



Bijlage J ICT-randvoorwaarden

Behorende bij de aanbesteding “financiële SaaS-applicatie”

Omschrijving van de ICT architectuur en uitgangspunten van de gemeente Bodegraven-Reeuwijk

Inhoudsopgave

Globale beschrijving ICT-Architectuur	3
Algemene uitgangspunten	3
Netwerk en internet	4
Server, Storage en Backup	4
Werkplek	4
Applicatiesoftware	5
Kantoorautomatisering / O365	5
Data integratie	6
Data ontsluiting	6
Beveiliging	6
Exit	6

Globale beschrijving ICT-Architectuur

Algemene uitgangspunten

Gemeente Bodegraven-Reeuwijk verwacht van nieuwe applicaties die door meerdere gebruikers worden gebruikt en voorzien zijn van een centrale opslag (database) de volgende algemene kenmerken:

- Web-based en te gebruiken in Edge of andere Chromium gebaseerde browser;
- Gehost/aangeboden wordt vanuit de datacenters van de applicatieaanbieder;
- Beveiligd met moderne technologie waarbij de aanbieder voor de applicatie en onderliggende componenten (netwerken, datacenter, etc) een geldige ISO27001 certificaat behoud gedurende de looptijd van de overeenkomst waarbij de scope alle componenten in scope heeft. Op verzoek een TPM verklaring als onderdeel van de BIO van de gemeente kan afgeven;
- Gebruikmakend van standaarden die zijn voorgeschreven door Forum Standaardisatie;
- Applicaties worden aangeboden vanuit een Citrix omgeving;
- Applicaties worden via Intune (Microsoft Endpoint Security) aangeboden op laptops;
- Applicaties behoeven *geen* verbinding met het LAN maar kunnen rechtstreeks op een veilige wijze vanuit een laptop connectie maken met centrale componenten;
- Applicaties worden up-to-date gehouden door de leverancier en gebruikt worden in combinatie met de laatste (GA-versies) van Windows en Office indien hier een afhankelijkheid mee bestaat;
- Autorisaties kunnen granulair worden toegepast. Als centrale directory wordt Azure Active Directory gebruikt. De web-applicatie kan hier als enterprise-app op aangesloten worden;
- Logging van gebruikers en systeemhandelingen voldoen aan de NEN7513 in het geval van persoonlijke gezondheidsgegevens en algemene CRUD logging voor overige gegevens;
- Data kan (volledig) ontsloten worden naar het datawarehouse van de gemeente middels ODBC of API koppelingen;
- De gemeente een sterke voorkeur heeft voor open technologieën maar de leverancier in alle gevallen alle centrale componenten (waaronder ook de gebruikte database technologieën) integraal onderdeel laat zijn van haar aanbod en ervoor zorgt dat deze up-to-date blijven gedurende de looptijd van de overeenkomst.

Meer in detail komen hierboven beschreven elementen terug in de rest van dit document.

Gemeente Bodegraven-Reeuwijk verwacht duidelijk en overzichtelijke documentatie voor gebruikers, applicatiebeheer, data-analisten, werkplekbeheer. Systeembeheer van de applicatie en onderliggende componenten worden belegd bij de leverancier, hier wordt geen documentatie over verwacht.

Gemeente Bodegraven-Reeuwijk heeft op dit moment nog 2 datacenters met een beperkte centrale omgeving en is deze wordt actief uitgefaseerd door middel van het verder inzetten van SaaS, ASP of een andere methode van hosting van applicaties.

Netwerk en internet

Vanwege het gedecentraliseerde, hybride werkplekconcept is er geen directe afhankelijkheid van het lokale (IP) netwerk.

Waar het koppelvlakken betreft op applicatiegebied lopen deze waar mogelijk via Gemnet en digikoppelingen en neemt de gemeente hiervoor de Makelaar en Cliq af van PinkRoccade (als Cloud-service) en dient hiermee geconnecteerd te worden. Zie hiervoor de relevante paragrafen in dit document.

Vanwege het decentrale hybride werkplekconcept mag er niet uit worden gegaan van een centrale internetverbinding. Gemeente Bodegraven-Reeuwijk houdt zelf aan dat iedere medewerker zelf een (consumenten) internet verbinding heeft of biedt als alternatief een 4G hotspot via de telefoon aan. In de centrale locaties van de gemeente wordt gebruik gemaakt van een 200Mbps symmetrische internetverbinding.

