Programma van Eisen

End users perspective

23 oktober 2025
Kenmerk 2025IPM819
Versie 1.0
Definitief

1. Functionele eisen

Eis 01.01:	De ICT-prestatie moet de performance en beschikbaarheid van web- en lokale ICT-prestaties kunnen meten vanaf een (virtuele) werkplek binnen de gemeentelijke IT-omgeving, vanuit het perspectief van een interne medewerker.
Eis 01.02:	De ICT-prestatie moet de performance en beschikbaarheid van de door de gemeente aangeboden ICT-prestaties kunnen meten vanaf een externe locatie, zonder gebruik van het interne netwerk, vanuit het perspectief van een inwoner.
Eis 01.03:	De ICT-prestatie moet in staat zijn om metingen uit te voeren inclusief de virtuele werkplek, waarbij de gebruikerservaring van de werkplek (zoals inlogtijd en ICT-prestatiereactie) onderdeel is van de meting.
Eis 01.04:	De ICT-prestatie moet rapportages genereren binnen de ICT-prestatie en moet deze rapportages geautomatiseerd kunnen distribueren (bijvoorbeeld via e-mail).
Eis 01.05:	De ICT-prestatie moet beschikken over een alerting mechanisme.
Eis 01.06:	De ICT-prestatie moet via API koppelingen kunnen integreren met de volgende systemen: Signl4, ServiceNow, SquaredUp.
Eis 01.07:	De ICT-prestatie moet gebruikersrollen ondersteunen op basis van Role Based Access Control (RBAC) zodat op een gecontroleerde manier toegang gegeven kan worden. Bijv. zodat iemand alleen eigen tests kan zien.
Eis 01.08:	Alle door de ICT-prestatie gegenereerde data moet worden opgeslagen binnen de door de of namens de gemeente beschikbaar gestelde omgeving.
Eis 01.09:	De ICT-prestatie moet zodanig ingericht zijn dat het configureren en uitvoeren van metingen mogelijk is zonder programmeerkennis of met beperkte programmeerkennis en ondersteunt 'no-code'/ 'low-code'.

2. Generieke aansluitvoorwaarden

Eis 02.01	De oplossing voldoet aan de gespecificeerde 'Pas toe of leg uit'-standaarden van het Forum Standaardisatie, waaronder HTTPS/TLS, SAML 2.0 en OpenAPI 3.0.
Eis 02.02	De ICT-prestatie voldoet aan de Baseline Informatiebeveiliging Overheid (BIO) op beveiligingsniveau 2 (BIO2).
Eis 02.03	De ICT-prestatie is volledig AVG-compliant, ondersteunt de rechten van betrokkenen en is gebaseerd op de principes van Privacy by Design en Privacy by Default. Bij het raadplegen, verwerken van persoonsgegevens conformeert de ICT-prestatie zich aan de geldende AVG-regels.
Eis 02.04	De ICT-prestatie functioneert binnen het virtuele datacenter van de gemeente. Zie bijlage a, waarin het virtueel datacenter overzicht staat beschreven.
Eis 02.05	De ICT-prestatie ondersteunt de uitwisseling van gegevens tussen ICT-prestatie middels API (web) services of een andere gestandaardiseerde methodiek.
Eis 02.06	Toegang tot de ICT-prestatie is dwingend geregeld op basis van Single-Sign-On, (SSO), zie bijlage b.
Eis 02.07	De ICT-prestatie ondersteunt de SSO standaarden zoals vermeldt in bijlage b.

