

Bijlage 6h Cloudbeleid (eis 117) bij 1^e NvI

Aanbesteding Personeels- en SalarisAdministratie (PSA) 2023 Kenmerk 2021-046219

In onderstaande tabellen staan de eisen van de gemeente Waalwijk ten opzichte van Cloud dienstverlening.

Algemeen

Nr.	Omschrijving
1.	De leverancier beschikt over een gecertificeerd (ISO27001 of vergelijkbaar) Informatie Beveiliging Management Systeem (ISMS), gerelateerd aan de te leveren diensten.
2.	De leverancier levert controleerbaar bewijs van de opzet, bestaan en werking van een passend stelsel van beveiligingsmaatregelen volgens een algemeen erkende overheidsnorm ten aanzien van het geheel van de te leveren dienst(en).
3.	De gemeente Waalwijk heeft het recht de door de leverancier geleverde dienst en bijbehorende processen te auditen, deze audit door een derde partij te laten uitvoeren en de statutaire rechten van de auditors te benoemen.
4.	De gemeente Waalwijk blijft eigenaar van alle data die hij binnen de Cloud verwerkt en/of opslaat.
5.	De fysieke systemen, programmatuur en gegevens staan en blijven in de Europese Economische Ruimte (EER).
6.	In het geval van een (dreigend) beveiligingsincident onderneemt de leverancier alle acties die noodzakelijk zijn om het risico voor de gemeente Waalwijk tot een minimum te beperken en meldt deze onmiddellijk aan de gemeente Waalwijk conform de procedurebeschreven in de standaard Verwerkersovereenkomst van Waalwijk.

Applicatie en koppelingen

Nr.	Omschrijving
7.	De leverancier heeft aantoonbaar maatregelen ingevoerd om de kans dat informatie kan worden onderschept tijdens transport/overdracht door onbevoegden te minimaliseren.
8.	Bij transport van informatie over onbetrouwbare netwerken (zoals het internet) is encryptie toegepast.
9.	Communicatie tussen de Private Cloud en Public Clouds vindt uitsluitend plaats via binnen de DMZ ¹ aangeboden webservices. Deze koppelingen moeten gecertificeerd zijn.
10.	Gegevensuitwisseling tussen vertrouwde en niet vertrouwde zones dient inhoudelijk geautomatiseerd gecontroleerd te worden op aanwezigheid van malware.
11.	De leverancier mag bij het verwerken van de gegevens alleen derden inschakelen met wie hij een schriftelijke overeenkomst heeft gesloten waarin geheimhoudings- en beveiligingsverplichtingen zijn opgenomen welke minimaal gelijkwaardig zijn aan het afgesproken beveiligingsniveau tussen de leverancier en Waalwijk.
12.	Bij SaaS-diensten wijkt de digitale identiteit (de user-id) niet af van die binnen de Private Cloud. Het beheer van toegangsrechten, inclusief de bewaking van functie-scheiding, geschiedt vanuit één (logisch) identiteit management systeem zonder hulp van de leverancier (zero-coding).

¹ Een demilitarized zone (DMZ) is een netwerksegment dat zich tussen het interne en externe netwerk bevindt. Het externe netwerk is meestal het internet. Een DMZ is feitelijk een gedeelte van het netwerk dat voor de buitenwereld volledig toegankelijk is maar wel beveiligd wordt door firewall.

Nr.	Omschrijving
13.	Bij het inloggen in een SAAS oplossing via een willekeurige internetverbinding wordt dit minimaal afgedwongen met behulp van een tweetraps-authenticatie.
14.	De leverancier heeft aantoonbaar maatregelen ingevoerd ten behoeve van sterke user authenticatie voor toegang tot gegevens
15.	De leverancier toont aan dat: • de organisatiegegevens logisch en functioneel zijn gescheiden van de overige afnemers. Een logische en functionele scheiding wordt gegarandeerd; • er geen afhankelijkheid bestaat van andere afnemers in geval van: ◦ onderhoud- en releasewerkzaamheden; ◦ technische uitwijk; • de performance niet lijdt onder de piekbelastingen door andere afnemers van de infrastructuur; • de schaalbaarheid en flexibiliteit niet worden beperkt.
16.	Op basis van voorspellingen van het gebruik wordt actie genomen om tijdig de benodigde uitbreiding van capaciteit te bewerkstelligen. Gemeente Waalwijk wordt hier tijdig over geïnformeerd.
17.	De leverancier waarborgt dat de oplossing niet meer dan één major versie achterloopt ('neerwaartse compatibiliteit') op de open standaarden van het Forum Standaardisatie en de landelijke standaarden.
18.	Aanvullende eisen gemeente Waalwijk (maatwerk per keer): • printen vanuit de oplossing op lokale printers moet zonder problemen mogelijk zijn • authenticatie verloopt via de Active Directory Federation Services (ADFS² van de gemeente Waalwijk. Na authenticatie via de Active Directory, hebben gebruikers door middel van Single Sign On (SSO) direct toegang tot alle onderdelen van de aangeboden Oplossing, uiteraard voor zover ze daartoe zijn geautoriseerd.

