STANDAARD ICT ARCHITECTUUR

VERSIE 19 SEPTEMBER 2022

Inhoudsopgave

1 Inleiding

1.1 Algemeen

Dit document beschrijft de standaard ICT-infrastructuur. Referentiekader voor de ICT-infrastructuur is het automatiseringsbeleid, het ICT-onderhoudsplan en de landelijke gemeentelijke architectuur (GEMMA).

1.2 Documenteigenschappen

Eigenaar
Afdelingsmanager Dienstverlening
Gemeente Veenendaal

Eerste vaststelling
19 december 2005

Laatste aanpassing
22 september 2022

Doel
Het document is voor:

- Leveranciers : waar dienen hun te implementeren componenten aan te voldoen;
- Klanten : afspraken over de standaard werkplek en standaardproducten en diensten.

1.3 Standaard ICT-infrastructuur

In de volgende hoofdstukken volgt de beschrijving van de standaard ICT-infrastructuur. Deze vormen meteen de te stellen eisen aan een te selecteren oplossing. De te selecteren oplossing mag hiervan niet afwijken. Wanneer er niet voldaan wordt aan een eis, wordt de partij uitgesloten van deelname. In de kolom ‘BEWIJS’ toont de partij aan dat en hoe zij zich conformeert aan de eis.

Deze beschrijving van de ICT-infrastructuur is onder meer van belang bij inkoop en aanbesteding van applicaties of andere componenten die in onze ICT-infrastructuur worden opgenomen. In het PvE zijn dit eisen waaraan de nieuwe componenten moeten voldoen. De door de inschrijver te leveren apparatuur en/of software en de daarbij behorende drivers dienen te functioneren op basis van de platformen zoals omschreven in dit document.

2 Algemeen

2.1 Voldoen aan de ICT-infrastructuur

Het door u te leveren systeem (hard- en/of software en de daarbij behorende drivers) werkt probleemloos binnen de ICT-infrastructuur van de gemeente Veenendaal. Het voldoet aan de beschrijving van de ICT-omgeving van de Gemeente Veenendaal. Beschrijf van uw te leveren systeem het volgende:

- Technische randvoorwaarden voor de database-, applicatie- en webservers (operating systeem, hardware eisen)
- De database (leverancier, versie, licentie binnen of buiten de aanneemsom, randvoorwaarden)
- Technische randvoorwaarden voor de cliënt (operating systeem, hardware eisen)
- Invulling van de middleware
- Vereisten voor het netwerk
- Inrichting van de beveiliging

Geef een technisch schema en overzicht van de informatiearchitectuur van uw systeem (in een schema voorzien van een toelichting).

Beschrijf uw:

- Certificeringen (ISO, NEN)
- Lidmaatschap van beroepsvereniging(en)
- Bedrijfsprotocollen

2.2 Voldoen aan GEMMA en Common Ground uitgangspunten

Uw oplossing voldoet aan de principes van de Gemma en de uitgangspunten van Common Groud. Verbindingen of SaaS-diensten moeten via GGI-Netwerk gerealiseerd een aangeboden worden.

2.3 Service

U heeft een in Nederland gevestigde Nederlandstalige helpdesk of ondersteuningskantoor. Ondersteuning wordt in het Nederlands geboden.
U biedt:

- Serviceovereenkomst (7x24 of 5x10 binnen 4 uur of 8 uur reageren)
- Onderhoudsovereenkomst (patches, updates, nieuwe versies)

2.4 Licentiestructuur

U geeft inzicht in de licentiestructuur, zowel in de verschillende elementen als de wijze waarop de aantallen zijn gebaseerd (aantal inwoners, formatieplaatsen, users, devices, enzovoort).

2.5 OTAP

Voor kritische bedrijfstoepassing moet een testomgeving beschikbaar zijn. Daarbij wordt de OTAP-aanpak gehanteerd, waarbij verschillende activiteiten in gescheiden omgevingen worden uitgevoerd om mogelijke verstoringen van productie en andere test processen te voorkomen.

Ontwikkel: Omgeving waar software (maatwerk) en inrichtingsmodellen ontwikkeld worden.

Test: Omgeving waar vastgesteld wordt of de ontwikkelde software goed functioneert binnen de kaders van de infrastructuur. Specifieke eigenschap van deze omgeving is dat deze zonder verstorende invloeden van andere applicaties en netwerk beschikbaar kan zijn om het technisch testen zo zuiver mogelijk kunnen laten verlopen.

Acceptatie: Omgeving waar de functioneel beheerder eventueel samen met een aantal toekomstige gebruikers de goede werking van de applicatie test. Specifieke eigenschap van deze omgeving is dat deze identiek is aan de productie omgeving om het testen zo natuurgetrouw mogelijk te laten zijn.

