Bijlage ICT randvoorwaarden bij aanbestedingen

Omschrijving van de huidige technische infrastructuur van ICT Gouwe-IJssel voor de gemeenten Gouda, Waddinxveen, Zuidplas, Montfoort en IJsselstein en de eisen die hieruit voortkomen bij de aansteding van on-premises applicaties.

gemeente gouda

Inhoudsopgave

1. Algemeen

De volgende indeling van soorten applicaties / systemen wordt gebruikt:

- Web-based
- Windows Client-server.
- Stand-alone: op een lokale PC/laptop of server. Installatie op afstand (rdp, vnc) moet mogelijk zijn
- Installatie van data en programmatuur op storage (inclusief installatie onder Citrix Virtual Desktops en Citrix Virtual Apps).
- Mobiele apps ontsloten door Microsoft Intune
- Applicaties zijn bij voorkeur web-enabled
- Applicaties zijn Citrix Virtual Apps-enabled.

Applicaties zullen in bovenstaand technische kader moeten passen. Met name de centrale installatie op de storage en het voldoen aan de standaard gebruikte (besturings)software op serverplatforms en de clients.

We verwachten een duidelijke en inzichtelijke documentatie voor gebruikers, het applicatiebeheer en het systeembeheer. Hetzelfde geldt voor de mogelijke foutboodschappen, voor zover deze betrekking hebben op het besturingssysteem of RDBMS.
Er dient een duidelijke scheiding te zijn in systeembeheer, technisch- en functioneel applicatiebeheer. Systeembeheer draagt zorg voor het uitvoeren van updates en heeft hiervoor de benodigde rechten. Functioneel Applicatiebeheer heeft contact met de leveranciers, coördineert de installatie van updates/upgrades en lost functionele vragen van gebruikers op.

De door de leverancier aan te bieden applicatie en eventuele hardware dient aan te sluiten op de binnen de gemeenten Gouda, Waddinxveen, Zuidplas, Montfoort en IJsselstein geldende standaarden ten aanzien van de ICT-infrastructuur. In onderstaand overzicht zijn de geldende ICT-standaarden weergegeven en daar waar van toepassing en nu reeds bekend welke standaarden zijn gepland. Gemeente Gouda host in twee eigen datacenters de ICT-infrastructuur van de vijf gemeenten. Indien de cellen zijn samengevoegd, is de tekst van toepassing op alle vijf de gemeenten.

Tenzij expliciet anders vermeld, hanteren de gemeenten de open standaarden uit de lijsten van het Forum Standaardisatie.

	Gouda	Waddinxveen	Zuidplas	Montfoort	IJsselstein
Centrale hardware/software	Citrix Virtual apps 7 op Citrix Hypervisor 8				
	Citrix Virtual desktops 7 op Citrix Hypervisor 8				
	Intel based hardware				
	Citrix Virtual apps servers op Windows Server 2019. Alle Xenapp server zijn W2019, moeten ook nog naar W2022 tzt			Citrix Virtual apps servers op Windows Server 2019	
	Linux CentOS 8.x/9,x, Almalinux 9 (LTS)				
	VMware ESXi 8				
	Applicatieservers op Windows, 2019 en 2022				
Decentrale hardware	Windows laptop			HP T610 Windows 10 Enterprise LTSB	HP T610 Windows 10 Enterprise LTSB
	HP Color Laserjet MFP 187650			HP Color Laserjet MFP 187650	HP Color Laserjet MFP 187650
Netwerk	TCP/IP (LAN), NFS/iSCSI (storage). Cisco				
RDBMS	Oracle19.x. met o.a. de modules spatial en Oracle text. Draaiend op Oracle Linux 7, in overgang naar Oracle Linux 8				
	SQLSERVER: deels 2016 , deels SQL-server 2019 en in overgang naar 2019/2022. SQL server draait in een cluster.				
Kantoorautomatisering	Microsoft 365 inclusief Teams en Sharepoint; docx als standaard formaat.				
Oracle client	Oracle 19 (standaard 64 bits)				
Middleware	Oracle Web Logic Suite met Forms 19 Oracle APEX (op Linux) Oracle Grid Control 13G				
Mail	Exchange 2019, Exchange Online (voorkeur), Exchange spamfilter				
Internet(beveiliging)	Cisco FTD firewall/IPS, MS Defender (XDR, Eindpunt)				
Identity management Access management	Tools4Ever HelloID (Identity) Microsoft Entra ID (Access): synchroniseert met AD on premises				
Mobile Device Management	Smartphones en laptops interne medewerkers: Microsoft Intune				

