valt uit; mutaties worden niet verwerkt; specifieke locatie/cluster kan kernproces niet uitvoeren.
P3 - Midden	Deelverstoring met beperkte impact; kernproces kan met workaround doorgaan.	Rapportagefunctie of niet-kritische batch vertraagd; beperkte functionele fout.
P4 - Laag / verzoek	Vraag, service request, cosmetische fout of wijzigingsverzoek zonder directe bedrijfsimpact.	Informatieverzoek, kleine configuratiewijziging, gebruikersvraag.

3. Beschikbaarheid, servicevenster en onderhoud

ID	Eis / minimumnorm	Meetwijze / bewijs
SLA-01	Productie-SIS en bedrijfskritische API's/koppeldiensten zijn 24x7 beschikbaar. De gemeten beschikbaarheid bedraagt minimaal 99,9% per kalendermaand, exclusief toegestaan gepland onderhoud.	Maandelijkse beschikbaarheidsrapportage met meetpunten, duur, oorzaak en uitgesloten onderhoud.
SLA-02	Tijdens kernservicetijd op werkdagen 07:00-19:00 uur bedraagt de beschikbaarheid minimaal 99,95%.	Meten per kalendermaand.
SLA-03	Voor vooraf aangewezen piek- en blackoutperioden (o.a. start schooljaar, inschrijf-/bekostigingsmomenten, examen- en diplomaperioden) mag geen regulier gepland onderhoud plaatsvinden.	Jaarlijkse kalender gezamenlijk vaststellen; afwijking alleen na schriftelijk akkoord Rijn IJssel.
SLA-04	Regulier gepland onderhoud wordt minimaal 10 werkdagen vooraf aangekondigd; impact, duur, rollback en contactpunt zijn beschreven.	Change-/onderhoudskalender.
SLA-05	Spoedonderhoud wegens een aantoonbaar acuut beveiligings- of continuïteitsrisico mag met kortere aankondiging, mits Rijn IJssel direct wordt geïnformeerd en impactbeperking wordt toegepast.	Incident/change-registratie.
SLA-06	De leverancier meet beschikbaarheid end-to-end vanuit gebruikersperspectief; alleen infrastructuur-uptime is onvoldoende.	Meetmethodiek en onafhankelijke/controleerbare meetgegevens beschikbaar.

4. Incidentmanagement en ondersteuning

De basis uit het aangeleverde document - 24x7 bereikbaarheid voor kritische meldingen, prioriteitsafhankelijke oplostijden en een Major Incident Report - is behouden, maar aangescherpt met responstijd, hersteldoel en communicatiefrequentie.

ID	Eis / minimumnorm	Meetwijze / bewijs
INC-01	P1: meldpunt 24x7 bereikbaar. Eerste menselijke respons binnen 15 minuten; gekwalificeerde behandeling start direct; workaround/hersteldoel binnen 2 uur; volledig serviceherstel streefwaarde binnen 4 uur.	Ticket- en tijdstempelrapportage. Norm: ≥95% per maand voor respons/hersteldoel.
INC-02	P2: eerste respons binnen 30 minuten tijdens 07:00-19:00 uur op werkdagen; behandeling binnen 1 uur; herstel/workaround binnen 8 uur.	≥95% per maand.
INC-03	P3: eerste respons binnen 4 kantooruren; oplossing of geaccepteerd plan binnen 2 werkdagen.	≥90% per maand.
INC-04	P4: eerste respons binnen 1 werkdag; afhandeling conform overeengekomen servicecatalogus/backlog.	≥90% per maand.
INC-05	Bij P1 communiceert leverancier minimaal elke 30 minuten status, impact, acties, verwachte hersteltijd en eerstvolgende update; bij P2 minimaal elke 2 uur zolang de verstoring voortduurt.	Communicatielog in MIR/SLR.
INC-06	P1/Major Incident Report uiterlijk binnen 5 werkdagen na herstel; bevat tijdlijn, root cause, impact, getroffen gegevens/ketens, genomen acties, structurele verbetermaatregelen, eigenaar en deadline.	100% van P1-incidenten.
INC-07	Bij herhaalde incidenten of structurele normoverschrijding wordt kosteloos een Problem Record/RCA gestart en een verbeterplan opgeleverd.	Trendrapportage; minimaal bij 2 vergelijkbare P1/P2's in 90 dagen of 3 maanden SLA-onderschrijding.

