

Bijlage L - Beschrijving ICT architectuur en uitgangspunten

Deze bijlage beschrijft het burgerzaken / BRP applicatielandschap en de globale ICT infrastructuur waarin de nieuwe SaaS-applicatie opgeleverd dient te worden.

Burgerzaken / BRP applicatielandschap

Gemeente Etten-Leur hanteert voor de aanschaf van applicatiesoftware het principe: SaaS, tenzij.... Daarbij is het streven om applicaties direct met elkaar te koppelen en gegevens tussen applicaties geautomatiseerd uit te wisselen in de daarvoor bestemde koppelstandaarden. Als dat niet mogelijk is, dan is het alternatief het handmatig kunnen uploaden van bestanden die volgens eens afgesproken format uit de aanbiedende applicatie worden geëxporteerd. De i-architectuur visualisatie in bijlage K – Burgerzaken / BRP applicatielandschap architectuur laat zien hoe de nieuw aan te schaffen burgerzaken / BRP SaaS-applicatie gepositioneerd dient te worden in het huidige applicatielandschap van specifiek de gemeente Etten-Leur. In de visualisatie zijn de interne en externe applicaties opgenomen die een (in-)directe relatie hebben met de Burgerzaken / BRP SaaS-applicatie.

ICT-Architectuur

Gemeente Etten-Leur heeft het technisch-beheer, systeembeheer en werkplekbeheer ondergebracht in de Gemeenschappelijke Regeling ICT West-Brabant West (ICTWBW). ICTWBW voorziet o.a. de Gemeente Etten-Leur van een complete technische infrastructuur. Functioneel beheer van de nieuw aan te schaffen Burgerzaken / BRP SaaS-applicatie wordt in eigen beheer gedaan. De functioneel beheerder is werkzaam bij de Gemeente Etten-Leur.

Uitgangspunten

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

1. Web-based en te gebruiken in Edge of andere Chromium gebaseerde browser.
2. Gehost/aangeboden wordt vanuit de datacenters van de applicatieaanbieder.
3. Beveiligd met moderne technologie waarbij de aanbieder voor de applicatie en onderliggende componenten (netwerken, datacenter, etc) een geldige ISO27001 of vergelijkbare certificering behoud gedurende de looptijd van de overeenkomst waarbij de scope alle componenten in scope heeft. Op verzoek een Third Party Mededeling (TPM verklaring) als onderdeel van de Baseline Informatiebeveiliging Overheid (BIO) van de gemeente kan afgeven.
4. Gebruikmakend van standaarden die zijn voorgeschreven door Forum Standaardisatie.
5. Applicaties kunnen worden gebruikt vanuit een Citrix omgeving én vanaf de lokale werkplek van de gebruiker via een browser;
6. Applicaties worden via Intune (Microsoft Endpoint Security) aangeboden op laptops, tablets en smartphones.
7. Applicaties behoeven geen verbinding met het LAN maar kunnen rechtstreeks op een veilige wijze vanuit een mobile device connectie maken met centrale componenten.
8. Applicaties worden up-to-date gehouden door de leverancier en gebruikt worden in combinatie met de laatste General Availability (GA) versies van Windows en Office indien hier een afhankelijkheid mee bestaat.
9. Autorisaties kunnen granulair worden toegepast. Als centrale directory wordt Azure Active Directory (AAD) gebruikt. De web-applicatie kan hier als enterprise-app op aangesloten worden.

10. Logging van gebruikers en systeemhandelingen voldoen aan de NEN7513 in het geval van persoonlijke gezondheidsgegevens en algemene Create, Read, Undo en Delete (CRUD) logging voor overige gegevens.
11. Data kan volledig ontsloten worden naar het datawarehouse (Azure dataplatform) van de gemeente middels Open DataBase Connectivity (ODBC) of Application Programming Interface (API) koppelingen.
12. 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.

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

Netwerk, internet en gegevensdistributie

Er is geen directe afhankelijkheid van het lokale Internet Protocol (IP) netwerk vanwege het gedecentraliseerde, hybride werkplekconcept. Waar het koppelvlakken betreft op applicatiegebied lopen deze waar mogelijk via Gemnet en digikoppelingen en neemt de gemeente hiervoor de gegevensmakelaar Key2Datadistributie van Centric en 2Secure Gateway / 2Orchestrate ESB van Enable-U af en dient hiermee geconnecteerd te worden.

Vanwege het decentrale hybride werkplekconcept mag er niet uit worden gegaan van een centrale internetverbinding. Gemeente Etten-Leur houdt zelf aan dat iedere medewerker zelf een (consumenten) internet verbinding heeft of biedt als alternatief een hotspot via de telefoon aan.

Server, Storage en Backup

Vanwege de uitvraag van een SaaS applicatie 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.

De volgende specificaties worden hier voor aangehouden:

- Recovery Time Objective (RTO): 12 uur. De RTO mag ingevuld worden middels een functioneel werkende workaround.
- Recovery Point Objective (RPO): 1 uur.

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

Werkplek

Aan medewerkers worden momenteel 2 platformen aangeboden:

1. Citrix
2. Windows 10/11 Laptops

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. Bij het inregelen hiervan werkt de applicatieleverancier samen met de CISO, de functioneel beheer M365 en ICTWBW. Op de werkplek is toegang tot centrale opslag binnen Office 365 (Sharepoint/Teams en Onedrive).

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 Java Runtime Environment (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 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.

Applicaties 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 / M365

De kantoorautomatiseringsomgeving is gebaseerd op Microsoft365. Dat wil zeggen dat deze zowel binnen Citrix als op de laptops permanent is voorzien van de meest actuele versie.

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

- Mail vanuit de applicatie dient via een eigen oplossing of via een Azure Exchange koppelvlak plaats te vinden.
- De Azure Active Directory (AAD) is voor SaaS-applicatie het centrale platform waarop Multi-Factor authenticatie (MFA) en Conditional Access is geïmplementeerd. De applicatie dient gebruik te maken van dit authenticatieplatform.

Data integratie

Gemeente Etten-Leur hanteert het principe van eenmalige registratie, meervoudig gebruik.

Om dit te bewerkstelligen wordt er waar mogelijk gewerkt met gestandaardiseerde gestructureerde koppelingen. Koppelingen worden via een veilige verbinding gerealiseerd met de verschillende (SaaS-)applicaties. In de separaat opgenomen bijlage K – Burgerzaken / BRP applicatielandschap architectuur staan de huidige en verwachte koppelvlakken.

Data ontsluiting

Gemeente Etten-Leur is al een aantal jaar bezig met centraal beschikbaar stellen van data uit het informatielandschap. Zij maakt hierbij gebruik van het Azure dataplatform (Datawarehouse) in combinatie met Microsoft PowerBI. Gegevens worden, afhankelijk van de applicatie, direct uit de

database ontsloten of middels een Extract, Transfer en Load (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 domeinen.

Gemeente Etten-Leur wenst van alle applicaties:

- Transparante toegang tot alle data van de gemeente met exportermogelijkheden.
- 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 Etten-Leur moet voldoen aan de BIO. Voor SaaS-applicaties dienen aanbieders een ISO27001 of vergelijkbare certificering te hanteren voor alle aangeboden componenten. Voor eventuele onderaannemers wordt deze eis doorgezet.

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 Etten-Leur 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 Indicators of Compromise (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 Etten-Leur 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.