2. Netwerk

Datacommunicatie binnen de gemeenten is gebaseerd op de facto industriestandaards. Verschillende vestigingen van de gemeente zijn middels glasvezel met elkaar verbonden, waarover datacommunicatie plaats vindt via het Ethernet protocol. Er is sprake van een geswitched en gerouteerd netwerk (ISO laag 2 en 3). De interne gebouwbekabeling UTP cat6a, de bekabeling van outlet naar werkplek op basis van UTP cat5E.

De ICT-omgeving wordt gehost vanuit twee datacenters op twee verschillende locaties. Volgens de constructie active-active. Deze twee locaties zijn via redundante glasvezels op laag 2 verbonden met een snelheid van 300Gbit (lan) en 100 Gbit (storage). De Storage, Oracle, UCS omgeving zijn dubbel uitgevoerd. Iedere locatie is met een aantal aanpassingen in staat autonoom te draaien.

De in beheer zijnde gemeentes zijn via een enkelvoudige glasvezelverbinding van 1Gb/s aangesloten op een van beide datacenters. Bij de diverse gemeentes draait een coreswitch die de subnetten daar routeert en switches voor de ontsluiting van de apparatuur.

3. RDBMS

Oracle 19 is de database-standaard en draait sinds medio 2025 op een apart cluster onder VMware.
Deze wordt minimaal 2 en maximaal 4 maal per jaar bijgewerkt naar de laatste patch-versie. Per gemeente is er éém productie en één testserver beschikbaar. In Gouda is nog een derde server tbv. Een aparte runtime/(ontwikkel) database van GWS. Alle servers zijn identiek van opzet en draaien op Oracle linux 8.
Het patch-level van alle applicaties/databases wordt gelijk gehouden wat betekent dat een patch-update een heel testtraject inhoudt van alle gemeentes met betrokken applicatiebeheerders. Er wordt overal gebruik gemaakt van een multitenant-architectuur met een aantal root-containers en geclusterde pluggable database (het applicatie-deel). De geïnstalleerde modules variëren per gecombineerd cluster maar bevatten meestal: Oracle XML DB, Oracle JVM, Oracle APEX en Oracle Spatial en Oracle Intermedia voor de applicaties met geometrie-componenten.
De Oracle versie is gebaseerd op de Standard Edition Two licentie in de gemeentes Gouda en Zuidplas draaiend op een apart Oracle cluster onder VMware. In de gemeentes Montfoort en IJsselstein is de variant met de melodies lijn van Centric (Enterprise Edition) actief draaiend ook op een VMware platform .
Voor de architectuur van Oracle wordt een aangepaste OFA-standaard gehanteerd. Een uitgangspunt is verder dat alle productie-applicaties 1 op 1 gekopieerd worden naar de test-omgeving, daarbij gebruik makend van exact dezelfde instance-benamingen. De kopieslag gebeurt door het maken van snapshots, c.q. flexcloning. De databases worden in een metrocluster (gespiegelde opslag) via NFS gekoppeld. Vanwege een uniforme structuur zijn deze (qua back-end) makkelijk te migreren naar een andere server.

4. Servers, storage en backup

Voor alle onderdelen van de infrastructuur geldt dat deze zo veel mogelijk gescheiden worden neergezet per functionaliteit. Zoals hierboven beschreven wordt de database in een aparte omgeving neergezet. De applicatieservices, en printservices worden beschikbaar gesteld via virtuele servers die opereren onder VMware ESXi 8. Afhankelijk van de applicatie kan een virtuele server worden uitgerust met o.a. Windows of Windows server 2019 of Windows Server 2022. Uitrol gebeurt via een standaardprocedure. De meeste virtuele servers beschikken over een productie- en testvariant. In principe geldt dat voor 1 applicatie een aparte virtuele omgeving wordt ingericht. Deze zijn eenvoudig te klonen. Een backup van deze virtuele servers gebeurt in principe via een volledige totaal-backup (Commvault). Het beheer van een dergelijke applicatieserver worden gedelegeerd aan de applicatiebeheerder.