Productie: Omgeving waar de bedrijfsapplicatie hoogbeschikbaar is voor de gebruikers.
Aangezien er vrijwel uitsluitend standaard applicaties worden aangeschaft, zullen er geen Ontwikkel- en Testomgevingen nodig zijn, maar volstaat het om naast de productieomgeving een Acceptatieomgeving in te richten, waarbij geprobeerd wordt de productieomgeving zo goed mogelijk na te bootsen. Doel van de acceptatieomgeving is, te verzekeren dat een nieuwe of aangepaste applicatie naar behoren functioneert in de standaard infrastructuur en daarmee goed integreert zonder de operationele omgeving te verstoren. Wijzigingen op applicaties worden daarom eerst aangebracht in de acceptatieomgeving om:

- de gebruikers in de gelegenheid te stellen de applicatie grondig functioneel te testen zonder de operationele omgeving te verstoren;
- fouten in de productieomgeving te kunnen reproduceren en mogelijke oplossingen te kunnen testen.

2.6 Integratie

Nieuwe applicaties koppelen met bestaande applicaties op basis van onderstaande uitgangspunten.
De koppelvlakken zijn gebaseerd op open standaarden, zoals XML en SOAP webservices.

BETREFT	COMPONENT	TOELICHTING
Enterprise Service Bus		Digikoppeling OpenTunnel StUF
Data-distributie		Key2Datadistributie / Key2VOA / Key2GBA-V StUF
ETL		ETL ten behoeve van Management Informatie Pentaho

3 SAAS (CLOUD)

3.1 Algemeen

In geval van SAAS gelden de in dit hoofdstuk genoemde uitgangspunten. De overige hoofdstukken zijn dan alleen van toepassing indien ze betrekking hebben op de SAAS-dienst. Bron: Factsheet SaaS van de IBD.

3.2 Verwerkersovereenkomst

De verwerkersovereenkomst van de IBD is van toepassing.

3.3 SaaS-infrastructuur en Privacy

Privacy is tegenwoordig het belangrijkste thema voor SaaS infrastructure. Dit is een gevolg van het invoeren van de GDPR die wettelijke vereisten voor privacy dicteert. Security en privacy zijn nauw met elkaar verbonden want SaaS Privacy is afhankelijk van SaaS Security. Hoewel bedrijven zelf verantwoordelijk zijn voor de naleving van de GDPR, moeten SaaS-providers ervoor zorgen dat de privacyregels geïmplementeerd zijn en blijven. De SaaS infrastructure moet hierop zijn ingericht.

Privacyregels variëren enorm per land en regio en de SaaS-applicatie moet voldoen aan al die regels. Voor SaaS-providers is het belangrijk om ten volle te profiteren van EU Safe Harbor-bepalingen om de aansprakelijkheid met betrekking tot de EU-privacywetgeving te minimaliseren. Dit is een belangrijk element voor het selecteren van een SaaS oplossing, biedt het product voldoende waarborgen om te voldoen aan de GDPR.

3.4 SaaS-infrastructuur en Security

SaaS-security was altijd de grootste zorg van bedrijven die SaaS wilden gebruiken. SaaS-providers nemen namelijk veel van de verantwoordelijkheden met hun SaaS Infrastructure platform op zich. Deze verantwoordelijkheden liggen traditioneel bij de IT afdeling van het bedrijf. De nieuwe verantwoordelijkheden van SaaS-providers omvatten:

- Gebruikersauthenticatie en toegangscontrole. De authenticatie en autorisatie verloopt via ADFS.
- Bescherming tegen ongeoorloofde toegang.
- Code hardening en auditing.
- Malware-detectie en verwijdering.
- Verdediging tegen bedreigingen zoals DDoS aanvallen.
- Fysieke beveiliging van de serverlocaties.
- Bescherming tegen toegang door andere gebruikers op hetzelfde systeem.
- Toegang en verbindingen zijn veilig (minimaal HTTPS).

Uw dienst geeft invulling aan de Factsheet:

- SaaS-dienst van de Informatiebeveiligingsdienst (IBD), zie bijlage.
- Cloud Computing en de BIG, zie bijlage.

3.5 Data Governance

Data Governance is ook een van de grotere zorgen van bedrijven die naar de cloud verhuizen. Datamanagement was iets waar softwareleveranciers zich vroeger geen zorgen over hoefden maakten. Het enige wat zij moesten doen is de software juist installeren en instellen. Het beheer van de data was de verantwoordelijkheid van de klant of hun IT-afdeling. Bij Cloud-modellen is de SaaS-provider, vaak in samenwerking met de IaaS- of PaaS-providers, volledig verantwoordelijk voor het beschermen van de data.