Server, Storage en Backup

Vanwege de uitvraag van een SaaS ligt de verantwoordelijkheid van het leveren van servers en storage bij de aanbieder waarmee de gewenste performance wordt geleverd beschreven in het programma van eisen. De gemeente heeft hierbij een voorkeur voor het gebruik van open technologie maar laat de uiteindelijke keuze van de platformen aan de aanbieder.

De verantwoordelijkheid voor het (consistent) uitvoeren van de back-up ligt bij de leverancier. Gemeente Bodegraven-Reeuwijk houdt hiervoor de volgende specificaties aan:

- RTO: 12 uur (de RTO mag ingevuld worden middels een functioneel werkende workaround);
- RPO: 1 uur.

Minstens 1x per jaar wordt er een consistentiecontrole gedaan van de back-up die functioneel wordt gecontroleerd door de gemeente.

Werkplek

De gemeente biedt de medewerker 2 platformen aan (situatie per 2021):

- Citrix XenApp 7.6 (LTSR) desktop;
- Windows 10 Laptops (builds volgens de reguliere MS updatecycli).

De Citrix-omgeving wordt in stand gehouden zolang niet iedere applicatie middels een moderne SaaS aangeboden wordt. Van de nieuw te implementeren applicaties wordt verwacht dat deze direct via de beheerde laptops kunnen worden gebruikt.

Beheer van de laptop vindt plaats via MS Endpoint Protection (Intune) vanuit Azure. Voor webapplicaties is daarnaast binnen het Azure platform Conditional Access ingebouwd zodat vanuit niet beheerde werkplekken de toegang tot webapplicatie gelimiteerd of geblokkeerd is.

Om dit mogelijk te maken dient de toegang tot de applicatie te lopen via de Microsoft Azure Active Directory (AAD), ook wel een enterprise-app genoemd.

Op de werkplek is toegang tot centrale opslag binnen Office 365 (Sharepoint/Teams en Onedrive). Toegang tot printfunctionaliteit is mogelijk door het koppelen van lokale printers. De gemeente voert in 2021 een aanbesteding uit via GT-Print voor het vervangen van de centrale print/scanomgeving op de centrale locaties. Hiervan mag worden uitgegaan dat er een Cloud Print en Scanservice beschikbaar zal zijn voor de gebruiker op de laptop en binnen Citrix.

Er wordt op de laptop geen verbinding gemaakt met het LAN van de gemeente noch is toegang direct mogelijk tot een centrale fileserver omgeving.

Gebruikers hebben geen installatie/adminrechten op de werkplekken. De gemeente is voornemens per 2021 applocker te implementeren om het starten van vreemde executables te voorkomen. De leverancier heeft een overzicht welke componenten behoren tot de geleverde applicatie.

Applicatiesoftware

Alle applicatiesoftware dient web gebaseerd te zijn. In uitzonderlijke gevallen kunnen voor specifieke functionaliteiten ook lokale componenten worden toegevoegd, de leverancier specificeert deze componenten en beschrijft ook op welke wijze interactie met andere applicaties wordt geïsoleerd (bijvoorbeeld de noodzaak tot een specifieke versie van JRE mag op geen enkele manier invloed hebben op de bestaande applicaties die ook JRE gebruiken).

Applicatiecomponenten worden middels MS Endpoint Protection waar nodig geïnstalleerd op laptops, de leverancier levert hiervoor ondersteuning.

Ten behoeve van de Citrix-omgeving dienen eventuele software componenten geschikt te zijn voor gebruik in een Shared-Usage (RDSH) omgeving. Citrix is geïmplementeerd op een Windows 2019 platform en volgt de reguliere updatecyclus van Microsoft.

Voor softwarecomponenten die geïnstalleerd dienen te worden is het aan de applicatieleverancier om een versie aan te bieden die formeel ondersteunt wordt door eventueel derde-partijen (zoals de eerder genoemde JRE versie).

Applicatie houden een eventuele cache buiten de browser bij in het lokale profiel van de gebruiker. Gebruikers hebben *geen* local admin rechten, dit is ook niet noodzakelijk voor het draaien van webapplicatie.

Kantoorautomatisering / O365

De kantoorautomatiseringsomgeving is gebaseerd op Office 365. Dat wil zeggen dat deze zowel binnen Citrix als op de laptops permanent is voorzien van de meest actuele versie.