Fileservices worden via het CIFS protocol aangeboden door de dubbel uitgevoerde Netapp filers (Netapp Metrocluster). Voor toepassingen dient rekening te worden gehouden met deze software en plugins. Backup

van deze filers gebeurt d.m.v. Commvault. Er worden vier maal per dag snapshots gemaakt zodat bestanden door de gebruiker tot enkele dagen terug zelf zijn te herstellen naar een vorige versie. Het restoren vanaf backup/tape is daarmee beperkt tot uitzonderingsgevallen.

De hardware onderliggend aan de VMware en de Citrix Xenserver omgeving is Cisco UCS-X op basis van Intel based servers. Deze servers zijn via een 40Gbit connectiviteit in de infrastructuur opgenomen.

5. Werkplek

Een standaard werkplek bestaat uit een Windows laptop. Op deze laptop wordt ook met behulp van Citrix Virtual Apps een published desktop aangeboden. Een aantal gebruikers hebben naast Citrix Virtual Apps ook nog een Citrix Virtual Desktop tot hun beschikking. EenVirtual Desktop dient vooral voor het aanbieden van een desktop met grafisch zware applicaties. Alle werkplekken hebben toegang tot internet.

Er zijn een aantal manieren om applicatiesoftware te installeren:

- Applicatieserver
- Netwerkschijf
- Centrale Citrix image Virtual Apps 7.X LTSR(vDisk) tbv de algemene desktop voor iedereen
- Centrale Citrix image Citrix Virtual Desktops 7.X LTSR (vDisk) tbv de grafische zware (CAD) applicaties

Bovenstaande lijst is gerangschikt van wenselijk naar onwenselijk. Met behulp van de Ivanti Workspace Control manager wordt een gepersonaliseerde desktop aan gebruikers aangeboden. Er moet bij de planning van een nieuwe toepassing daarom rekening worden gehouden met benodigde tijd voor installatie van de software, het inleren van RES en het uitvoeren van een testtraject in samenwerking met systeem- en applicatiebeheer. (Ivanti Workspace Control is EOL 31-12-2026) onderzoek naar vervanging loopt

Een standaard werkplek bezit de volgende eigenschappen:

Eigenschap	Instelling
Desktop resolutie	1920*1080 of 1920*1200
Platform	Windows server 2019 of Windows server 2022
Java	8
Kantoorautomatisering	Zie paragraaf 1.9
Monitor	standaard 1 per werkplek, helft van de werkplekken 2
PDF reader	Adobe Acrobat reader DC
Browser	Chrome, Edge
Plugins	.NET is beschikbaar

6. Internet

De internet verbinding gaat via een firewall (Cisco FPR1250) en dan, afhankelijk van de route, naar Diginet of internet. De firewall is multiprovider redundant (eGem en Eurofiber), 2x 900Mbit.
De Firewalls gebruiken ook IP/URL filters en IPS functionaliteit.
.De gemeenten hebben de mogelijkheid tot “thuiswerken” via een Citrix portal waar zowel een Citrix Virtual Apps sessie als een Citrix Virtual Desktops sessie gestart kan worden. Webmail wordt direct via exchange online gedaan.
Voor extern <-> intern of extern <-> extern berichtenverkeer wordt een on-premise (Gouda) of cloud (IJsselstein en Montfoort) OpenTunnel van Jnet gebruikt als gateway en digikoppelingsadapter. Zuidplas gebruikt de centric cloudconnector.