Datamanagementprocessen zijn de basis voor het invullen van de security-, privacy- en compliancerequirements. De kwaliteit van de data is belangrijk, vooral omdat er steeds meer data uit Social Media en big data bronnen in de SaaS-oplossing zijn geïntegreerd.

Een ander Data Governance aandachtspunt bij SaaS is het eigendom van de data. Veel bedrijven benadrukken niet alleen dat ze rechten hebben op alle data die wordt geproduceerd door de SaaS-applicaties, maar ook op de afgeleide data die gebruikt wordt voor datamining en analyse. Bekijk het contract en de SLA hoe dit is geregeld.

We kunnen bij de data voor management informatie

3.6 Compliantie-eisen voor SaaS infrastructuren

In alle sectoren van de samenleving zijn de compliance vereisten in de afgelopen jaren enorm toegenomen. Compliance, zoals beveiliging, heeft een grotere impact op de SaaS provider dan op on-premise softwareleveranciers. Dat komt omdat zij ook operationele verantwoordelijkheden hebben voor het systeem en de bijbehorende data. Implementatie van software op locatie was primair de verantwoordelijkheid van de IT-afdeling van het bedrijf en in de tweede plaats de verantwoordelijkheid van de softwareleverancier. Die situatie is omgedraaid voor SaaS-toepassingen.

Compliance kwesties houden verband met requirements voor beveiliging en privacy, maar kennen zeer specifieke overheidsvereisten, een breder toepassingsgebied en mogelijk een hogere boetes.

3.7 Beschikbaarheid van systemen

Hoewel de meeste bedrijven een lagere beschikbaarheid van hun on premise systemen hebben dan SaaS-providers, vormde de beschikbaarheid van de SaaS infrastructure een belangrijke barrière voor de acceptatie van SaaS. Een SaaS infrastructure kent meerdere componenten met ieder hun eigen beschikbaarheidskenmerken. Omdat het uitvallen van een van deze componenten ertoe kan leiden dat de SaaS-oplossing wegvalt, moet de SaaS-provider zijn infrastructuur zo ontwerpen dat hij meerdere redundante systemen gebruikt om een hogere mate van beschikbaarheid te garanderen.

SaaS-klanten met hoge beschikbaarheidseisen zullen ervoor zorgen dat ze toegang hebben tot hun data in het geval van een storing bij de SaaS-provider. Zij zullen eisen dat de SaaS-provider over een Disaster Recovery plan beschikt.

3.8 Performance

Performance is vaak een van de zorgen als een SaaS applicatie via internet wordt aangeboden. De prestaties van webtoepassingen moeten op meerdere plaatsen worden ingesteld.

- De applicatie moet op een bepaalde manier worden geprogrammeerd om optimaal te profiteren van de technieken.
- Content Delivery Networks (CDN's) kunnen worden gebruikt om inhoud fysiek dichter bij de eindgebruiker te cachen en zo laadtijden te versnellen.
- Netwerkoptimalisatietechnieken kunnen worden gebruikt om data efficiënter te streamen.
- Effectief schalen van de omgeving moet kunnen door virtuele machines toe te voegen en acceptabele prestaties te leveren.
- Een stabiele internet verbinding met een hoge bandbreedte op alle locaties waar gewerkt is noodzakelijk.

3.9 Integratie van SaaS-applicaties

Een gebrek aan integratiemogelijkheden met bestaande systemen is een veel genoemde belemmering voor bedrijven om naar de cloud te verhuizen. Integratie met andere SaaS-oplossingen, cloud-applicaties en legacy-systemen is een grote wens van veel bedrijven.

Koppelingen tussen on-premise softwaresystemen onderling is al tientallen jaren een probleem. In sommige On-premise-omgevingen is Service Oriented Architectures (SOA) geïmplementeerd om een goede interface te bieden voor de legacy applicaties. Een goede SaaS infrastructure biedt echter geen mogelijkheden om direct toegang te krijgen tot de data. Alle toegang tot data loopt via de SaaS-applicatie. Gelukkig bieden de meeste leveranciers API's om systemen te kunnen koppelen. Desondanks is het complex om meerdere SaaS en legacy on-premise systemen te integreren.

4 Datacenter

4.1 Computerruimten Twin Datacenter

Onze infrastructuur is opgebouwd op basis van twee gelijkwaardige datacenters, welke redundant is uitgevoerd. De datacenters zijn gevestigd in het gemeentehuis van Veenendaal en bij het datacenter BIT in Ede.

Redundantie en clusteren van systemen zijn uitgangspunt bij het toevoegen of vervangen van componenten in de ICT-infrastructuur.

Toegang tot computerruimten en patchkasten is fysiek beveiligd met pasjes en sleutels.