Gemeente Bodegraven-Reeuwijk is in het bezit van de volgende Office 365 licenties (per Q1-2021):

- E3 + EMS;
- ATP P1;
- AD P1.

De gemeente heeft nog een hybride omgeving maar de leverancier dient rekening te houden met:

- De Azure Exchangeserver heeft geen standaard SMTP relay meer. Mail vanuit de applicatie dient via een eigen oplossing, via de sendgrid omgeving van de gemeente of via een Azure Exchange koppelvlaak plaatsvinden.
- De Azure Active Directory is voor SaaS-applicatie het centrale AIM platform waarop MFA en Conditional Access is geïmplementeerd. De Applicatie dient gebruik te maken van dit authenticatieplatform.

Data integratie

Gemeente Bodegraven-Reeuwijk hanteert het principe “eenvoudige registratie meervoudig gebruik”. Om dit te bewerkstelligen wordt er waar mogelijk gewerkt met gestandaardiseerde gestructureerde koppelingen.

De gemeente maakt hierbij voor Stuf en landelijke voorzieningen gebruik van de enterprise servicebus oplossing van PinkRoccade (makelaar) in combinatie van Cliq.

Koppelingen worden via een veilige verbinding gerealiseerd met de verschillende (SaaS-)applicaties.

In de separaat opgenomen Bijlage L staan de huidige en verwachte koppelvlakken.

Data ontsluiting

Gemeente Bodegraven-Reeuwijk is gestart met het meer centraal beschikbaar stellen van data uit het informatielandschap. Zij maakt hierbij steeds meer gebruik van PowerBi. Gegevens worden, afhankelijk van de applicatie, direct uit de database ontsloten of middels een ETL in een centrale omgeving beschikbaar gesteld. Doelstellingen van de dataontsluiting zijn meerledig:

- Data-analyse over domeinen heen, retrospectief en prospectief;
- Centraal overzicht voor gebruikers over de verschillende (PIOFACH) domeinen.

Gemeente Bodegraven-Reeuwijk wenst van alle applicaties:

- Transparante toegang tot alle data van de gemeente met exporteer mogelijkheden;
- Toegang is op basis REST API's of rechtstreekse ODBC (ODBC heeft vanuit security oogpunt geen voorkeur) of periodieke (instelbare) datadump naar een hotfolder.

De leverancier levert bij een dataexport een bestand op met relevante delta's ten opzichte van de laatst uitgevoerde (structurele) export.

Leverancier levert een datamodel op van de geëxporteerde gegevens of een beschrijving van de REST API.

Beveiliging

Gemeente Bodegraven-Reeuwijk moet voldoen aan de BIO. Voor SaaS-applicaties dienen aanbieders een ISO27001 te hanteren voor alle aangeboden componenten. Voor eventuele onderaannemers wordt deze eis doorgezet (er wordt geen gebruik gemaakt van een Himalaya-clausule).

Volledigheidshalve worden de volgende kenmerken bij de leverancier neergelegd:

- Beveiliging/veiligheid van eigen personeel (incl. VOG vereisten voor medewerkers);
- Beveiliging van bedrijfsmiddelen inclusief beveiliging van laptops en andere voorzieningen van engineers is onderdeel van de het beveiligingsbeleid van de dienstleverancier en wordt actief nageleefd;
- Toegangscontrole tot gegevens van de gemeente Bodegraven-Reeuwijk zijn ten alle tijden afgeschermd met behulp van Multi-Factor authenticatie;
- Alle verbindingen van en naar de data van de gemeente zijn door middel van moderne cryptografische methodes afgeschermd;
- Back-end en front-end systemen worden actief bewaakt en beschermd tegen IoC's;
- Back-up, Restore en disaster recovery wordt periodiek getest op werking;
- Er is een actief managementsysteem rondom informatiebeveiliging en in de risico-analyse worden de systemen/processen/mensen die onderdeel zijn van de aangeboden dienst meegenomen (ISMS conform ISO27001).

Exit

Alle door gemeente Bodegraven-Reeuwijk ingevoerde data kan worden opgeleverd bij het beëindigen van de overeenkomst. Dit wordt opgeleverd in een voor machines leesbaar formaat (zoals XML) inclusief een beschrijving van de structuur.