Eis 02.08	De ICT-prestatie ondersteunt Multi-Factor Authenticatie (MFA).
Eis 02.09	Indien de functionaliteit van de door u aangeboden ICT-prestatie het verzenden of ontvangen van e-mail vereist, garandeert u dat de ICT-prestatie succesvol kan worden gekoppeld met de e-mailinfrastructuur van de gemeente. U bent verantwoordelijk voor het realiseren en onderhouden van deze koppeling conform de (dan geldende) technische specificaties zoals uiteengezet in Bijlage c. Deze garantie geldt voor de gehele duur van de overeenkomst, inclusief alle updates en wijzigingen aan zowel de ICT-prestatie als de e-mailomgeving van de gemeente.
Eis 02.10	Gegevens die via een openbaar netwerk (waaronder het internet) worden uitgewisseld dienen op een bij de data passende manier te worden beveiligd. Privacygevoelige gegevens moeten versleuteld worden. Deze versleuteling dient te voldoen aan de actuele richtlijnen en best practices van het Nationaal Cyber Security Centrum (NCSC). Voor alle verbindingen geldt dat minimaal TLS 1.2 of een hogere, als veilig erkende versie, verplicht is.
Eis 02.11	Bij berichtuitwisseling met externe voorzieningen wordt authenticatie d.m.v. 2-zijdig TLS1.2 of hoger toegepast.
Eis 02.12	U verstrekt Opdrachtgever proactief, en ten minste tweemaal per jaar, inzicht in de product-roadmap van de door u aangeboden ICT-prestatie voor de komende 12 tot 24 maanden. Deze roadmap bevat geplande functionele en technische ontwikkelingen, updates en uitfasering van onderdelen. Op verzoek van Opdrachtgever zult u deze roadmap nader toelichten.

3. Gegevensbescherming aansluitvoorwaarden eisen

Eis 03.01	U garandeert dat u beschikt over een gedocumenteerd en gestructureerd proces voor het tijdig identificeren, classificeren, testen en installeren van beveiligingsupdates voor alle componenten van de geleverde ICT-prestatie.
Eis 03.02	De ICT-prestatie zorgt voor adequate logging van beveiligingsrelevante gebeurtenissen. Dit omvat minimaal: a) Gelukte en mislukte aanmeldpogingen. b) Het gebruik van systeemhulpmiddelen met verhoogde privileges (auditing).
Eis 03.03	Deze logging wordt minimaal zes (6) maanden bewaard.
Eis 03.04	Beheerders hebben enkel toegang tot de functionaliteiten waarvoor zij specifiek bevoegd zijn. De verzamelde logging van de ICT-prestatie is adequaat beschermd tegen ongeautoriseerde toegang, wijziging en verwijdering. De toegang tot logbestanden is beperkt tot medewerkers van opdrachtnemer voor wie dit strikt noodzakelijk is voor de uitvoering van hun functie (principe van 'need-to-know'). Wijziging of verwijdering van logs is uitsluitend mogelijk via gecontroleerde en geautoriseerde processen.
Eis 03.05	Data moet veilig worden opgeslagen in databases of bestanden, waarbij zeer gevoelige gegevens worden versleuteld. Bijvoorbeeld: privacygegevens, waaronder, persoonsgegevens of inloggegevens.
Eis 03.06	Er moet gebruik gemaakt worden van versleuteling bij de uitwisseling van gegevens over interne als externe netwerken.
Eis 03.07	Gebruikers hebben enkel toegang tot de data waarvoor zij specifiek bevoegd zijn, conform een nog nader te bepalen en te implementeren autorisatiematrix.

Eis 03.08 Persoonsgegevens moeten worden verwijderd zodra zij niet langer noodzakelijk zijn voor het doel waarvoor zij zijn verzameld, conform de geldende bewaartermijnen.

Eis 03.09 Informatiebeveiligingsincidenten en (mogelijke) datalekken moeten onverwijld, en uiterlijk binnen 24 uur na constatering worden gerapporteerd aan de gemeente.

4. Informatiebeheer-eisen

Eis 04.01 De ICT-prestatie moet voorzien in een vernietigingsproces waarmee gegevens kunnen worden verwijderd zodra de geldende bewaartermijnen zijn verstreken.

5. Azure Native eisen

Eis 05.01 De ICT-prestatie moet functioneren binnen de Azure landing zone zoals beschreven in bijlage a.