5. Continuïteit, back-up, restore en disaster recovery

ID	Eis / minimumnorm	Meetwijze / bewijs
CON-01	Voor productiegegevens geldt een Recovery Point Objective (RPO) van maximaal 15 minuten voor transactionele SIS-data, tenzij Rijn IJssel voor een specifieke dataset een andere waarde accepteert.	Architectuur-/back-upbeschrijving en periodieke restoretest.
CON-02	Recovery Time Objective (RTO) voor een calamiteit bedraagt maximaal 4 uur voor de kern-SIS-dienst en kritische gegevensverwerking.	DR-testresultaat; ≥95% van tests/incidenten binnen norm.
CON-03	Back-ups zijn logisch en organisatorisch gescheiden van de productieomgeving, beschermd tegen ongeautoriseerde wijziging/verwijdering en passend bestand tegen ransomware-scenario's. immutable backup	Auditbewijs, architectuur en herstelprocedure.
CON-04	Leverancier voert minimaal jaarlijks een volledige disaster-recoverytest uit en minimaal elk kwartaal een aantoonbare restoretest op representatieve gegevens.	Testrapport met bevindingen en verbeteracties binnen 20 werkdagen.

CON-05	Rijn IJssel ontvangt minimaal jaarlijks een continuïteitsrapport met afhankelijkheden, uitwijklocaties/regio's, single points of failure, RTO/RPO en testresultaten.	Jaarlijkse rapportage.
CON-06	Bij langdurige uitval levert leverancier op verzoek een actuele export van essentiële gegevens of een vooraf afgesproken noodvoorziening zodat kritieke onderwijs-/administratieprocessen zo veel mogelijk kunnen doorgaan.	BCP/noodprocedure en jaarlijkse validatie.

6. Performance, capaciteit en schaalbaarheid

ID	Eis / minimumnorm	Meetwijze / bewijs
PER-01	Minimaal 95% van interactieve gebruikersacties heeft bij normale belasting een server-/applicatieresponstijd ≤2 seconden; minimaal 99% ≤5 seconden, exclusief aantoonbare externe afhankelijkheden buiten leveranciersverantwoordelijkheid.	APM-rapportage per maand; meetdefinitie vooraf vastleggen.
PER-02	Kritische batch- en ketenprocessen worden binnen overeengekomen tijdvensters afgerond. Overschrijding wordt proactief gemeld voordat een onderwijs- of wettelijke deadline geraakt wordt.	Batchmonitoring en SLR.
PER-03	Leverancier voert capaciteitsmanagement uit en schaalt tijdig op. Groei van gebruikers, transacties en API-verkeer binnen overeengekomen bandbreedtes mag niet leiden tot degradatie onder de SLA.	Kwartaalrapport capaciteit/trends.
PER-04	Voor grote releases en proces kritische periodes voert leverancier aantoonbaar performance-/loadtests uit op representatieve scenario's en geen downscalen tijdens die periodes	Testrapport en acceptatiecriteria.