Aan leveranciers waarmee over veel poorten of op veel adressen gecommuniceerd moet worden, of waarbij de beveiliging niet via SSL ingeregeld kan worden, kan er een VPN tunnel worden gemaakt. Maar dit is alleen als de gemeente Gouda hier het voordeel van ziet.
De mail gaat via Exchange online spamfilters, het transport is voorzien van IPv6, SPF, DKIM, DMARC en TLS. Voor beveiligd mailen wordt Zivver gebruikt voor IJsselstein, Gouda en Zuidplas. Montfoort gebruikt zorgmail en Waddinxveen cryptshare.

7. Web applicaties

Interne web applicaties draaien hetzij op internet information server (IIS) versie 10.0 van Microsoft of Apache Tomcat op Windows server 2019/2022 of Linux (CentOS / Almalinux).
Oracle WebLogic Suite is nog in gebruik als webapplicatie server voor Oracle Forms applicaties. Oracle Forms moet zonder gebruik van een JVM browser plugin aangeboden worden.
Oracle Forms 12 wordt per 31-12-2026 uitgefaseerd omdat er geen support vanuit Oracle meer is op Oracle12 Forms/Reports.
Alle ‘Key2’- applicaties van Centric die tot nu toe gebruik maakten van Form op een Weblogic platform moeten dan vervangen zijn door de IIS variant, deels met .Net-technologie. De weblogic platforms moeten per eind 2026 zijn vervangen.
Naast de interne webapplicaties wordt er ook gebruik gemaakt van Saas-applicaties.

8. Applicatiesoftware

Applicatiesoftware wordt op file- en applicatieservers gescheiden naar toepassing. Services, batches en draaiende programmatuur draaien op de applicatieserver, alsmede ook html- en xml-bestanden draaiend op een web-server. Voor de file-based bestanden kunnen deze terecht komen op een Oracle Server of filer die mbv het CIFS protocol wordt gemount op een Windows-desktop.

De rechten op de bovengenoemde shares, mappen en bestanden hierbinnen zijn geregeld via de applicatie- en afdelingsgroepen van Windows 2012R2 Active Directory.
LET OP: het maximale aantal tekens van mappen op de Windows-omgeving mag 255 tekens zijn en inclusief document-benaming 260 tekens.
Applicaties die gebruik maken van extreem lange mapstructuren of documentbenamingen worden daarom niet ondersteund.

Versiebeheer van applicaties

Versiebeheer is in principe een verantwoordelijkheid van de applicatiebeheerder. In het geval van grotere applicaties worden nieuwe ontwikkelingen, aanpassingen, updates en fixes altijd getest in een (identieke) testomgeving. Pas na toestemming en goedkeuring van de applicatiebeheerder wordt software in de productieomgeving geplaatst. De applicatiebeheerder dient bij de installatie op de productieomgeving aanwezig te zijn. Tijden gaan in overleg. Systeembeheer verricht technische ondersteuning bij de uitvoering van updates op het gebied van datamanagement of aanpassingen in de database en verricht controle op de handhaving van het OTAP-principe. Aanpassingen ten gevolge van nieuw ontwikkelde koppelingen of maatwerptoepassingen dienen zoveel mogelijk in een aparte ontwikkelomgeving te geschieden. Voor gewennings- of opleidingstoepassingen is het mogelijk een opleidingsomgeving te gebruiken.

9. Kantoorautomatisering

De gestandaardiseerde kantoorautomatiseringomgeving maakt gebruik van Microsoft Office365.
Koppelingen van de applicatie met de kantoorautomatiseringomgeving moet derhalve via genoemde suite plaats vinden. Het ODF wordt via Office ondersteund.

Als emailplatform wordt Exchange Online gebruikt. Het email berichtenverkeer vanuit de applicatie moet via deze online dienst worden afgehandeld. Het van buitenaf komende emailverkeer wordt gescand op bijlagen en virussen. Het overgrote deel van de postbussen van ICT omgeving wordt gehost bij Exchange Online.

Zivver draait als plugin op Exchange (GDA, ZPL, IJS) voor veilig versturen van email en (veilig) mailen van grote bijlagen. WDV gebruikt Cryptshare, MON gaat Zorgmail gebruiken (ja is in gebruik)?