Eis 05.02 De leverancier stemt vooraf de benodigde Azure componenten en solution architectuur af met de afdeling Cloud Delivery Center (CDC) middels het Cloud onboarding proces.

Eis 05.03 De gemeente maakt gebruik van Infra as a Code (IaC) op basis van Azure Devops, de componenten dienen hiermee samen te werken.

Eis 05.04 De gemeente beschikt over een centrale internet break-out in Azure, deze moet voor dataverkeer van en naar internet gebruikt worden.

7. Social Return eisen

Eis 07.01 U conformeert zich aan alle verplichtingen die voortvloeien uit het document ‘Handleiding Social Return’. Voor deze overeenkomst geldt een in te zetten percentage Social Return van 5%.

Eis 07.02 De gemeente bepaalt de in te zetten waarde aan Social Return op basis van de werkelijke waarde van de (nadere) opdracht. Dit is inclusief eventuele aanvullende opdrachten, zoals meerwerk, opties of wijzigingen van de opdracht.

Eis 07.03 U realiseert de Social return-invulling tijdens de looptijd van de overeenkomst.

Eis 07.04 U bent zelf verantwoordelijk voor invulling van de Social Return-opgave.

Eis 07.05 Na gunning van de opdracht plant u via socialreturn@utrecht.nl een gesprek met een adviseur Social Return. De gemeente adviseert de leverancier graag over mogelijkheden. Het toepassen van Social Return is maatwerk waarbij de gemeente rekening houdt met uw wensen: we zoeken naar een ‘win-win-winsituatie’.

8. Algemene eisen

Eis 08.01 Om de overeengekomen kwaliteit te borgen en te meten en een gezamenlijke werkwijze te hebben, maken leverancier en gemeente duidelijke afspraken die vastgelegd worden in een Service Level Agreement (SLA) en een Dossier Afspraken & Procedures (DAP). Deze documenten worden in samenspraak, doch minimaal eenmaal per jaar, gecontroleerd en bijgewerkt.

De SLA bevat daarbij minimaal de volgende afhandelings- en responsetijden volgens de gemeente prioriteitenmatrix:

Onderstaand een overzicht van prioriteitenmatrix op basis van de impact en urgentie voor incidenten.

Prioriteitenmatrix		**Impact**		
		Alle gebruikers (1)	Team, afdeling, OO (2)	Eén of enkele gebruikers (3)
Urgentie	Werk uitvoeren is (bijna) niet meer mogelijk. (1)	1	2	3
	Werk uitvoeren is verstoord (2)	2	3	4
	Werk uitvoeren is nog mogelijk (3)	3	4	5

Impact

Impactniveau		**Criteria**
1	Alle gebruikers	Meer dan 500 gebruikers
2	Team, afdeling, OO	
3	Één of enkele gebruikers	Max. 5 gebruikers

Urgentie

Urgentieniveau		**Criteria**
1	Werk uitvoeren is (bijna) niet meer mogelijk	Indien er een work-around beschikbaar is dan is werken uitvoeren **wel** mogelijk.
2	Werk uitvoeren is verstoord	
3	Werk uitvoeren is nog mogelijk	

Oplostijden prioriteiten

Prioriteiten	**Oplostijden**
Prio 1	4 uur (halve werkdag)
Prio 2	9 uur (1 werkdag)
Prio 3	18 uur (2 werkdagen)
Prio 4	36 uur (4 werkdagen)

Prio 5	90 uur (2 weken)

*Service window van Domstad IT is van 8:00 t/m 17:00 (9 uur). Dit is ook toegepast in de oplostijden.

Eis 08.02 U heeft een vastgelegd releasemanagement-proces en biedt onderhoud op de door u geleverde ICT-prestatie waarmee uw ICT-prestatie voldoet aan de laatste compliancy- en securityrichtlijnen door updates en patches beschikbaar te stellen conform de in Eis 08.01 gestelde afspraken.