7. Informatiebeveiliging en cyberweerbaarheid

ID	Eis / minimumnorm	Meetwijze / bewijs
SEC-01	Leverancier beschikt gedurende de contractduur over een passend, onafhankelijk getoetst ISMS, bij voorkeur ISO/IEC 27001 of aantoonbaar gelijkwaardig. Scope omvat de aangeboden SIS-dienst en relevante beheerprocessen.	Geldig certificaat/auditrapport en scope.
SEC-02	Leverancier sluit aan op de voor Rijn IJssel geldende beveiligingskaders en actuele NCSC-richtlijnen voor veilige software, webapplicaties, API's en TLS, voor zover van toepassing.	Compliance-matrix en periodieke assurance.
SEC-03	MFA is verplicht voor beheer- en privileged accounts. Voor eindgebruikers ondersteunt de dienst federatieve authenticatie/SSO en sterke authenticatie conform Rijn IJssel-beleid.	Technische documentatie en acceptatietest.
SEC-04	Autorisatie ondersteunt fijnmazige rol- en rechtenstructuren moet de toepassing van de AVG in onze organisatiestructuur ondersteunen, least privilege, functiescheiding en periodieke recertificatie van rechten.	RBAC/ABAC-documentatie, auditlog.
SEC-05	Alle data in transport is versleuteld met actuele veilige TLS-configuratie; gevoelige data at rest is versleuteld met passend sleutelbeheer.	Configuratie-/auditbewijs.

SEC-06	Beveiligingslogging omvat minimaal authenticatie, autorisatiewijzigingen, privileged handelingen, bulkexport, mutaties en lezen van kritieke gegevens en beveiligingsgebeurtenissen. Logs zijn tijdgesynchroniseerd, integer en exporteerbaar naar SIEM.	Logcatalogus, retentie en testexport.
SEC-07	Kritieke kwetsbaarheden met aantoonbare exploitatie of zeer hoog risico worden zo spoedig mogelijk gemitigeerd, streefwaarde ≤24 uur; overige kritieke kwetsbaarheden ≤72 uur; hoge kwetsbaarheden ≤14 dagen, tenzij gemotiveerd risicobesluit.	Vulnerability-/patchrapportage.
SEC-08	Minimaal jaarlijks en na majeure architectuurwijzigingen wordt een onafhankelijke penetratietest uitgevoerd. Kritieke bevindingen worden vóór productie opgelost of aantoonbaar gemitigeerd.	Samenvatting pentest en opvolgplan.
SEC-09	Leverancier heeft een CVD/responsible-disclosureproces en een 24x7 security-incidentcontact.	Beleid/contactgegevens.
SEC-10	Leverancier beheert supply-chainrisico's, houdt zicht op kritieke onderaannemers/subverwerkers en meldt materiële wijzigingen vooraf.	Leveranciers-/subverwerkersoverzicht en wijzigingsprocedure.

8. Privacy, gegevensbescherming en datalocatie

ID	Eis / minimumnorm	Meetwijze / bewijs
PRV-01	Leverancier verwerkt persoonsgegevens uitsluitend in opdracht van Rijn IJssel en conform AVG, verwerkersovereenkomst en gedocumenteerde instructies.	Verwerkersovereenkomst en privacydocumentatie.
PRV-02	Productiegegevens en back-ups worden uitsluitend verwerkt/opgeslagen inclusief eigenaar binnen de EER, tenzij Rijn IJssel vooraf schriftelijk instemt met een andere rechtmatige inrichting.	Datacenter-/subverwerkersoverzicht.
PRV-03	Nieuwe subverwerkers en materiële wijzigingen worden minimaal 30 dagen vooraf gemeld, inclusief locatie, taak, gegevenscategorieën en relevante waarborgen.	Wijzigingsregister.
PRV-04	Leverancier ondersteunt Rijn IJssel bij verzoeken van betrokkenen, DPIA's, audits en onderzoeken van toezichthouders binnen redelijke, vooraf afgesproken termijnen.	Procesbeschrijving.
PRV-05	Een (mogelijk) datalek of beveiligingsincident met persoonsgegevens wordt onverwijld en uiterlijk binnen 4 uur na vaststelling bij Rijn IJssel gemeld, met doorlopende actualisering van beschikbare feiten.	Incidentprocedure en communicatielog.
PRV-06	Dataretentie en verwijdering zijn configureerbaar conform Rijn IJssel-beleid en wettelijke bewaartermijnen; verwijdering omvat kopieën/back-ups en actuele data, niet alleen backup en kopieën volgens gedocumenteerde lifecycle.	Retentie-/deletionbeleid.
PRV-07	Productiedata mag niet worden gebruikt voor generatieve AI, modeltraining, productverbetering of andere secundaire doeleinden zonder voorafgaande expliciete schriftelijke toestemming van Rijn IJssel.	Contractuele verklaring en technische/organisatorische borging.

