

1. Managementsamenvatting

De gemeente Amersfoort vernieuwt de infrastructuur voor Storage, Compute en Backup om een toekomstbestendige, veilige en beheersbare basis te creëren voor de gemeentelijke informatievoorziening. De huidige omgeving ondersteunt de bedrijfsvoering goed, maar bevindt zich in een transitie naar een hybride architectuur waarin cloud en OnPremise voorzieningen naast elkaar bestaan. Deze PSA beschrijft de architectuurkaders voor de aanbesteding. Het Programma van Eisen (PvE) vertaalt deze kaders naar toetsbare functionele, technische en beheereisen.

De doelarchitectuur is gebaseerd op modulaire bouwblokken* voor Storage, Compute, OnPremise Backup, Microsoft 365 Backup, Security en Beheer. Door deze scheiding kunnen bouwblokken onafhankelijk worden vervangen, opgeschaald of uitbesteed. Daarmee wordt vendor lock-in beperkt, blijft de gemeente regie houden op haar gegevens en ontstaat een flexibele infrastructuur die aansluit bij GEMMA, NORA en de BIO.

Een **architectuurbouwblok is een **herbruikbaar, logisch afgebakend onderdeel van een architectuur** dat een specifieke functie of capability beschrijft, zonder direct vast te leggen hoe deze technisch wordt geïmplementeerd.*

2. Aanleiding, doel en scope

2.1 Aanleiding

De bestaande infrastructuur is ingericht rondom twee gemeentelijke datacenters met een active - active opzet*. De aanbesteding heeft als doel deze infrastructuur toekomstbestendig te vernieuwen, waarbij continuïteit van dienstverlening, informatiebeveiliging en schaalbaarheid centraal staan. Tegelijkertijd sluit de gemeente aan bij landelijke ontwikkelingen zoals Common Ground en de Nederlandse Digitale Strategie.

**Het begrip active-active is dus NIET op systeem niveau; waarbij meerdere systemen tegelijkertijd actief één bron benaderen voor lees- en of schrijfacties.*

2.2 Doel

Deze PSA beschrijft de architectuuruitgangspunten voor de aanbesteding. Zij vormt het kader waarbinnen het PvE is opgesteld. De PSA beschrijft waarom de architectuur is ingericht zoals zij is; het PvE beschrijft wat de leverancier moet leveren.

2.3 Scope

- Storage
- Compute
- OnPremise Backup
- Microsoft 365 Backup
- Security
- Beheer

Buiten scope vallen applicaties, kantoorautomatisering en netwerkdiensten, behoudens de architectuurafhankelijkheden.

3. Architectuurvisie

De gemeente kiest voor een hybride informatievoorziening waarin cloud en OnPremise voorzieningen elkaar aanvullen. Cloud is het voorkeursplatform, tenzij eisen op het gebied van prestaties, continuïteit, datasoevereiniteit, wet en regelgeving of kosten een lokale voorziening noodzakelijk maken. De infrastructuur wordt opgebouwd uit modulaire bouwblokken met een duidelijke scheiding van verantwoordelijkheden tussen gemeente en leverancier.

De architectuur ondersteunt een gefaseerde migratie, waarbij bestaande dienstverlening beschikbaar blijft. De omgeving moet hoog beschikbaar zijn, eenvoudig uitbreidbaar zijn en voldoen aan de eisen uit de BIO, AVG en overige relevante wet en regelgeving.

4. Governance

4.1 Uitgangspunt

De gemeente Amersfoort voert regie op haar informatievoorziening en blijft eindverantwoordelijk voor de continuïteit, veiligheid en kwaliteit van de dienstverlening. De leverancier levert, beheert en ondersteunt de overeengekomen bouwblokken binnen de afgesproken servicelevels, terwijl de gemeente eigenaar blijft van de architectuur, de gegevens en de strategische keuzes.

De governance is gebaseerd op **situationele regie**: per bouwblok wordt bewust bepaald welke verantwoordelijkheden bij de gemeente liggen en welke aan de leverancier worden belegd. Hiermee wordt een goede balans gevonden tussen ontzorging, flexibiliteit en behoud van regie.