Eis 08.03 De communicatiekanalen die u aanbiedt zijn minimaal per telefoon en per e-mail.

Eis 08.04 De ondersteuning is ten minste 5 werkdagen per week beschikbaar tijdens reguliere kantooruren.

Eis 08.05 Release notes worden overhandigd aan de gemeente bij een upgrade.

Eis 08.06 De Servicedesk van de Opdrachtnemer is Nederlandstalig en levert ondersteuning in het Nederlands, zowel in woord als geschrift.

9. Commerciële eisen

Eis 09.01 Uw inschrijving is in de Nederlandse taal gesteld en de gehanteerde tarieven zijn in euro's exclusief BTW.

Eis 09.02 Uw inschrijving bevat een volledig ingevuld Prijsinvulformulier bijlage 10.

Eis 09.03 De opdrachtgever garandeert een afname van minimaal 1.000.000 metingen per contractjaar. Het totaalbedrag voor deze gegarandeerde afname is vast en wordt ongeacht het daadwerkelijke gebruik betaald.

Eis 09.04 U vermeldt de prijzen in de daarvoor bestemde velden in het prijzenblad en volgens de genoemde staffelindeling. De staffels worden elk contractjaar opnieuw toegepast:

Staffel 1: 1 t/m 1.000.000 metingen (gegarandeerde afname)
Staffel 2: 1.000.001 t/m 2.000.000 metingen
Staffel 3: 2.000.001 t/m 2.200.000 metingen

De volumes in staffel 2 en staffel 3 zijn indicatief en niet gegarandeerd. Deze staffels worden uitsluitend toegepast indien en voor zover het daadwerkelijke verbruik binnen een contractjaar de gegarandeerde afname van 1.000.000 metingen overschrijdt. De verrekening van dit meerverbruik vindt plaats op daadwerkelijk verbruik:

- Metingen die vallen in de bandbreedte van staffel 2 (1.000.001 tot en met 2.000.000) worden per stuk afgerekend tegen het tarief van staffel 2.
- Metingen die vallen in de bandbreedte van staffel 3 (vanaf 2.000.001) worden per stuk afgerekend tegen het tarief van staffel 3.

Voorbeeld: Bij een totaal jaarverbruik van 1.500.000 metingen wordt de facturatie als volgt opgebouwd:

De eerste 1.000.000 metingen worden afgerekend tegen het tarief van staffel 1 (conform de gegarandeerde afname).

De daaropvolgende 500.000 metingen (van 1.000.001 tot 1.500.000) worden afgerekend tegen het tarief van staffel 2.

De staffels en de bijbehorende verrekenmethodiek worden elk contractjaar opnieuw toegepast. De telling van het aantal metingen dat de toepasselijke staffel bepaalt, wordt aan het begin van ieder nieuw contractjaar (op de contractverjaardag) opnieuw op nul (0) gesteld.

Eis 09.05 In afwijking van artikel 11.8 van de GIBIT, zijn de door u in het Prijsinvulformulier aangeboden tarieven en vergoedingen vast voor de eerste 12 maanden na de ingangsdatum van de overeenkomst en worden gedurende deze periode niet geïndexeerd

Na het verstrijken van deze eerste periode van 12 maanden kunnen de overeengekomen doorlopende vergoedingen en uurtarieven jaarlijks worden geïndexeerd, telkens op de verjaardag van de ingangsdatum van de Overeenkomst. Gedurende de initiële contractlooptijd van 24 maanden kan er derhalve maximaal één keer worden geïndexeerd.

De indexering is uitsluitend van toepassing op de volgende kostenposten uit het Prijsinvulformulier:

- Post 1.1: Jaarlijkse licentiekosten.
- Post 1.2: Jaarlijkse onderhoudskosten.
- Post 1.5: Uurtarieven extra ondersteuning op afroep.

Eenmalige kosten, zoals post 1.3 (Implementatiekosten) en post 1.4 (Ondersteuningskosten), zijn expliciet uitgesloten van indexering.