9. Integraties, API's en ketenverantwoordelijkheid

Voor Rijn IJssel is het SIS geen geïsoleerd systeem maar een kerncomponent in een breder onderwijs- en applicatie-ecosysteem. Daarom worden koppelingen en gegevensuitwisseling expliciet onderdeel van de SLA.

ID	Eis / minimumnorm	Meetwijze / bewijs
INT-01	Leverancier biedt gedocumenteerde, versieerbare en beveiligde API's/koppelvlakken voor overeengekomen gegevens en processen. Documentatie is actueel en toegankelijk voor Rijn IJssel en geautoriseerde ketenpartners.	API-documentatie/OpenAPI of gelijkwaardig.
INT-02	Wijzigingen die bestaande koppelingen kunnen breken worden minimaal 6 maanden vooraf aangekondigd, tenzij een acute beveiligingsreden dit onmogelijk maakt. Er is een deprecation- en migratiepad.	Release-/API-roadmap.
INT-03	Kritische API's vallen onder dezelfde beschikbaarheids- en incident-SLA als het SIS. API-fouten, wachtrijen en mislukte berichten zijn actief gemonitord en traceerbaar.	Monitoringdashboard/SLR.
INT-04	Berichtenverwerking is waar passend idempotent, herstartbaar en voorzien van foutafhandeling/retry; geen stille gegevensverliezen.met dus een logging/journal	Technisch ontwerp en ketentest.
INT-05	Leverancier ondersteunt de voor het mbo relevante wettelijke/sectorale gegevensuitwisselingen en standaarden die binnen scope vallen, inclusief wijzigingen daarvan binnen wettelijke termijnen.	Roadmap, releaseplanning en conformiteitstest.
INT-06	Voor koppelingen met o.a. DUO/RIO en overige afgesproken ketenpartners wordt end-to-end monitoring en ketenincidentafhandeling ingericht, met één coördinerend aanspreekpunt bij leverancier voor diens deel van de keten.	Keten-SLA/procesbeschrijving.
INT-07	Rijn IJssel kan eigen data zonder additionele vendor lock-in via API en periodieke bulkexport ontsluiten voor geautoriseerde toepassingen, rapportage en datawarehouse/BI.	Acceptatietest en exportformaten.

10. Change-, release- en lifecyclemanagement

ID	Eis / minimumnorm	Meetwijze / bewijs
CHG-01	Leverancier onderhoudt een actuele releasekalender en deelt minimaal kwartaalvooruitblik en jaarroadmap.	Releasekalender.
CHG-02	Majeure releases worden minimaal 8 weken vooraf aangekondigd; release notes, impactanalyse, testinformatie en eventuele beheer-/gebruikersimpact zijn beschikbaar.	Release dossier.
CHG-03	Rijn IJssel beschikt over een representatieve acceptatie-/testomgeving. Majeure wijzigingen zijn daar minimaal 4 weken vóór productie beschikbaar, tenzij anders overeengekomen.	Omgevingsplanning.
CHG-04	Elke productiechange heeft een risico-/impactanalyse en rollback- of herstelplan. Bij mislukte release kan leverancier gecontroleerd terug naar een werkende toestand.	Change record.

