EA Oracle/Linux DBMS en KVM

Bijlage 1. bij Concept Overeenkomst

Versie: 1.0
Datum: 18 april 2025
TenderNed: 515661

SVHW
Rijksstraatweg 3b
Postbus 7059
3286 ZH Klaaswaal
www.svhw.nl
(0186) 57 72 00

Bijlage B1: Checklist ICT-Kwaliteitsnormen GIBIT 2023 i.z. Oracle/Linux DBMS beheer en KVM

Deze checklist vormt een bijlage bij de Overeenkomst tussen Opdrachtgever en Leverancier voor de implementatie en het beheer van Oracle/Linux DBMS-omgevingen. Deze checklist is gebaseerd op de ICT-Kwaliteitsnormen bij GIBIT (versie maart 2020) en aangevuld met vereisten uit relevante nationale en Europese regelgeving (zoals AVG, NIS2, BIO).

1. Beveiliging (informatiebeveiliging & privacy)

☐ Leverancier werkt aantoonbaar conform de BIO (Baseline Informatiebeveiliging Overheid) en ISO/IEC 27001.

☐ Alle gegevens worden versleuteld opgeslagen en verzonden (encryptie in transit en at rest).

☐ Logging en monitoring zijn ingericht conform GIBIT 2023 en detecteren afwijkingen en incidenten.

☐ Een verwerkersovereenkomst is opgesteld en ondertekend.

☐ Leverancier hanteert een gevalideerde procedure voor de detectie en melding van eventuele datalekken en heeft een uitgewerkte incidentmanagement procedure in gebruik conform AVG en BIO.

2. Continuïteit

☐ Er is een uitgewerkt exitplan inclusief overdracht van data, kennis en documentatie, conform Overeenkomst.

☐ Back-up en recovery procedures zijn beschreven en getest.

☐ SLA's waarborgen beschikbaarheid in overeenstemming met het belang van de te leveren ICT Prestatie (bijv. 99,9% uptime).

☐ Er is een plan voor disaster recovery en business continuity afgestemd op het de eisen en wensen van Opdrachtgever.

3. Transparantie & eigendom

☐ Opdrachtgever behoudt te allen tijde volledige eigendomsrechten op te verwerken data.

☐ De Leverancier biedt inzage in configuraties, versies en installatiescripts indien gewenst.

☐ Alle wijzigingen worden gelogd en zijn traceerbaar via een changelog of CMDB.

4. Beheer & onderhoud

☐ Patchmanagement is aantoonbaar ingericht met tijdige installatie van beveiligingsupdates conform en in overeenstemming met de eisen die door de oorspronkelijke leverancier worden gesteld (Oracle).

☐ Gebruik van ondersteunde Enterprise Linux-distributies (bijv. Oracle Linux, RHEL).

☐ Updates en upgrades van Oracle-databases zijn gepland en getest voor livegang.

☐ De leverancier beschikt over een actueel CMDB en beheerdocumentatie in het Nederlands.

5. Open standaarden & interoperabiliteit

☐ Koppelvlakken maken gebruik van open standaarden volgens het principe van 'pas toe of leg uit' (Forum Standaardisatie).

☐ Data-uitwisseling (bijv. met belastingapplicaties) gebruikt overeengekomen standaarden (bijv. STUF, RGBZ).

☐ Documentatie van interfaces en koppelingen is beschikbaar en actueel.

6. Toegankelijkheid & bruikbaarheid

☐ Beheertools zijn toegankelijk voor bevoegde medewerkers van Opdrachtgever (gebruiksvriendelijk en Nederlandstalig).

☐ Rapportages over prestaties, storingen en wijzigingen zijn beschikbaar voor de Opdrachtgever.

☐ Leverancier biedt selfservice mogelijkheden voor melding van incidenten, werking dashboards en statusinformatie.

7. Wet- en regelgeving

☐ Leverancier houdt zich aan de AVG, NIS2, EU Cybersecurity Act en Archiefwet.

☐ Leverancier staat jaarlijkse controle/audit op naleving van bovenstaande normen (met rapportage aan Opdrachtgever) door een door Opdrachtgever aan te wijzen daartoe gekwalificeerde partij .

☐ Toepassing van BIO-profiel, dat van toepassing is de op de organisatie van Opdrachtgever, is aantoonbaar gemaakt in technische en organisatorische maatregelen.