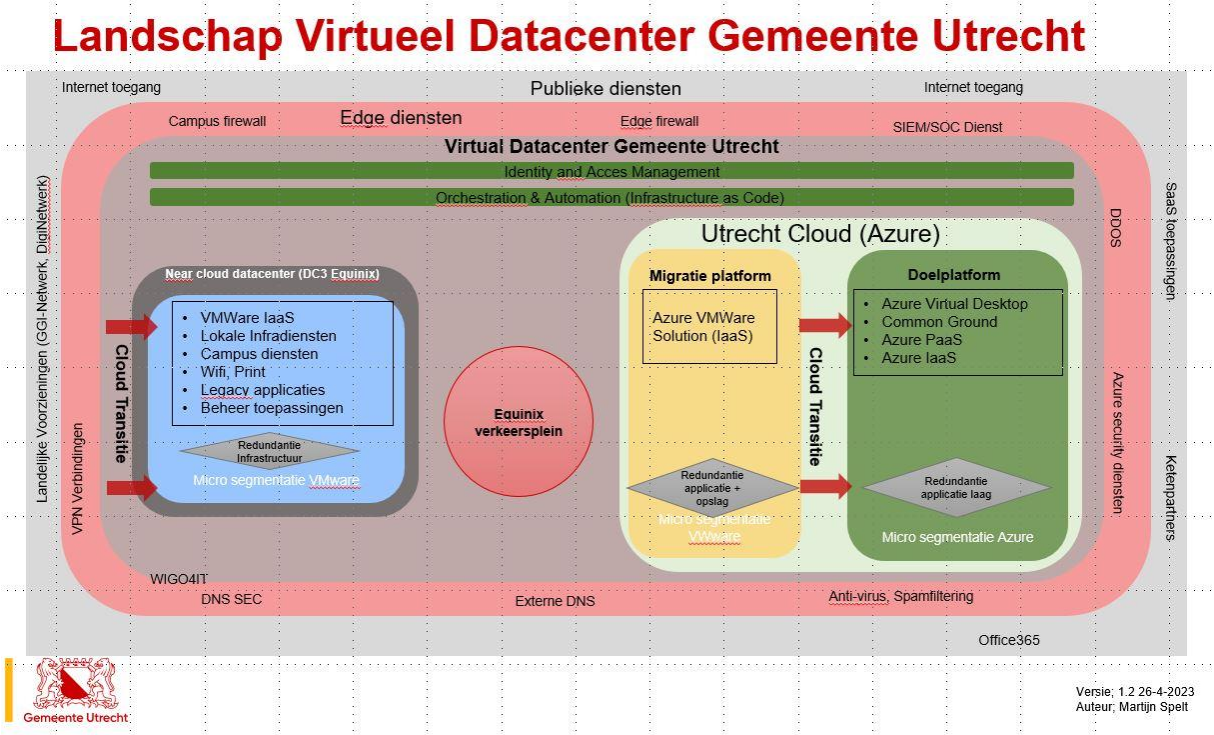
De aanpassing van de tarieven vindt plaats conform de berekeningsmethode zoals beschreven in artikel 11.8 van de GIBIT. De stijging is gelimiteerd tot maximaal de (eventuele) stijging van het op het moment van aankondiging laatst door het Centraal Bureau voor de Statistiek (CBS) gepubliceerde definitieve prijsindexcijfer dienstenprijzen commerciële dienstverlening en transport (index 2015=100), althans de opvolger daarvan, voor groep J62, althans J6202, over het gehele jaar in vergelijking met het prijsindexcijfer van het jaar daarvoor van diezelfde index.

Eis 09.06 U dient een voorgenomen prijsaanpassing minimaal één maand voorafgaand aan de indexatiedatum (de jaarlijkse verjaardag van de ingangsdatum van de overeenkomst) schriftelijk aan Opdrachtgever aan te kondigen.