4.2 Stroomvoorziening (NSA, UPS)

IT beheert de UPS (unattended power supply). IT werkt met UPS voor continue stroomvoorziening ter bescherming van de servers. Stroomstoringen en meldingen zo spoedig mogelijk doorgeven aan de helpdesk. Het aanschaffen en beheren van de UPS wordt door IT gedaan.

Voor beide computerruimten in Veenendaal en BIT Ede wordt door middel van NSA gezorgd voor beschikbaarheid van stroom, ook bij stroomuitval.

4.3 Koeling

Redundante aircovoorzieningen in computerruimten.

4.4 Computervloer

Verhoogde computervloer.
Verstevigde computervloer voor gewichtsverdeling over de hele vloeroppervlakte.

4.5 Racks

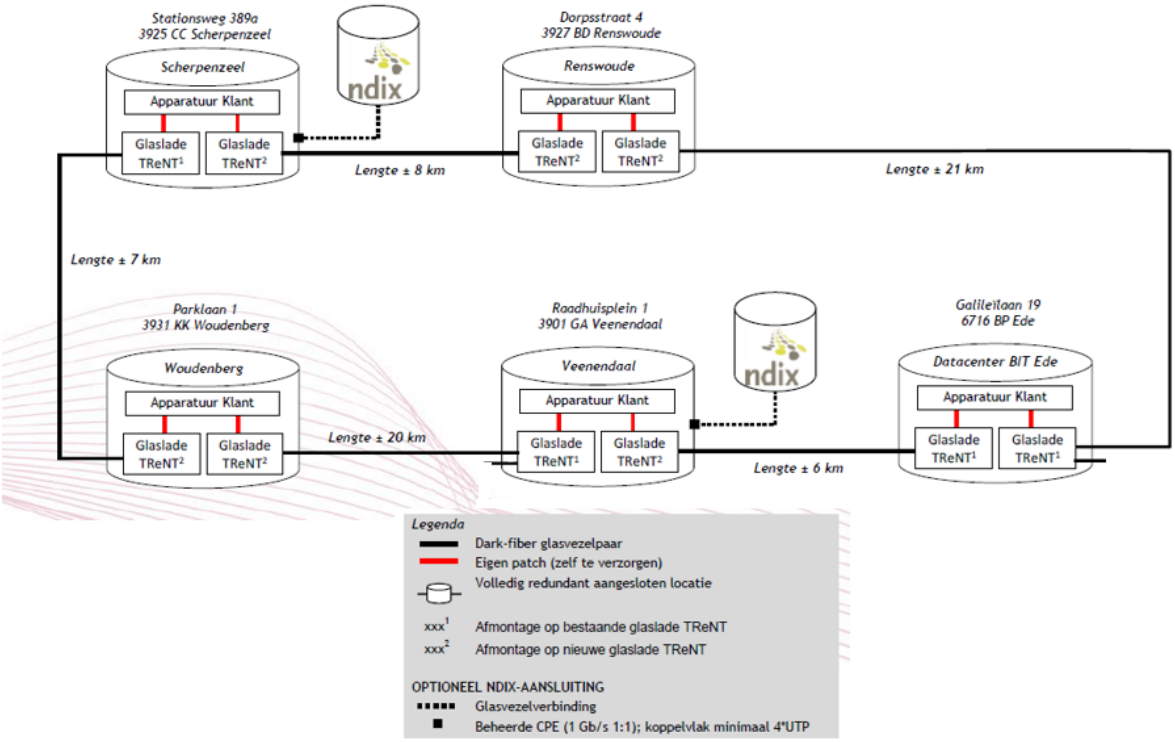
Gestandaardiseerd. Kabelmanagement.

5 Connect

5.1 DF-ring (WAN)

Een Wide Area Network (WAN) is een netwerk dat twee of meer lokale netwerken (LAN's) verbindt die geografisch verspreid zijn. De gemeente koppelt de LAN-omgevingen van vestigingen via het WAN aan de hoofdlocatie via glasvezel. De LAN's van externe (trusted) partijen worden gekoppeld via de firewallinfrastructuur. Andere koppelingen worden via routers aan de firewall geplaatst. De gemeentelijke locaties vormen, via glasvezel verbonden, één netwerk. Deze glasvezelverbindingen zijn via CWDM-componenten (fiber optics) gekoppeld.

BETREFT	COMPONENT	TOELICHTING
WAN	SOLID OPTICS	Solid Optics passieve componenten voor belichting glasgezelverbindingen van TReNT, KPN en Eurofiber



5.2 Lokaal netwerk

Het Local Area Network (LAN) is een essentiële schakel in de ICT-infrastructuur. Het is de lokale verbinding tussen de eindgebruikers (clients) en servers. Het netwerkverkeer op het LAN is in de loop der jaren toegenomen. Deze toename is het gevolg van een verdergaande automatisering en toename in de dataopslag en grafisch werk. Fast Ethernet (100 Mbps) en Gigabit Ethernet (1Gbps oftewel 1000 Mbps) worden momenteel ingezet. Er

zijn ook mogelijkheden om op 10 Gbps te werken, daarvoor moeten speciale afmontages van de glasvezel-componenten worden toegepast. Advies is om het gebruik van Ethernet te continueren.

