BIJLAGE 24 ICT INTEGRATIEPRINCIPES

1.1 INLEIDING

Voor de vervanging van het (financiële) ERP systeem van Gemeente Groningen gelden principes vanuit de referentiearchitecturen GEMMA en NORA, daarnaast zijn er specifieke aanscherpingen te noemen voor de Gemeente. Er is een selectie gemaakt van de voor relevante architectuurprincipes en richtlijnen vanuit de genoemde referentiearchitecturen.
Binnen het project Vervanging (financieel) ERP systeem is een selectie gemaakt van de meest toepasselijke Principes, Richtlijnen en Uitgangspunten vanuit de diverse referentiearchitecturen.

Binnen deze scope wordt ervan uitgegaan dat de Principes, Richtlijnen en Standaarden van toepassing moeten zijn voor een SaaS-applicatie.

1.2 PRINCIPES

Voor het project zijn vanuit de NORA, Gemma en eigen GG (Gemeente Groningen) referentiearchitecturen de volgende principes van toepassing op dit project.

GEMMA / NORA / GG	Principe	Implicaties
NAP13	Beheers risico's voortdurend	- Bepaal de continuïteitseisen . Bepaal de exit strategie vooraf . Data moet periodiek en geautomatiseerd door de leverancier worden aangeleverd. . Informatie voor het SOC dient door de leverancier te worden opgeleverd. Hierbij geldt een voorkeur om aan te sluiten bij de SIEM/ SOC standaard van de GG
GG_INT001	Point-2-Point / Out-of-the-box integraties zijn de voorkeursmanier om applicaties te koppelen	Point-2-Point/ Out-of-the-box integraties tussen applicaties houdt in dat applicaties naadloos native met elkaar communiceren en gegevens uitwisselen zonder dat er complexe en op maat gemaakte integraties vereist zijn. Het doel is om de ontwikkeling en implementatie van nieuwe systemen te versnellen en de afhankelijkheid van op maat gemaakte integraties te verminderen
GG_INT003	Applicatie-integratie tussen externe en interne systemen wordt gerealiseerd door middel van een Gemeente Groningen gateway.	Deze gateway fungeert als een veilige en gecontroleerde toegangspoort voor het uitwisselen van gegevens tussen externe en interne applicaties, waarbij de vertrouwelijkheid en integriteit van de gegevens worden gewaarborgd. - Adeptia 2Secure, in beheer bij de Gemeente Groningen (externe partner)
GG_INT004	Voor maatwerk integraties tussen applicaties wordt gebruikt gemaakt van de ESB	Bij maatwerk integraties tussen applicaties wordt gebruik gemaakt van een ESB (Enterprise Service Bus). De ESB fungeert als een centraal systeem die de communicatie en integratie tussen verschillende applicaties faciliteert, waardoor gegevensuitwisseling efficiënt en gestandaardiseerd plaatsvindt. Deze ESB is in staat om mappings en transformaties van berichten uit te voeren. - Adeptia Connect, in beheer bij de Gemeente Groningen (externe partner)

1.2 RICHTLIJNEN

De volgende richtlijnen dienen in acht genomen te worden bij het koppelen van systemen aan het ERP-systeem 'SAP4HANA' van gemeente Groningen.

R-NR	Richtlijnen	Toelichting	NORA LAAG
1	In alle ICT-oplossingen is voor de data een exit-strategie opgenomen, en hierbij wordt specifiek aandacht besteed aan de archiefbescheiden. Alle data moet bij het stopzetten van een SaaS worden geëxtraheerd op zodanige wijze dat deze bruikbaar is op basis van de geldende archiefnormen. Deze informatieobjecten worden daarna overgebracht naar een andere archiefruimte.	Voor SaaS geldt dat bij een exit, de informatie uit het systeem moet kunnen worden gehaald en inclusief het informatiemodel via een standaard bestandsformaat wordt opgeleverd aan de GG.	Informatielaag
2	Voor het inloggen in het informatiesysteem en het beheer van gebruikersnaam/ wachtwoord wordt gebruik gemaakt van Active Directory of Azure AD.		Applicatielaag
3	Alle gegevens moeten binnen de Europese Economische Ruimte (EER) opgeslagen worden.		Informatielaag
4	Voor de uitwisseling van gegevens is het gebruik van de meest actuele StUF-standaarden, waar deze bestaan en nog niet vervangen zijn door een API-standaard, verplicht.	Voor SaaS geldt dat de API-standaard verplicht is.	Informatielaag
5	Gegevens die opgeslagen worden op storage en back-up systemen worden versleuteld opgeslagen.		Informatielaag
6	Inloggegevens worden alleen over versleutelde verbindingen verstuurd.		Informatielaag
7	Webapplicaties moeten browser-onafhankelijk en W3C-compliant zijn.		Applicatielaag

1.3 STANDAARDEN (VERPLICHT EN AANBEVOLEN)

De onderstaande standaarden geven een totaaloverzicht van de standaarden die voor SaaS-applicaties conform de VNG ICT Kwaliteitsnormen verplicht en aanbevolen zijn. Voor alle standaarden geldt: Pas toe of Leg uit.