4.2 Eigenaarschap

Voor ieder bouwblok wordt een duidelijke eigenaar aangewezen. De eigenaar is verantwoordelijk voor de functionele ontwikkeling, lifecycle, risicoafweging en aansluiting op de gemeentelijke architectuur.

Rol	Verantwoordelijkheid
Gemeente	Architectuur, beleid, informatiebeveiliging, gegevens, lifecycle, contractsturing en strategische keuzes.
Leverancier	Levering, technisch beheer, onderhoud, beschikbaarheid, beveiligingsupdates en afgesproken dienstverlening.
Product Owner Product Manager	Prioritering van wijzigingen, afstemming met gebruikers en bewaking van de functionele behoefte.
Architect	Bewaken van de architectuurprincipes, samenhang tussen bouwblokken en toetsing van wijzigingen.

Enterprise Architect	Toetsing aan de gemeentelijke architectuur, strategische uitgangspunten en uitzonderingen op architectuurprincipes.
Contractmanager	Bewaken van contractafspraken, SLA's, leveranciersprestaties en escalaties.

4.3 Lifecyclemanagement

Alle bouwblokken worden gedurende hun volledige levenscyclus actief beheerd. Dit omvat planning van lifecyclevervangingen, capaciteitsuitbreidingen, beveiligingsupdates, technische vernieuwingen en gecontroleerde uitfasering.

Door lifecyclemanagement als integraal onderdeel van de governance op te nemen wordt voorkomen dat technische schuld ontstaat en blijft de infrastructuur toekomstbestendig.

4.4 Wijzigings- en architectuurgovernance

Wijzigingen aan de infrastructuur worden getoetst aan de architectuurprincipes uit deze PSA. Wijzigingen die invloed hebben op de samenhang tussen bouwblokken, datasoevereiniteit, beveiliging of leveranciersafhankelijkheid worden vooraf beoordeeld door de architectuurfunctie.

Hiermee wordt geborgd dat individuele wijzigingen niet leiden tot ongewenste afhankelijkheden of afbreuk doen aan de doelarchitectuur.

6.5 Contract- en leverancierssturing

De gemeente stuurt op resultaten en dienstverlening in plaats van op individuele technische componenten. De leverancier rapporteert periodiek over beschikbaarheid, prestaties, beveiliging, lifecycle, capaciteit en afgesproken KPI's.

Door de infrastructuur op te delen in zelfstandige bouwblokken blijft het mogelijk onderdelen afzonderlijk te vervangen of opnieuw aan te besteden zonder de volledige infrastructuur te wijzigen. Hiermee worden leveranciersafhankelijkheid en vendor lock-in beperkt en behoudt de gemeente maximale regie over haar informatievoorziening.

5. IST situatie

De huidige infrastructuur van de gemeente Amersfoort is ingericht als een hybride OnPremise platform dat de primaire gemeentelijke dienstverlening ondersteunt. De omgeving bestaat uit twee geografisch gescheiden datacenterlocaties die gezamenlijk een active - active infrastructuur vormen. Deze architectuur biedt een hoge beschikbaarheid en maakt het mogelijk om de dienstverlening bij uitval van één locatie gecontroleerd voort te zetten.

5.1 Huidige architectuur

De huidige omgeving bestaat uit een virtualisatieplatform op basis van VMware ESX, ondersteund door een stretched storage oplossing. De primaire opslag is gebaseerd op HPE Nimble All Flash storage. Daarnaast is een afzonderlijke NetApp NAS omgeving

aanwezig voor specifieke opslagbehoeften. De datacenters zijn verbonden via redundante dark fiberverbindingen waardoor synchrone replicatie tussen beide locaties mogelijk is.

5.2 Bouwblokken van de huidige omgeving

Bouwblok	Huidige inrichting
Storage	HPE Nimble All Flash storage verdeeld over twee datacenters met synchrone replicatie.
Compute	VMware virtualisatieplatform waarop de gemeentelijke servers en databases draaien.
OnPremise Backup	Veeam gebaseerde backup omgeving met kruislingse replicatie tussen beide datacenters conform het 3-2-1 principe.
Microsoft 365 Backup	Cloudgebaseerde Barracuda oplossing voor Exchange Online, SharePoint, Teams en OneDrive.
NAS	NetApp opslag voor specifieke opslagfunctionaliteit.
Netwerk	Redundante dark fiberverbindingen tussen beide datacenters.