CHG-05	Niet-standaard wijziging: impactanalyse inclusief kosten en doorlooptijd binnen maximaal 10 werkdagen; uitvoering conform gezamenlijk goedgekeurde planning.	≥95% binnen norm.
CHG-06	Security-, wet- en regelgeving- en sectorstandaardwijzigingen die noodzakelijk zijn om de dienst compliant te houden worden tijdig ingepland en mogen niet leiden tot onvoorzien verlies van kernfunctionaliteit.	Roadmap/compliance-overleg.
CHG-07	End-of-life/end-of-support van relevante functionaliteit, API of technologie wordt minimaal 12 maanden vooraf aangekondigd met migratiepad, tenzij externe urgentie aantoonbaar een kortere termijn vereist.	Lifecyclebericht en migratieplan.
CHG-08	Alle courante browsers worden ondersteund en devices met een backwards compatibality zolang de leverancier van die browser de ondersteuning faciliteert	browserversie

11. Servicelevelrapportage, monitoring en governance

ID	Eis / minimumnorm	Meetwijze / bewijs
GOV-01	SLR wordt minimaal 4x per jaar uiterlijk binnen 5 werkdagen na afloop van het kwartaal geleverd en bevat minimaal: beschikbaarheid, incidenten, responstijden, herstel, performance, changes, securitypatches, back-up/restore, capaciteit, API/koppelingen, problemen, klachten en verbeteracties.	100% tijdige rapportage.
GOV-02	Rijn IJssel krijgt toegang tot actuele statusinformatie en bij voorkeur een service/statusdashboard voor beschikbaarheid en verstoringen.	Dashboard/portal.
GOV-03	Tactisch serviceoverleg minimaal per kwartaal; strategisch overleg minimaal jaarlijks. Bij structurele SLA-afwijking kan Rijn IJssel tijdelijk een hogere overlegfrequentie verlangen.	Verslagen en actie-/besluitenlijst.
GOV-04	KPI-definities, meetbron, meetperiode, uitzonderingen en berekeningswijze worden vóór start dienstverlening gezamenlijk vastgesteld en mogen niet eenzijdig worden gewijzigd.	Meetplan.
GOV-05	Leverancier voert jaarlijks een klantgerichte service improvement review uit met trends, risico's, technische schuld, lifecycle, innovatie en concrete verbetermaatregelen.	Jaarplan/service improvement plan.

12. Auditrechten, assurance en compliance

ID	Eis / minimumnorm	Meetwijze / bewijs
AUD-01	Rijn IJssel ontvangt jaarlijks relevante assurance-informatie, certificeringen en managementsamenvattingen van audits die de SIS-dienst betreffen.	Jaarlijkse oplevering.
AUD-02	Rijn IJssel of een door haar aangewezen onafhankelijke auditor heeft, met redelijke aankondiging en rekening houdend met multi-tenant beveiliging, recht op aanvullende audit bij gegronde aanleiding.	Contractuele bepaling.

AUD-03	Materiële auditbevindingen worden voorzien van risico, maatregel, eigenaar en oplosdatum. Kritieke bevindingen worden direct geëscaleerd.	Verbeterplan.
AUD-04	Leverancier meldt verlies/schorsing van relevante certificering of een materiële non-conformiteit onverwijld aan Rijn IJssel.	Meldprocedure.

13. Exit, dataportabiliteit en continuïteit bij einde contract

ID	Eis / minimumnorm	Meetwijze / bewijs
EXT-01	Rijn IJssel blijft te allen tijde eigenaar/rechthebbende van de eigen gegevens. Leverancier oefent geen retentierecht uit op data.	Contractuele bepaling.
EXT-02	Bij einde overeenkomst levert leverancier alle Rijn IJssel-data, inclusief relevante historie, referentiedata, documenten/bijlagen, auditinformatie en noodzakelijke metadata, in open en gedocumenteerde formaten.	Exitplan en proefexport.
EXT-03	Minimaal jaarlijks wordt een volledige of representatieve data-export technisch gevalideerd zodat exporteerbaarheid niet pas bij exit wordt ontdekt.	Jaarlijkse test.
EXT-04	Leverancier verleent gedurende een overeengekomen transitieperiode redelijke exit- en migratieondersteuning en waarborgt continuïteit totdat overdracht is voltooid.	Exitplan met rollen, tarieven en doorlooptijden.
EXT-05	Na schriftelijke bevestiging van succesvolle migratie verwijdert leverancier resterende Rijn IJssel-data volgens overeengekomen termijnen en verstrekt een vernietigingsverklaring.	Verwijderingsverklaring.
EXT-06	Essentiële configuratie-, datamodel-, API- en exportdocumentatie blijft gedurende contract en exit beschikbaar zodat migratie naar een opvolgend SIS uitvoerbaar is.	Documentatieregister.