Bijlage a - Algemene beschrijving van de inrichting van het virtuele datacenter

Virtueel datacenter overzicht

Onderstaande architectuur geeft een hoog-over beeld van het ICT-landschap van de gemeente, en de daarbij behorende diensten en componenten. Verdere informatie wordt in de volgende paragrafen gegeven, eventuele detail-vragen kunnen aan het team architectuur worden gesteld.



Figuur 1 Landschap virtueel datacenter Gemeente Utrecht

De gemeente bevindt zich in een Cloud transitie-programma, het eigen datacenter wordt naar een near-cloud datacenter en Azure VMWare overgezet en aansluitend vindt een applicatie-transitie plaats van IaaS naar SaaS, Common Ground en/of Azure native omgeving. Dit is een langlopend programma.

Algemeen

De door de leverancier aan te bieden ICT-Prestatie dient aan te sluiten op de binnen de gemeente geldende standaards ten aanzien van de ICT-infrastructuur.
In onderstaande beschrijving worden deze infrastructuur verder beschreven.

De beschreven infrastructuur en componenten zijn aan verandering onderhevig mede vanwege de Cloud-transitie, onderstaande beschrijving is een momentopname en wordt twee keer per jaar geactualiseerd. De beschrijving kan op punten afwijken van de actuele situatie.

Server hosting (datacenters)

De gemeente kent een Near Cloud datacenter (extern gehost) op basis van VMWare virtualisatie en een public Cloud omgeving op basis van Microsoft Azure, hierbinnen is voor IaaS zowel Azure VMWare (op basis van NSX-T) als Azure native hosting beschikbaar. De Azure en Near Cloud omgevingen vormen samen het gemeentelijke virtuele datacenter en zijn middels een verkeersplein-oplossing met elkaar verbonden.

Verkeersplein (connectiviteit)

De gemeente maakt gebruik van een centrale verkeersplein-oplossing, hier worden alle externe verbindingen gekoppeld zoals GGI-netwerk, internet en de verbindingen (Express route) met Azure en het campus. Deze omgeving bevat tevens Edge security functionaliteit zoals een Next Generation firewall.

Microsoft Azure

De gemeente heeft de beschikking over één Microsoft Azure omgeving , ingericht conform de Microsoft Enterprise Scale Hub-Spoke architectuur. Er is een directe synchronisatie tussen de gemeentelijke directory en Azure AD. Er wordt gebruik gemaakt van Azure policies voor beveiliging beleid o.a. BIO, ISO27001 en beheerders policies. Subscriptions in de tenant zijn onder te verdelen in 3 hoofdgroepen;

1. Platform
    a. Centrale connectiviteit, identiteit en management-diensten
2. Landing zone
    a. Locatie van de Azure-diensten voor de organisatie
3. Sandboxes
    a. Geïsoleerde omgevingen voor ontwikkel- en test-trajecten
        i. Deze sandboxes zijn afgeschermd van de overige Azure omgeving.

Als onderdeel van de landing zone is een omgeving ingericht voor IaaS op basis van Azure VMWare Solutions, dit is netwerk-technisch een extensie van het Near Cloud datacenter. Azure VMWare is voorzien van vSAN opslag en NetApp Cloud Volumes ONTAP voor de opslag van data en informatie.

Azure Automation

Binnen de Azure omgeving wordt zoveel mogelijk geautomatiseerd gewerkt, hiervoor wordt gebruik gemaakt van pipelines en Azure Devops CI/CD.

Near Cloud datacenter

Het netwerk binnen het Near Cloud datacenter is opgebouwd conform het SDDC-concept, netwerk virtualisatie wordt gerealiseerd met behulp van VMWare NSX-T. Dit netwerk is uitgebreid naar de Azure VMWare omgeving. Microsegmentatie en zero trust worden als concept toegepast, er wordt gebruik gemaakt van 802.1X authenticatie. VMWare wordt als hypervisor gebruikt, het Near Cloud datacenter is voorzien van een Pure storage opslag platform.