5.3 Beheerorganisatie

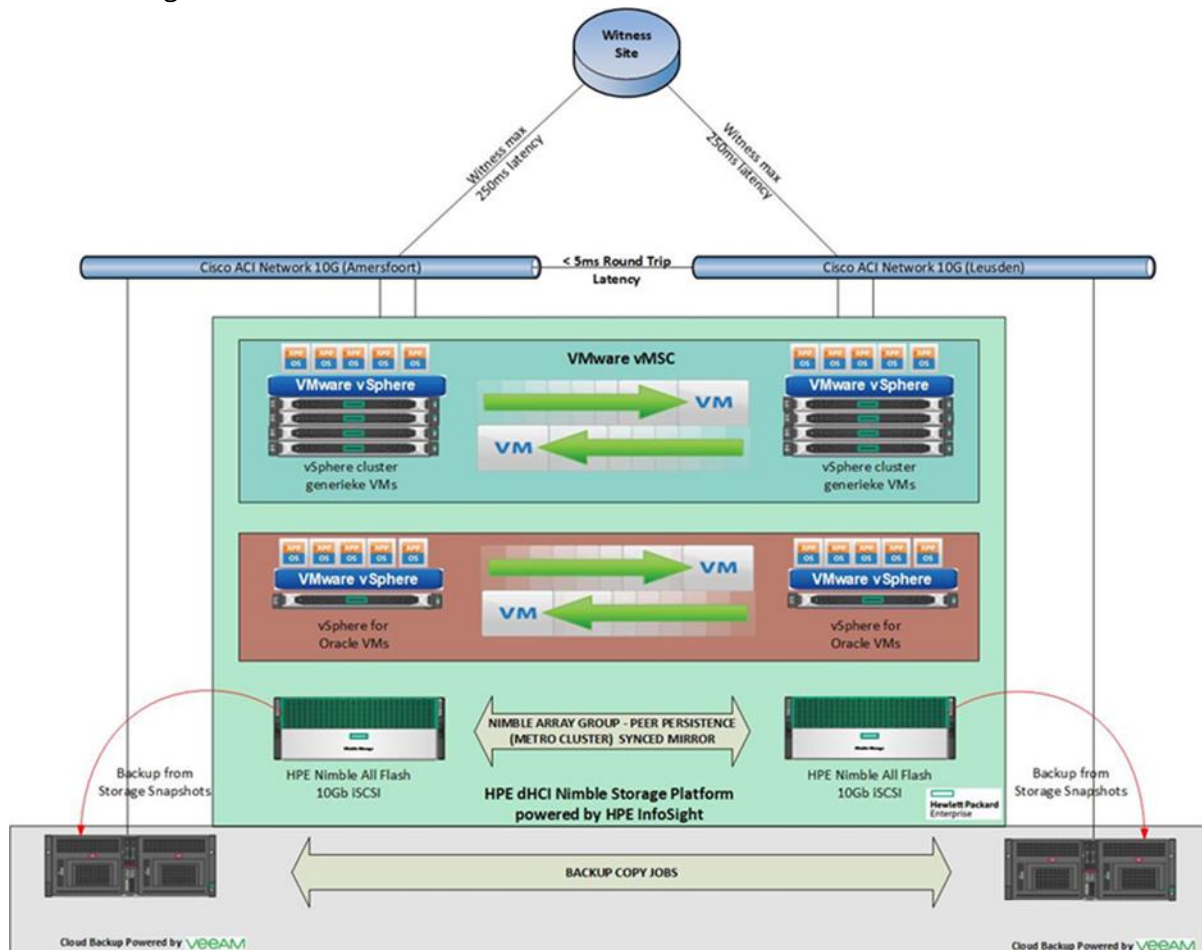
Het beheer is verdeeld tussen leverancier en gemeente. De leverancier is verantwoordelijk voor het beheer van de fysieke infrastructuur, storage, compute hardware, firmware en de virtualisatielaag. De gemeente beheert het besturingssysteem, de middleware, de applicaties, de autorisaties en de uitvoering van restore acties.