14. Servicecredits, escalatie en structurele tekortkoming

Voor een bedrijfskritisch SIS adviseert dit eisendocument om naast herstelverplichtingen ook contractuele consequenties op te nemen. De exacte financiële staffel kan in de overeenkomst worden ingevuld.

ID	Eis / minimumnorm	Meetwijze / bewijs
ESC-01	Overschrijding van een SLA leidt minimaal tot een corrigerende maatregel en, bij herhaling of ernstige afwijking, een formeel service improvement plan.	Procedure in overeenkomst.
ESC-02	P1, structurele beschikbaarheidstekorten, herhaald missen van RTO/RPO of ernstige security-/privacytekortkomingen kennen een directe managementescalatie.	Escalatiematrix.
ESC-03	Servicecredits/boetes mogen nooit de verplichting vervangen om de dienst te herstellen, oorzaken weg te nemen en schade te beperken.	Contractuele bepaling.
ESC-04	Bij herhaalde materiële tekortkoming behoudt Rijn IJssel passende contractuele rechten, waaronder aanvullende assurance, herstel op kosten leverancier en - conform hoofdovereenkomst - beëindigingsrechten.	Contractuele bepaling.

15. Samenvattende KPI-set voor beoordeling en contractering

Domein	Kernnorm
Beschikbaarheid	99,9% per maand 24x7; 99,95% tijdens kernservicetijd
P1 respons	≤15 minuten, 24x7
P1 workaround/hersteldoel	≤2 uur; volledig herstel streefwaarde ≤4 uur
P2 respons	≤30 minuten binnen servicevenster
RTO calamiteit	≤4 uur
RPO transactionele SIS-data	≤15 minuten
P1 communicatie	Elke 30 minuten
MIR	≤5 werkdagen na herstel
Performance	95% interactieve acties ≤2 sec; 99% ≤5 sec
Restoretest	Minimaal per kwartaal
Disaster-recoverytest	Minimaal jaarlijks
Pentest	Minimaal jaarlijks + na majeure architectuurwijziging
SLR	4x per jaar, ≤5 werkdagen na kwartaal
API breaking change	≥6 maanden vooraf
Major release	≥8 weken vooraf; testomgeving ≥4 weken
End-of-life	≥12 maanden vooraf
Datalek/security-incident persoonsgegevens	Onverwijld, uiterlijk binnen 4 uur na vaststelling
Exit/proefexport	Minimaal jaarlijks technisch valideren

Aanbestedingsinstructie aan inschrijver

Wij gaan ervan uit dat elke leverancier een eigen SLA heeft die als kritische applicatie bij een ROC alle genoemde onderwerpen in zich heeft en verwacht dat de eisen die hier genoemd zijn als minimum ingebed zijn. Graag willen wij van de leverancier weten of dit zo is en als dat niet is waar de afwijking zit via de nota van inlichtingen.

Antwoordveld	Toe te passen door inschrijver
Voldoet?	Ja / Nee
Leveringsvorm	Standaard / Configuratie / Maatwerk
Toelichting	Max. 250 woorden
Meetwijze	Bron, meetpunt, frequentie
Bewijs	Certificaat, rapport, referentie of demonstratie
Afhankelijkheden/uitsluitingen	Volledig benoemen
Kosten	Inbegrepen / meerprijs, conform prijsblad