Netwerkvirtualisatie en zero trust

De gemeente volgt het zero trust concept met segmentatie waar benodigd. ICT-systemen worden op basis van functie, locatie en gebruik gescheiden van elkaar. Hiervoor is op het VMWare platform NSX-T beschikbaar. Binnen Azure native wordt er gebruik gemaakt van NSG's en USG's voor netwerkscheiding.

Ondersteunde operating systemen

De gemeente ondersteunt de volgende systemen binnen zijn virtuele datacenters;

- Windows Server 2022 en hoger;
- Red Hat 8.X Enterprise Linux;
- Oracle Linux voor hosting van Oracle databases;
- Windows 10 64 bits en hoger (werkplek)

Databases

Er wordt een aantal soorten databases ondersteunt;

- SQL Server 2022 en hoger (op Windows Server)
- MariaDB (op Redhat Linux)
- Oracle 12 (op Oracle Linux)
- Postgress (op Docker platform)

De werkplek

De werkplek wordt tweeledig aangeboden;

1. Een mobiele werkplek op basis van Windows 11 of hoger.
2. Een Azure Virtual Desktop op basis van Windows 11 Multiuser.
3. Voor specials zoals presentatie-pc's is een aparte procedure beschikbaar.

Taak-applicaties worden op basis van applicatievirtualisatie aangeboden op de werkplekken. Daarnaast wordt er gebruik gemaakt van een "bedrijfsportal" en Application proxy om legacy applicaties te presenteren op de mobiele werkplek. Er wordt gebruik gemaakt van een lokale Microsoft Office 365 installatie.

Voor het beheer van de werkplekken wordt gebruik gemaakt van zowel SCCM als Microsoft Endpoint manager (Intune) in Azure. SCCM wordt gebruikt voor het distribueren van datacenter-gebonden servers en werkplekken en Endpoint manager voor het configureren op afstand van de mobiele werkplekken.

Microsoft 365

De werkplek is voorzien van de OneDrive client, deze fungeert als opslag van persoonlijke informatie, SharePoint wordt gebruikt voor de opslag van afdelings- en bedrijfsinformatie.

De werkplek is tevens voorzien van de Microsoft Teams client voor communicatie en delen van niet-bedrijfskritische informatie met collega's en externe partijen.

Email

De mailomgeving is gebaseerd op Exchange online. Er is een lokale Exchange server aanwezig voor legacy applicaties en specials, deze is hybride verbonden met Exchange online. Indien er aansluiting benodigd is op de mailomgeving wordt er gebruik gemaakt van een centrale SMTP gateway. (zie bijlage c - aansluiting op de mail). Er is geen centrale bulkmail-voorziening.

Voor het versturen van gevoelige informatie is er een veilige mail-voorziening.

IAM proces identity provisioning

De gemeente conformeert zich aan de IAAA-standaard (Identificatie, Authenticatie, Autorisatie en Accountability). Hiervoor is een geautomatiseerd proces ingericht; medewerkers, externen en ketenpartners worden vanuit bronsystemen geautomatiseerd beheerd gedurende de gehele levenscyclus van de identiteit. Binnen het IAM-systeem is selfservice beschikbaar en kunnen rollen worden toegekend. Taak-applicaties kunnen worden aangesloten voor identity provisioning via SCIM. Hiervoor is Azure Identity provisioning beschikbaar en een lokale SCIM API voor specials.

Authenticatie en SSO

De gemeente hanteert het Single Sign-On beleid voor interne en externe applicaties aangevuld met een tweede factor. Medewerkers van de gemeente beschikken over één identiteit en een 2e factor op basis van Microsoft MFA. Ten behoeve van SSO wordt er federatie toegepast op basis van Azure Federatie aangevuld met conditionele toegangsbeleid.