Ons netwerk is ingericht volgens het *'Collapsed Backbone Model*. Deze architectuur is een backbone topologie waarbij de patchkasten op de verschillende verdiepingen in een sterconfiguratie zijn verbonden met een centrale high performance switching patchkast. Onze centrale MER's (Main Equipment Rooms ofwel computerruimtes) in de gemeentehuis Veenendaal en BIT Ede zijn gekoppeld met meerdere SER's (Secondary Equipment Rooms ofwel patchkasten).

De backbone (ruggengraat van het netwerk) is gebaseerd op 10 Gb (over glasvezel). In de computerruimten staan met name de centrale massaopslag (SAN), centrale core switches en de servers. In de patchkasten staan de switches in de racks, waar de apparatuur van de eindgebruiker op is aangesloten.

We werken met gestandaardiseerde netwerkswitches en routers. De actieve componenten zijn gebaseerd op open standaards. De patchkasten zijn met glasvezel verbonden aan de computerruimten. Vanaf de patchkasten naar de werkplek ligt koperbekabeling. Enkele nevenlocaties zijn via ADSL-lijnen verbonden aan ons netwerk.

BETREFT	COMPONENT	TOELICHTING
Netwerk Core		Fortigate netwerksegmentering en virtuele domeinen. Routering
Draadloos netwerk		FortiAP.
Netwerk Edge		HP Switching
Storage netwerk		Dell EMC Fiber Channel Storage Network

5.3 Toegang tot internet en Diginetwerk

Doordat de gemeente steeds meer dienstverlening via het Internet aanbiedt, is het niet wenselijk om afhankelijk te zijn van één ISP. In beide datacenters zijn er meerdere ISP- of Internetverbindingen ingepast om het niveau van digitale dienstverlening aan de burger te garanderen. In de toekomst redundant blijven uitvoeren op 2 ontsluitingspunten.

BETREFT	COMPONENT	TOELICHTING
Internet Access		Eurofiber, voor zakelijke toepassingen
		Ziggo voor algemeen browsen
Digi-netwerk		Diensten verder uitgaande van GGI-netwerk uitgangspunten.

5.4 Network Protocol en Adress Management

Het gebruikte netwerkprotocol is TCP/IPv4. Voor het beheer is ondersteunende programmatuur vereist om de beheerder in staat te stellen effectieve subnet strategieën te bepalen en te implementeren, DHCP en DNS-server architecturen te ontwerpen (bij voorbeeld, geclusterde vs. gedistribueerde redundante servers) en de uitgifte van IP-adressen aan IP-apparatuur. Openbare IP-adres ranges moeten worden aangevraagd en DNS-domein namen moeten worden aangevraagd en gepubliceerd. Het is belangrijk nu te inventariseren op welke punten de processen en IT-infrastructuur in uw organisatie aangepast dienen te worden voor het inzetten van IPv6. Er zijn een aantal keuzes te maken, en de impact van de verkeerde keuze kan grote gevolgen hebben. Denk bijvoorbeeld aan het onderzoeken of de apparatuur al geschikt is voor IPv6 of dat er in de nabije toekomst ondersteuning voor IPv6 beschikbaar zal zijn. Advies is om bij toekomstige investeringen na te gaan of de apparatuur IPv.6 is gecertificeerd of hiervoor is voorbereid.

5.5 Power over Ethernet (PoE)

Steeds meer apparaten, zoals netwerkcomponenten, access point, camera's en telefoontoestellen worden via Ethernet van stroom voorzien. Dit heft als voordeel het aantal stroomkabels te beperken, betrouwbaardere stroomvoorziening en betere noodstroomvoorzieningen, beter beheermanagement en tevens de mogelijkheid tot verdere standaardisatie. Advies is om bij toekomstige investeringen in apparatuur en netwerkbekabeling rekening te houden met PoE.

5.6 Telefonie

We beschikken over een redundante Mitel telefooncentrale die de vestigingen ondersteund. Daarnaast wordt gebruik gemaakt van een GSM-voorzieningen. Deze zijn via Vast-Mobiel integratie gekoppeld. Voorzien is de migratie naar GT-connect.

6 Compute & Store

6.1 Servers

We gaan uit van virtualisatie. Servers worden virtueel uitgevoerd onder VMware vSphere. De desktops zijn met VMware Horizon gevirtualiseerd.

BETREFT	COMPONENT	TOELICHTING
Servers		Dell servers.