5.4 Belangrijkste kenmerken

- Hybride OnPremise infrastructuur met twee datacenters.
- Active - active inrichting voor Storage en Compute.
- VMware als virtualisatieplatform.
- HPE Nimble All Flash storage als primaire opslag.
- NetApp NAS als aanvullende opslagvoorziening.
- OnPremise Backup met replicatie tussen beide locaties.
- Microsoft 365 Backup via Barracuda (in de cloud).
- Redundante dark fiberverbindingen tussen de datacenters.
- Architectuur gericht op hoge beschikbaarheid, continuïteit en schaalbaarheid.

5.5 Architectuurschets huidige situatie

De technologische Bouwstenen



Het huidige OnPremise storage & compute concept

De VMware omgeving van gemeente Amersfoort is, dat bij uitval van 1 van de datacenters, 75% van de totale workload op het overgebleven datacenter moet gaan draaien. Dit proces vindt automatisch plaats. Om dit te realiseren wordt gebruik gemaakt van vSphere HA in combinatie met VM- en host groups en Should rules.

5.6 Analyse van de huidige situatie

De huidige architectuur biedt een stabiele en hoog beschikbare basis voor de gemeentelijke dienstverlening. Tegelijkertijd is de omgeving opgebouwd uit meerdere leverancier specifieke componenten en afzonderlijke beheeroplossingen. De gewenste doelarchitectuur richt zich daarom op een modulaire opbouw in zelfstandige bouwblokken, een duidelijke scheiding van verantwoordelijkheden en een betere aansluiting op de hybride cloud strategie van de gemeente. Deze uitgangspunten vormen de basis voor de architectuurvisie en de bouwblokken in de volgende hoofdstukken van deze PSA.

5.7 De huidige situatie in cijfers

Omgeving	Configuratie
Storage & Compute	Common Cluster Compute 8 × HPE ProLiant DL360 Gen10 8SFF (1U) 2 × CPU per host • 16 cores per CPU @ 2,7 GHz 1 TB RAM per host
	SQL Cluster Compute 2 × HPE ProLiant DL360 Gen10 hosts Intel Xeon Gold 5217 (3,0 GHz, 8 cores) 768 GB RAM per host
	Oracle Cluster Compute 2 × HPE ProLiant DL360 Gen10 hosts Intel Xeon Gold 5217 (3,0 GHz, 8 cores) 512 GB RAM per host
	VMware Witness Server HPE ProLiant DL360 1 × Intel Xeon-B 3204
	Storage 2 × HPE Nimble AF40 All-Flash Storage Arrays (4U)
Backup voorziening (on-site BaaS)	2 × HPE DL380 Gen10 (2U) 2 × HPE D6020 Disk Expansion Units (5U) VEEAM Backup & replication (HDD)
NetApp-omgeving	NetApp NAS-opslag (100 TB)
Microsoft 365 Backup	Barracuda Cloud-to-Cloud Backup-oplossing Cloud-to-Cloud Backup-licentie voor Microsoft 365