Standaard kunnen gebruikers downloaden. Het downloaden van executables is niet mogelijk. Alleen bepaalde applicatiebeheerders hebben de mogelijkheid om alles te downloaden bijvoorbeeld tbv. updates, release documentatie en dergelijke. Uitvoeren van vreemde executables is standaard onmogelijk op de werkplek. Pas na goedkeuring (whtielisting) door systeembeheer kan een nieuwe executable uitgevoerd worden.

Voor videovergaderen en hybride vergaderen wordt MS Teams gebruikt. De medewerker start buitende Citrix desktop de app op de laptop, smartphone of eigen thuiswerkplek.

10. Dataopslag

De dataopslag gebeurt op een NetApp omgeving, bestaande uit een metrocluster met 2 clusters met elk 2 nodes. De clusters zijn verdeeld over 2 locaties. Beide clusters zijn in staat om de resources van de andere over te nemen om in geval van uitwijk op 1 locatie te kunnen werken. Elk cluster bestaat uit 2x een AFF-C250 met een aantal diskshelfs en zijn middels fiberswitches met elkaar verbonden.
De dataopslag wordt gebruikt voor kantoordata (CIFS), VMware (NFS), Windows (iSCSI), Oracle (NFS) en diverse andere databases zoals MSSQL. In totaal omvat de dataopslag zo'n 150Tb. Het opslagsysteem is voorzien van een multistore licentie voor dataopslag van meerdere organisaties.

Om de datagroei nog enigszins te beperken wordt gebruik gemaakt van thin-provisioning en deduplicatie. Ten behoeve van het opbouwen van een test- en/of ontwikkelomgeving wordt er gebruik van gemaakt van flexclone technologie. Daarnaast gebruiken we snapshot technologie voor het snel kunnen maken van backups. Zo'n backup wordt eventueel met behulp van snapvault overgebracht naar een backupfiler (FAS2720).

11. Backup

Voor centrale backups wordt gebruik gemaakt van een SAN-systeem. Commvault is de software die hiervoor wordt gebruikt. De aan te bieden hard- en software moet hierop aan sluiten. Het SAN maakt geen deel uit van het servernetwerk, op dit moment worden backups via switches naar de cloud (AWS) getransporteerd. Dagelijks worden incremental backups gemaakt van alle centrale systemen. Alle voor productie ingezette servers worden meegenomen in de dagelijks backup. Wekelijks vindt een full-backup plaats. Als middel om de backups te kunnen streamen wordt gebruik gemaakt van staging (disk-2-disk-principe). Backups worden (afhankelijk van de behoefte direct of later naar de cloudstorage weggeschreven. Aan het einde van de maand wordt de data van de backupfiler naar de cloudstorage weggeschreven.

Daarnaast worden van alle bedrijfskritische systemen dmv Oracle archive logging online mutaties bewaard. De maximale verlies-tijd van database transacties wordt daarmee theoretisch beperkt tot 10 minuten.
Voor deze backup wordt gebruik gemaakt van een separate NetApp filer.
Het NAS-systeem op de filer maakt online-snapshots mogelijk. Van alle CIFS volumes wordt dan ook 4 per dag een snapshot gemaakt. Ook voor LUN of NFS-gebaseerde opslag is het mogelijk op relatief snelle wijze een kloon of snapshot te maken.

12. Virtualisatie

Applicatieservers worden gevirtualiseerd op een VMware-omgeving. De VMware hosts maken gebruik van meerdere gezamenlijk datastores op het NAS. Door deze configuratie is een High Availability omgeving gecreëerd waarin de ene VMware host de virtuele machines van de andere host over kan nemen. De VMware hosts zijn voorzien van VMware Infrastructure 8 (ESXi 8) en staan fysiek gescheiden over twee lokaties. De lokaties zijn door middel van glas aan elkaar gekoppeld.
De Oracle-databases worden gevirtualiseerd op een Oracle VM omgeving, waarbij virtuele VM's zijn toegewezen aan de diverse gemeentes die worden gehost. nb: Q4-24/Q1,2-25: in overgang naar VMware m.u.v. Weblogic ivm licentie-model G+Z. Tot einde uitfasering Weblogic.
Citrix Virtual Apps Servers en Citrix Virtual Desktops worden gevirtualiseerd op Citrix Hypervisor
Oracle VM's draaien nu ook op VMware!