6.2 Clients

BETREFT	COMPONENT	TOELICHTING
Desktops, NUC's, laptops, workstations, monitoren		Workstations en desktops.
Thin clients		Op basis van Thin OS en PCoIP als protocol. Worden momenteel uitgefaseerd door laptops.
Tablets, smartphones		Beheerd via Microsoft Intune.

Sommige toepassingen maken gebruik van speciale randapparatuur. Rechtstreekse aansluiting van dergelijke apparatuur aan een (virtuele) server is niet mogelijk.

Randapparatuur kan via goedkeuring door ICT worden aangesloten aan een werkstation op basis van USB of rechtstreeks aan ethernet op basis van IP.

6.3 Storage

Voor het opslaan van data hanteren we de volgende uitgangspunten:

- Documenten worden, cf. autorisatie, geplaatst op de virtuele fileserver en in de Office 365 cloud;
- Applicaties komen op een daarvoor ingerichte virtuele applicatieserver; één applicatie op één virtuele applicatieserver;
- De databases worden op de Oracle database-infrastructuur geplaatst en beheerd;

- Mails komen op de (Exchange Online) mailserver;
- Programmatuur en data worden gescheiden opgeslagen;
- Er mogen geen vaste driveletters worden gebruikt; er mag geen gebruik gemaakt worden van vaste paden; instellingen van paden (installatiemap, etc.) moeten met parameters gezet kunnen worden.
- De benodigde ruimte aan diskcapaciteit moet minimaal zes weken van tevoren worden opgegeven. Zonder een ruim van tevoren afgegeven indicatie kan er geen garantie gegeven worden dat er voldoende diskruimte beschikbaar is.
- Data wordt gerepliceerd opgeslagen.

BETREFT	COMPONENT	TOELICHTING
SAN	FUJITSU	Fujitsu Eternus AF250 Full Flash SAN (redundant en gerepliceerd) in de datacenters Veenendaal en BIT Ede.
NAS	FUJITSU	Fujitsu NAS.
SDS	ATLANTIS	Voor VDI wordt Atlantis USX ingezet in combinatie met locale storage op de VMware servers. Wordt momenteel uitgefaseerd.

6.4 Backup & Restore

BETREFT	COMPONENT	TOELICHTING
On premise Backup & Restore	VEEAM rubrik	Dell backupserver en disktarget. Voor backup zijn Dell tapedrives en tapeunits ingezet (LTO). De backup's worden gemaakt met Veeam Backup & Restore. Backup van alle virtuele servers en de Oracle RMAN backup bestanden. In onderzoek is een transitie van de on premise backup & restore omgeving naar een tapeless backup & restore.
Cloud Backup & Restore	AvePoint	Cloud Backup & Restore ten behoeve van Microsoft 365.

7 Deployment

7.1 Identity Management en Autorisaties

BETREFT	COMPONENT	TOELICHTING
Account-beheer	SMARTAIM	Het beheer van accounts met SmartAIM incl. rechtenbeheer op en binnen applicaties.
Autorisaties	SMARTAIM	Beschrijf: - De ondersteuning van single sign-on - Hoe de toegang van de gebruikers in een applicatie of softwarepakket is georganiseerd, geprogrammeerd. Is dit in de applicatie opgelost, via Microsoft Active Directory, LDAP of anders? - Hoe de autorisatie binnen de applicatie georganiseerd is - Dongels, HASP (hardwarematige licenties) of licenties gebaseerd op de hardware zijn niet toegestaan (uitwijkconcept). - Hoe dit AD-gebaseerd werkt.
Directory		Microsoft Active Directory. LDAP-connectiviteit zodat een gebruikersaccount niet op 2 verschillende locaties aangemaakt hoeft te worden
Federatie SSO		Beschrijf in geval van SaaS hoe SSO en federatie van accounts is geregeld. Dit moet minimaal mogelijk zijn via OAuth.

Elke gebruiker dient een toepassing onder een eigen gebruikersnaam te benaderen.

Iedere gebruiker dient met een eigen login via de applicatie in te loggen op de database. Wanneer binnen een applicatie gebruik wordt gemaakt van een netwerklogin, dan dient er binnen de applicatie een autorisatiesysteem aanwezig te zijn en moet het mogelijk zijn een gebruiker te koppelen aan processen binnen de database.

Als er een eigen autorisatiesysteem binnen de applicatie is en er gebruik wordt gemaakt van één gemeenschappelijke database gebruikersnaam, dan mag deze niet de eigenaar van het schema zijn en of DBA-rechten hebben. In de documentatie dient duidelijk opgenomen te zijn hoe de verschillen in de autorisatie geregeld kunnen worden.