Informatiebeheer

Nr.	Omschrijving
19.	De oplossing beschikt over een niet-muteerbare audit-trail zodat van elke van de onderstaande handelingen bekend is wie, wanneer en waar deze is uitgevoerd. — Raadplegen; • Creëren / toevoegen; • Wijzigen; • Verwijderen; • Archiveren; • Vernietigen / Overdragen.
20.	De gemeente Waalwijk krijgt toegang tot de audit-trail.
21.	De logbestanden uit de audit-trail (zie bovenstaand punt) worden gedurende minimaal twee jaar bewaard.
22.	De leverancier kan te alle tijden aantonen dat de logbestanden uit de bovengenoemde audit-trail na afgesproken periode zijn verwijderd.
23.	De leverancier beschikt over een gedegen back-up en recoverybeleid betreffende de omgang met en afhandeling van (beveiliging)incidenten. Gemeente Waalwijk kan op verzoek inzage krijgen in het plan.
24.	De leverancier draagt ten behoeve van migratie naar een andere oplossing, mogelijke verwerking door een ander systeem of beëindiging van contract altijd alle data (inclusief meta-data) uit de oplossing, kosteloos, over aan de gemeente. Dit in een origineel en een duurzaam bestandsformaat (conform standaarden van Forum Standaardisatie Rijksoverheid). Na bevestiging van overdracht wordt alle data van de systemen van de leverancier vernietigd in overleg en met goedkeuring van de gemeente Waalwijk. De leverancier levert een verklaring van vernietiging.
25.	Eisen van de gemeente t.o.v. conversie van gegevens: • data moet in een open standaard formaat (conform standaarden van Forum Standaardisatie Rijksoverheid) aangeboden worden.

² Active Directory Federation Services (ADFS) een softwarecomponent om gebruikers te voorzien van eenmalige aanmelding voor systemen/applicaties die over organisatorische grenzen liggen.



Licentie, overeenkomsten en dienstverlening

Nr.	Omschrijving
26.	Beschrijving van basispakket en aanvullende (optionele) diensten en de daarvoor gehanteerde tarieven dient vooraf helder te zijn.
27.	Bij afname van Clouddiensten zijn er voor beide partijen (de leverancier en de gemeente Waalwijk) eenduidige aanspreekpunten.
28.	Software licenties (van wie zijn deze en mogen deze in een Cloud worden gebruikt) dienen vooraf helder te zijn
29.	De looptijd van het contract, verlengingsopties en opzegtermijnen zijn vooraf helder
30.	Er dienen duidelijke afspraken te zijn over de inhoud van rapportages en de periodes van aanleveren
31.	Personen in dienst van of werkzaam voor de leverancier zijn verplicht tot geheimhouding met betrekking tot gegevens van Waalwijk waarvan zij kennis kunnen nemen. De leverancier heeft met hen contractuele geheimhouding geregeld.
32.	De respectievelijke aansprakelijkheden van de partijen die bij de overeenkomst zijn betrokken, zijn contractueel vastgelegd.
33.	Bij verwerking persoonsgegevens dient er een verwerkingsovereenkomst te zijn tussen leverancier (verwerker) en gemeente. De leverancier gaat akkoord met de voorgestelde verwerkersovereenkomst door de gemeente Waalwijk.
34.	De leverancier gaat ermee akkoord dat de Gemeentelijke inkoopvoorwaarden bij IT (GIBIT) van toepassing zijn.
35.	De duurzaamheid van de oplossing is gegarandeerd als de oplossing niet langer ondersteund wordt door de leverancier. Hierbij wordt de broncode (open source, escrow) beschikbaar gesteld of bestaat de mogelijkheid om het onderhoud en de ondersteuning voort te zetten bij een andere partij (exclusief de Inschrijver en zuster-, dochter- en moedermaatschappijen).
36.	Het beoogde serviceniveau en onaanvaardbare serviceniveaus zijn in de SLA beschreven.
37.	Op basis van het afgesloten contract garandeert de leverancier dat de oplossing, gedurende de contractperiode, doorontwikkeld zal worden zonder additionele kosten. Onder deze doorontwikkeling wordt, naast additief, correctief en preventief, ook verstaan dat op de oplossing adaptief onderhoud wordt uitgevoerd om te blijven voldoen aan geldende wet- en regelgeving.
38.	Iedere wijziging (change) met een hoge impact wordt door de leverancier aan de gemeente Waalwijk ter beoordeling voorgelegd en waar mogelijk voorzien van een alternatief voorstel en/of een overzicht van mitigerende maatregelen, inclusief een indicatie van de tijdelijkheid van afwijking (gedoogsituatie).

Op verzoek van de gemeente Waalwijk moeten door de leverancier onderstaande stukken kunnen worden aangeleverd:

- Bewijs van de opzet, bestaan en werking van een passend stelsel van beveiligingsmaatregelen zoals certificering, periodieke externe controles zoals audits of TPM's, assurance rapport met conclusies over de bevindingen van de auditor.
- Auditbeleid
- Exitbeleid
- Service Level Overeenkomst
- Beschrijving van de wijze van user authenticatie (gebruikersnaam/wachtwoord / etc.) en aan welke specifieke eisen dit moet voldoen
- Wijziging/Releasebeleid leverancier
- Back-up en recoverybeleid
- Implementatieplan conform de eisen die de GIBIT daaraan stelt (zie artikel 5.3 van de GIBIT)