13. Beveiliging

Functionele organisatie

Functies zijn gesplitst in gebruikers, functioneel applicatiebeheerders en systeembeheerders (technisch applicatiebeheerders).
Systeem- en databasebeheer zorgt voor het uitvoeren van updates in samenspraak met de functioneel applicatiebeheerder en de leverancier.
Functioneel applicatiebeheer zorgt voor alle zaken binnen de applicatie (toekennen van menu's, privileges etc.)
Eerst geven systeembeheerders een gebruiker toegang tot een applicatie en vervolgens stelt de functioneel beheerder in welke rechten de gebruiker binnen de applicatie heeft.

De gebruiker heeft geen mogelijkheden om op de centrale servers (Windows en Unix) andere dingen te doen dan alleen het opstarten van applicaties of het wegschrijven van data of bestanden. De functioneel applicatiebeheerder heeft een aantal extra mogelijkheden. In principe kan niemand anders dan de systeembeheerders op de Windows servers en/of Unix-prompt wezenlijke wijzigingen aanbrengen.

Systeembeheer heeft de volledige rechten op alle systeem- en applicatie-software. Een aparte rol is weggelegd voor de leverancier die voor aparte doeleinden remote kan inloggen op het systeem. Als een leverancier incidenteel toegang nodig heeft dan wordt toegang gegeven dmv Teamviewer. Wanneer een leverancier regelmatig werkzaamheden moet uitvoeren dan kan de leverancier een eigen account krijgen. De MFA loopt dan via een interne gebruiker, bv een applicatiebeheerder.

Technische organisatie

Van buitenaf is het netwerk beschermd door een firewall. Hiermee is toegang tot en van het Internet geregeld. Koppelingen met landelijke voorzieningen, ketenpartners en leveranciers gaan encrypted en/of via Diginet. Tevens wordt voor sommige functionaliteiten zoals de portal (via 2FA) de Netscaler voor hardening gebruikt.

Alle binnenkomende bestanden worden gescand.

Bestanden met de extensie .zip of .doc worden doorgezet met een waarschuwing in de mail ze alleen te openen als je het vertrouwt. Bestanden met de extensie .exe worden in quarantaine geplaatst. Dit geldt ook voor bestanden met de extensie .zip afkomstig van andere domeinen dan .nl of .com.
(Dit is nu door MS Defender geregeld, Policies bepalen of emails eerst in Quarantaine komen voordat deze door een beheerder vrijgegeven of verwijdert worden)

Alle bijzondere bestanden worden alleen op verzoek van de gebruiker en na goedkeuring van de postmaster doorgezonden. Als het niet mogelijk is om een bijzonder bestand te scannen, wordt het bestand in quarantaine geplaatst en wordt de verantwoordelijkheid bij de eindgebruiker gelegd.

Voor het beschikbaar houden van de technische infrastructuur zijn maatregelen getroffen voor continuïteit en/of beheerste shutdown.

De gemeente heeft grote delen van de technische infrastructuur dubbel uitgevoerd en een eigen uitwijk ingericht. Deze uitwijk kan voor een groot deel in werking treden binnen één uur. Alleen herstel van externe verbindingen duurt langer.

Om de mobiele apparatuur te beveiligen, maken de gemeenten gebruik van Microsoft Intune Endpoint Manager voor het beheren van de persoonsgebonden laptops en smartphones van de vaste medewerkers. Voor de smartphones wordt dit in combinatie met Samsung Knox gebruikt. Voor on-premises en cloud-applicaties wordt de login verzorgd door Microsoft EntraID via het SAML of OpenID Connect protocol. HelloID wordt daarnaast in gezet voor User-provisioning via het SCIM protocol of eventueel andere API's.

14. **Monitoring**

De ICT-infrastructuur wordt pro-actief gemonitord met behulp van Zabbix. Naast servers en koppelingen, worden onderdelen van applicaties zoveel mogelijk in de monitoring opgenomen.