Alle wachtwoorden die worden opgeslagen in de database dienen versleuteld te zijn. Wachtwoorden mogen niet leesbaar in bestanden of databases worden opgeslagen. In een toepassing dient een mogelijkheid opgenomen te zijn om het eigen wachtwoord zelf te vernieuwen.

Er worden geen wachtwoorden gebruikt in scripts e.d. Er mag geen gebruik worden gemaakt van standaard door leveranciers aangeleverde wachtwoorden. Standaardwachtwoorden van leveranciers worden na installatie door de systeem-/netwerkbeheerder gewijzigd.

Er mag geen gebruik worden gemaakt van speciale hardware zoals een dongel.

In applicaties ingebouwde functionaliteit, of via een applicatie benaderbare functionaliteit, die potentiële beveiligingsrisico's met zich mee brengt (bijvoorbeeld toegang tot een commandoprompt) kan door het team ICT

worden geweigerd of uitgeschakeld. Het gebruik en het functioneel beheer van de applicatie moeten zodanig zijn ingericht, dat hiervoor geen bijzondere rechten (zoals SYS ADMIN) noodzakelijk zijn.

7.2 Serverdeployment

BETREFT	COMPONENT	TOELICHTING
Virtuele Servers		MS Windows Server Datacenter template SCCM
Database-servers	ORACLE	Oracle Linux
Applicatie-servers	ORACLE	Oracle Linux
		MS Windows Server Datacenter 2022 EE 64bit of hoger
Achtergrond-processen		MS Windows Server Datacenter 2022 EE 64bit of hoger

7.3 Databases

BETREFT	COMPONENT	TOELICHTING
Databases	ORACLE	Oracle Enterprise Edition.

7.4 Desktopdeployment

BETREFT	COMPONENT	TOELICHTING
Desktops		Fat clients op basis van Microsoft Windows 11. Autopilot, Intune
Virtuele Desktops		Virtuele desktops met Windows 11 op basis van PCoIP. SCCM
Windows OS		Autopilot, Intune

7.5 Device management

BETREFT	COMPONENT	TOELICHTING
Desktops	LIQUIT	Autopilot, Intune, Liquit
Laptops	LIQUIT	Autopilot, Intune, Liquit
Thin clients	DELL	Wyse Device Management
Tablets en Smartphones		Intune

7.6 Applicationdeployment

BETREFT	COMPONENT	TOELICHTING
Packaging	LIQUIT	Liquit Setup Store
Set-up & Distributie	LIQUIT	Liquit Setup store
Applicatie-virtualisatie		Wordt niet toegepast.

Voor toepassingen geldt het volgende:

a. Er moet gebruik gemaakt worden van door de gemeente gebruikte versies van besturingssystemen, database management systemen en middleware componenten.
b. Voor alle software geldt dat deze moet voldoen aan de richtlijnen van de fabrikant van het besturingssysteem waarop de software wordt geïnstalleerd.
c. De leverancier dient aan te geven wat de frequentie is van reguliere updates.
d. Specificaties van hard- en software moeten vroegtijdig worden opgeleverd.
e. Ondersteuning door de leverancier dient gedurende de geplande gebruiksduur gewaarborgd te zijn.
f. Bij oplevering van de toepassing dient er overdracht plaats te vinden aan het team ICT van de handleidingen, installatiebeschrijving, licentiegegevens, etc.
g. Alle te installeren software wordt aangeleverd op dusdanige wijze, dat deze binnen de gemeente gearchiveerd kan worden en gebruikt kan worden bij herinstallaties.
h. Na afsluiting van een applicatie moeten de gebruikte resources worden vrijgegeven en moeten tijdelijke bestanden worden opgeruimd.
i. Een niet meer gebruikte applicatie moet verwijderd kunnen worden.

7.7 Patchmanagement

BETREFT	COMPONENT	TOELICHTING
Ivanti Patch	ivanti	Ivanti Patchmanagement
Applicaties	LIQUIT	Setup Store

7.8 File- en mailservices

BETREFT	COMPONENT	TOELICHTING
Fileserver		Microsoft Windows Server. Wordt gemigreerd naar Office 365 (SharePoint, Teams).
Mailserver		Office 365.
Veilig verzenden grote bestanden	zivver	Zivver.

7.9 Licentie- en certificaatmanagement

BETREFT	COMPONENT	TOELICHTING
Licentie-server		Virtuele licentieserver op basis van MS Windows Server.
Certificaat-server		Virtuele certificaatserver op basis van MS Windows Server.

7.10 Printen, kopiëren en scannen

BETREFT	COMPONENT	TOELICHTING
Printserver	uniFLOW	MS Windows Server met Canon Uniflow t.b.v. Follow-me printing.

