

1. Migratie

Beschrijf uw migratieplan voor de dienstverlening bij aanvang van het contract. Geef de migratiekosten aan per migratieactiviteit. Deze kosten worden niet meegewogen in de prijsvergelijking. De dienstverlening moet uitgevoerd worden over alle te beheren Hardware. Beschrijf per migratieactiviteit de gevolgen voor Opdrachtgever met aandacht voor de tijdsinvestering van de kant van het personeel van Opdrachtgever. Houd hierbij rekening met alle in de aanbestedingsleidraad gestelde eisen.

Belangrijke punten, die in het migratieplan naar voren moeten komen zijn de volgende:

- Migratieactiviteiten
- Wijze van toetsen van de migratieactiviteiten
- Mitigatiemaatregelen
- Een planning
- Risico's en maatregelen
- Gegarandeerde rimpelloze migratie
- Benodigde inzet van andere partijen (Opdrachtgever of leveranciers)
- Kosten van de migratie

2. Security/privacy

Beschrijf hoe u de informatiebeveiliging, privacy en continuïteit van de dienstverlening voor SALTO aantoonbaar waarborgt. De volgende zaken moeten in ieder geval aan de orde komen:

- inrichting en periodieke toetsing van technische en organisatorische beveiligingsmaatregelen;
- MFA, least privilege, beheeraccounts en periodieke autorisatiereviews;
- logging, monitoring en detectie van verdachte activiteiten;
- kwetsbaarheden-, patch- en configuratiemanagement;
- back-up, herstel, restore-tests, BCP en disaster recovery;
- melding, opvolging en evaluatie van beveiligingsincidenten en vermoedelijke datalekken;
- ondersteuning bij audits en het actuele IBP Normenkader Funderend Onderwijs;
- omgang met subverwerkers en opslag of verwerking van persoonsgegevens;
- aanlevering van auditinformatie en bewijsstukken;
- verbetermaatregelen wanneer beveiligingseisen of normenkaders niet worden gehaald.

Beschrijf tevens een concreet scenario waarin een beheerdersaccount mogelijk is gecompromitteerd, welke acties u in de eerste uren uitvoert, wanneer en hoe u SALTO informeert en welke bewijsmateriaal, analyses en verbetermaatregelen u na afloop oplevert. SALTO verlangt onder andere aantoonbare back-up- en herstelmaatregelen, jaarlijkse restore-tests, actuele BCP- en DRP-documentatie en melding van security-incidenten of vermoedelijke datalekken uiterlijk binnen twaalf uur na constatering. Ook worden periodieke beveiligingscontroles, herstelplannen en risicogebaseerde hersteltermijnen verlangd.

3. Wijzigingen

Alle wijzigingen die binnen het gestelde in het Programma van Eisen vallen, beschouwt Opdrachtgever als Standaard Wijziging. Geef uw definitie van een Niet-Standaard wijziging. Beschrijf vanuit deze definitie wat de procedure is, de doorlooptijd en wat de tarieven zijn per uur op senior-, medior- en juniorniveau. Geef ook aan voor welke activiteiten de verschillende niveaus worden ingezet. Prijzen worden niet meegewogen in de prijsvergelijking.

4. Beheer van devices

Beschrijf hoe u het dagelijkse technische beheer van de apparaten, identiteiten en platformomgevingen van SALTO uitvoert. De volgende zaken moeten in ieder geval aan de orde komen:

- beheer van Windows-apparaten en iPads via Microsoft Intune;
- beheer van Chromebooks via Google Workspace for Education;
- beheer van Microsoft 365, Entra ID, Conditional Access, Defender en Autopilot;
- geautomatiseerde provisioning en deprovisioning vanuit AFAS, ParnasSys en Basispoort;
- patching, softwaredistributie en controle op de veiligheid van applicaties;
- beheer van rollen, rechten, uitzonderingen, serviceaccounts en beheerdersaccounts;
- ondersteuning van gedeelde apparaten en jonge leerlingen;
- monitoring van compliance en afwijkingen;
- afhandeling van defecte, verloren, vervangen en uit dienst genomen apparaten;
- wijze waarop SALTO aantoonbaar inzicht en hoofdbeheerrechten behoudt;
- KPI's en rapportages waarmee de kwaliteit van het beheer wordt aangetoond.

6. Incidentafhandeling, SLA en regie als SPoC

Beschrijf hoe u 24/7 als Single Point of Contact de volledige regie voert over incidenten, serviceverzoeken, problemen en wijzigingen, inclusief meldingen waarbij een derde leverancier betrokken is. De volgende zaken moeten in ieder geval aan de orde komen:

- registratie, classificatie, prioritering en opvolging van meldingen;
- bewaking van reactie- en oplostijden;
- aanpak van prioriteit 1-, 2- en 3-incidenten;
- communicatie met de melder, SALTO en betrokken leveranciers;
- eigenaarschap wanneer een melding wordt doorgezet naar een derde;
- vastlegging van ticketnummers, acties, afspraken, terugkoppelingen en escalaties;
- escalatie bij dreigende overschrijding van een serviceniveau;
- probleemmanagement en structurele aanpak van herhaalde incidenten;
- rapportage over behaalde en niet-behaalde SLA's;
- maatregelen wanneer een afgesproken serviceniveau niet wordt gehaald.

7. Exitstrategie en Transitieondersteuning

De opdrachtnemer dient gedurende de volledige contractperiode een actuele exitstrategie te onderhouden en bij beëindiging van de overeenkomst volledige medewerking te verlenen aan de overdracht van dienstverlening, kennis, systemen, configuraties, documentatie en beheeractiviteiten aan opdrachtgever en/of een opvolgende opdrachtnemer.

Beschrijf concreet hoe u aan deze eis gaat voldoen, ook als u geen commercieel belang meer hebt.