Applicatie functie	Verplichte standaard (pas toe of leg uit)	Aanbevolen standaard	Implementatie
Gegevens integratie	• OpenAPI Specification 3.0 • REST-API Design Rules 1.0 • NL GOV Assurance Profile for OAuth 2.0	• REST • OData 4.0 • SOAP 1.2	• Koppelingen tussen SaaS en SaaS-applicaties dienen Native koppelingen te zijn zonder dat hiervoor ontwikkeld hoeft te worden. • Koppeling met on premise systemen van gemeente uitsluitend via gemeentelijke (API) gateway. • Transformatie en queueing d.m.v on premise ESB mogelijk. • SFTP mogelijk voor bestandsuitwisseling. • Geen rechtstreekse koppeling (ODBC, JDBC, SQL Net) met databases toegestaan. • Geen rechtstreekse koppelingen tussen externe en interne systemen zonder ontkoppeling (proxy). • Rechtstreekse koppelingen tussen leveranciers onderling zijn (onder voorwaarden) toegestaan. • Gegevens worden uitsluitend binnen EER opgeslagen en verwerkt, maar bij voorkeur binnen Nederland.
Uitwisseling financiële gegevens	• XBRL 2.1	• NLCIUS	
Authenticatie & SSO	• SAML 2.0	• OIDC, OAUth 2.0 • RBAC • Least privilige	• Vereist is een koppeling met de gemeentelijke Azure AD op basis van een van de genoemde standaarden. • Door deze koppeling wordt tevens voorzien in twee factor authenticatie en single sign-on. • Deze eis impliceert dat een eventuele eigen 2 factor authenticatie implementatie van de leverancier uitgeschakeld moet kunnen worden, zodat de 2fa van gemeente gebruikt kan worden.
Identity provisioning	• SCIM 2.0	• Actuele versie MS Graph API	• SCIM d.m.v. Azure AD heeft de voorkeur.
E-mail	• DKIM • DMARC • SPF • DNSSEC • Exchange webservices		• Mailhosting alleen on premise, Microsoft Exchange. • Wanneer als onderdeel van de applicatie e-mail verzonden moet worden uit naam van de gemeente, dan is dit alleen toegestaan wanneer de leverancier vanuit een eigen e-mailvoorziening de mail verstuurt en verwerkt. Gemeente stelt daarvoor een subdomein ter beschikking. De mailserver van leverancier die dit subdomein host, wordt opgenomen in de gemeentelijke SPF-records. • Overige vormen van e-mail integratie zijn niet toegestaan.
Data migratie	• Inzicht Informatiemodel.		

Front-end	• Voor het gebruik van de applicatie(s) volstaat een HTML5 compliant Web Browser (browser onafhankelijk) • Digitoegankelijk (EN 301 549 met WCAG 2.1) • Ontwikkeld en ingericht op basis richtlijnen OWASP Top 10, of aantoonbaar gelijkwaardige richtlijnen.		• Gemeente Groningen heeft een HTML5 compliant Web Browser.
Verbinding	• HTTPS • HSTS • TLS 1.2 • DNSSEC	• TLS 1.3 • IPv6	• Voor burgers en bedrijven toegankelijke voorzieningen moeten zowel via IPv4 als IPv6 bereikbaar zijn. • Verbinding over Internet d.m.v. TLS heeft voorkeur, alternatief kan een IPsec verbinding over Internet worden gerealiseerd. • Leverancier dient applicatie uitsluitend naar het IP-adres van gemeente te ontsluiten, bijvoorbeeld door middel van whitelisting. • (TLS) encryptie ingericht conform actuele richtlijnen Nationaal Cyber Security Centrum (NCSC).
Cryptografie/ versleuteling		• Gegevens die de SaaS-applicatie opslaat dienen versleuteld te zijn.	• Er dient een gedegen versleuteling van toepassing te zijn op data die door de SaaS-applicatie wordt opgeslagen. • Richtlijn: Elk wachtwoord heeft een eigen salt waarde (minimaal 64 bits) en wordt gehashed met een SHA-2 algoritme met minimaal 1000 iteraties).
Inloggegevens		• Inloggegevens worden alleen over versleutelde verbindingen verstuurd.	
Toegang tot applicatie via netwerk		• SaaS-applicaties dienen voor de gebruikers uitsluitend benaderbaar te zijn via het netwerk van de gemeente Groningen.	• Let hierbij op het gebruik van mobiele applicaties zonder aansluiting op het bestaande Gemeente Groningen netwerk.