8 Security & Monitoring

8.1 Edge

BETREFT	COMPONENT	TOELICHTING
Firewall		Firewallinfrastructuur. De firewallinfrastructuur beschermt de voor- en achterdeuren van onze ICT-infastructuur en bestaat uit de volgende onderdelen: - FortiGate: firewall (IP-filtering, NAT-vertaling, VPN, DNS, Authenticatie, Bandbreedte Management, http-screening) - FortiMail: mailscanning (smtp-screening) - FortiAnalyser: logging, analyse - FortiAP: Wi-Fi. Deze infrastructuur is voor beschikbaarheid en continuïteit redundant uitgevoerd. VPN (SSL) en twee DMZ-zones voor webtoegang.
Externe toegang		FortiWeb: toegang van buiten af tot webapplicaties.
	vmware	VMware Security Server i.c.m. VMware Horizon View Client.
		Censornet MFA: toepassing voor strong authentication voor veilige (secure) toegang tot webapplicaties en/of VDI.
Sandboxing		Voor sandboxing aan de deur wordt Forigate sandboxing ingezet.
Segmenten		Segmentering en Demilitarized Zones. De DMZ fungeert als een soort loopgracht tussen het interne - veilige - netwerk en de buitenwereld. In de praktijk staat de DMZ tussen twee firewalls of er zijn aan de firewall drie segmenten gekoppeld: een intern segment, een extern segment en een LAN segment. Segmentering tussen netwerk segmenten.
VLAN's		Netwerken worden virtueel van elkaar gescheiden om reden van beveiliging of routeren van verkeer.

8.2 Active Defense

BETREFT	COMPONENT	TOELICHTING
Deep Discovery Inspection		Hiervoor wordt Trend Micro Deep Discovery Inspector ingezet. Incl. sandboxing.

8.3 Endpoints

BETREFT	COMPONENT	TOELICHTING
MDM		Microsoft Intune
AV/AS		Virussen, spam en spyware worden een steeds grotere bedreiging. Bij vermoeden van de aanwezigheid van virussen, spam en spyware en andere bedreigingen, meldt een ieder dit direct aan de helpdesk. Steeds geldt als er rare dingen gebeuren of bijzonder meldingen verschijnen: laat de PC aanstaan en neem direct contact op met de helpdesk. Het in bedrijf houden van onze systemen is een gezamenlijke verantwoordelijkheid. We maken gebruik van Microsoft Defender for Endpoints.

8.4 Certificaten en encryptie

BETREFT	COMPONENT	TOELICHTING
Encryptie		Versleutelen: - Internetverkeer (http en smtp) - Netwerkverkeer - Databases - File- en mailservers - Servers en SAN - Endpoints
Certificaten		Certificaten en certificaatbeheer

8.5 Fysieke toegangsbeveiliging

Fysieke toegangsbeveiliging: de toegangscontrole werkt op basis van pasjes voor de medewerkers en bezoekers. De toegang kan per deur ingesteld worden. Met het camerasysteem worden op strategische plekken opnames gemaakt en vastgelegd om achteraf situaties te kunnen analyseren.

8.6 Beschikbaarheid van applicaties via Internet

Toepassingen die vanuit Internet benaderbaar zijn, worden geplaatst in de DMZ en ontsloten via firewallrules. Communicatie tussen internet en netwerk verloopt altijd via de DMZ. De toepassing in de DMZ is de enige die mag communiceren met het internet en het netwerk. Er is dus nooit rechtstreeks verbinding tussen internet en netwerk. De leverancier dient aan te geven van welke specifieke poorten gebruik zal worden gemaakt. Het gebruik van ‘ranges’ van poorten is niet toegestaan.

Bij toepassingen die vanuit Internet benaderbaar zijn, wordt encryptie van gegevens en cookies toegepast.

De webapplicaties moeten aantoonbaar gevrijwaard zijn van minimaal de OWASP top 10 webapplicatie kwetsbaarheden.

8.7 Remote support

Inbel- of remote support is alleen toegestaan via een door de gemeente Veenendaal ter beschikking gestelde voorziening (portaal met persoonsgebonden token en clientsoftware op basis van Secure IP). De leverancier krijgt de beschikking over een account met de overeengekomen autorisaties. Dit account staat standaard ‘dicht’, maar wordt op verzoek en in overleg met de functioneel beheerder en ICT tijdelijk opengezet. Eventuele alternatieven van derden worden alleen toegestaan na uitdrukkelijke toestemming van de teamcoördinator ICT & Inkoop van de gemeente Veenendaal.

8.8 Monitoring

BETREFT	COMPONENT	TOELICHTING
Service-monitoring		TOPdesk
System-monitoring	centreon	Centreon
Database-monitoring	ORACLE	Cloud Control
Security-monitoring		FortiAnalyzer
Klimaat-monitoring	ATAL	Datacenter sensoren