Identiteiten worden automatisch beheerd, applicaties worden aangesloten voor authenticatie op de gemeente identiteit. Hiervoor zijn aansluitvoorwaarden van toepassing (zie **Fout! Verwijzingsbron niet gevonden.**)

Bijlage b - Authenticatie en SSO

De gemeente hanteert een Single Sign-On (SSO) beleid voor zowel interne als externe applicaties, waarbij toegang consequent wordt beveiligd met een verplichte tweede authenticatiefactor via Microsoft Multi-Factor Authentication (MFA). De implementatie van SSO gebeurt door middel van federatie via Microsoft Entra ID, wat aangevuld wordt met een strikt Conditioneel Toegangsbeleid. Applicaties zijn verplicht te authenticeren tegen de centraal en automatisch beheerde gemeentelijke identiteit, waarvoor strikte aansluitvoorwaarden en standaarden van toepassing zijn. Zie Authenticatie en Provisioning standaarden

Authenticatie en provisioning standaarden

De gemeente maakt gebruik van moderne authenticatie op basis van Azure Federatie. Onderstaande tabel bevat de door de gemeente ondersteunde protocollen en toepassing daarvan. Er is een IAM loket beschikbaar welke de federatieve koppeling samen met de leverancier realiseert. (IAM@Utrecht.nl)

Authenticatie middelen (*1,2*)

Nr.	**Protocol**	**Status**	**Middel**	**Interne applicaties**	**SaaS/Cloud-applicaties**
1	**OpenID Connect** **Oauthv2**	**Voorkeur**	**Azure Federatie** (*3*)	**Ja**	**Ja**
2	SAML v2.0	Alternatief	Azure Federatie	Ja	Ja
3	Kerberos	Alleen intern	Active Directory	Ja	Nee
4	LDAPS	Niet toegestaan		n.v.t.	n.v.t.

Identity Provisioning[5]

Nr.	Protocol	Status	Middel	Interne applicaties	SaaS/ Cloudapplicaties
1	**SCIMv2** (Omada Identity Cloud)	**Voorkeur**	**SCIM endpoint**	**Ja**	**Ja**
2	SCIMv2 (Entra ID)	Alternatief	SCIM endpoint	Ja	Ja
3	Maatwerk REST API	Alleen bij uitzondering		Ja	Ja
4	Maatwerk XML SOAP	Alleen bij uitzondering		Ja	Ja
5	Eigen implementatie	Alleen bij uitzondering		Ja	Ja
6	Handmatig	Afhankelijk van BIV classificatie toegestaan		Ja	Ja
7	Microsoft LDAPS	Niet toegestaan		n.v.t.	n.v.t.
8	Bestand: XML, JSON (beveiligd)	Niet toegestaan		n.v.t.	n.v.t.

Toelichting;

1. Nummering van protocollen staat in volgorde van voorkeur
2. De mate en inrichting van identity provisioning is mede afhankelijk BIV-classificatie en het gebruik van rollen.
3. Bij Container platform met Keycloak als broker
4. Punt 5 en 6 - Alleen bij uitzondering; na afstemming met product owner en architectuur

Bijlage c - Aansluiting op de mail-voorziening

De gemeente maakt voor de mail-voorziening primair gebruik van Microsoft 365 Exchange Online i.c.m. een lokale Exchange installatie voor specials en interne routering.
Alle applicaties welke verzending namens een gemeentelijk email adres nodig hebben sluiten aan op de Exchange online SMTP-dienst (smtp.office365.com). Bij voorkeur wordt er gebruik gemaakt van Graph API om te koppelen aan Exchange online. Deze SMTP-dienst is geschikt voor het versturen van reguliere hoeveelheden email (specificaties). Voor grote hoeveelheden email of specifieke wensen wordt per project een dienst afgenomen. Het aansluitproces email is verder uitgeschreven per scenario in het document aansluiten op de mail-voorziening en is op verzoek beschikbaar.
Bij uitzondering is verzending met een eigen SMTP-dienst middels spf-records mogelijk, hiervoor wordt een risicoanaylse uitgevoegd per situatie.