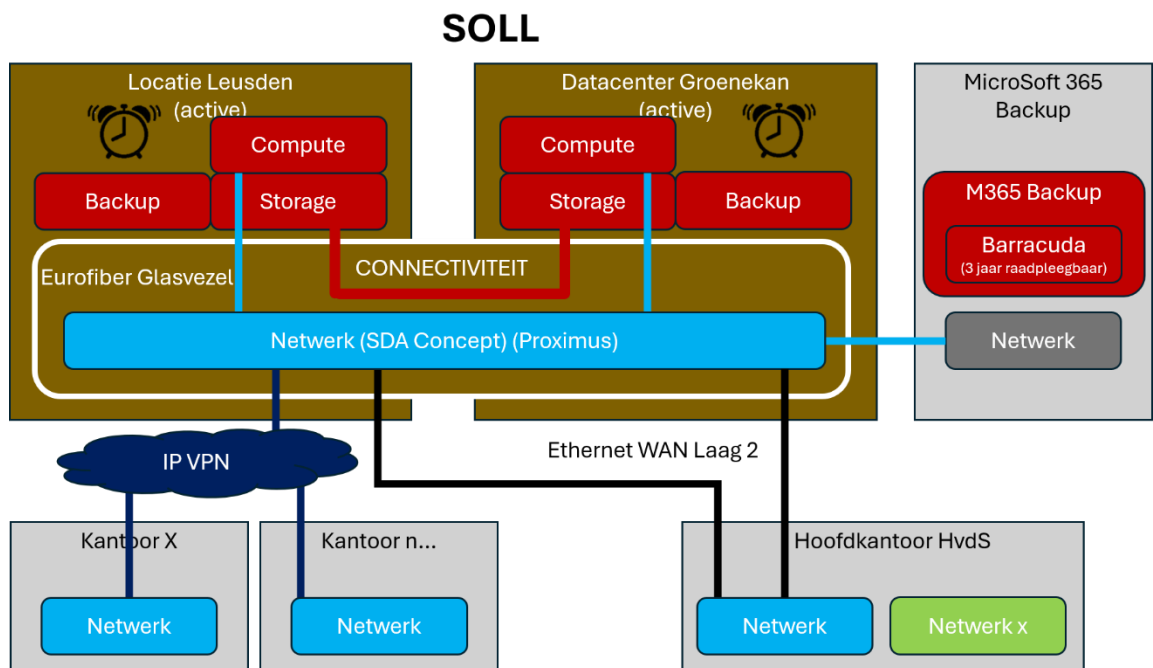
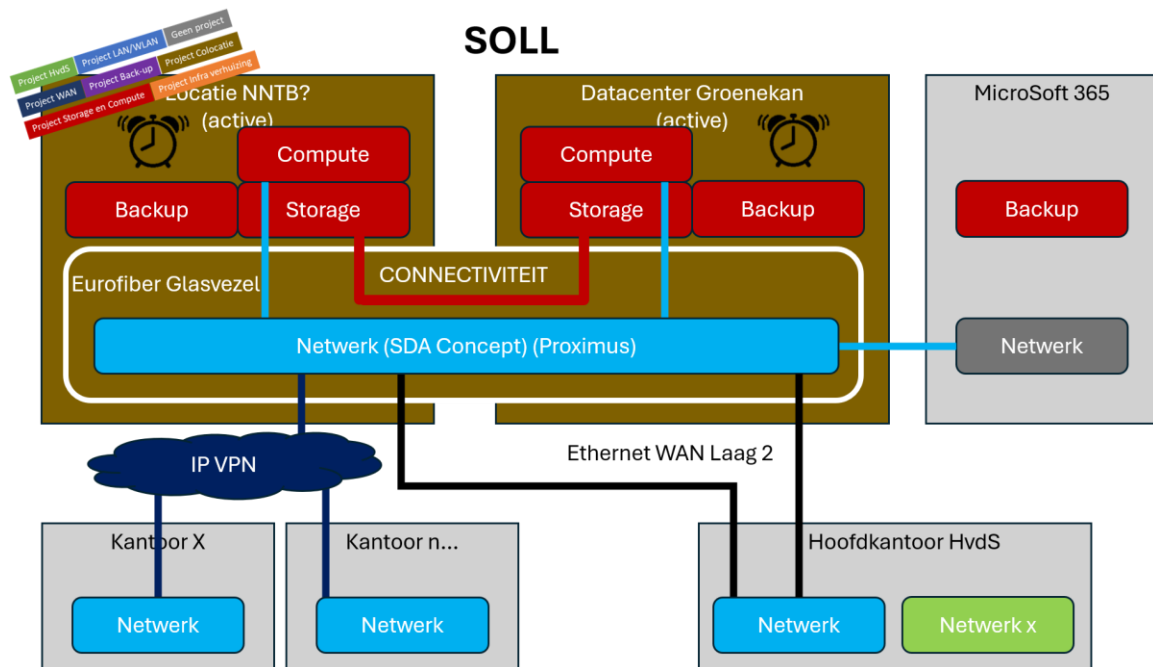
6. Toekomstige verwachte Architectuur

6.1 SOLL Architectuur

De toekomstige Storage & Compute omgeving van Gemeente Amersfoort zal bestaan uit het volgende:

- De locatie Leusden zal blijven bestaan.
- De locatie voor het nieuwe datacenter is Groenekan.
- Zowel de levering en beheer van hardware als de virtualisatie technologie valt in scope van deze aanbesteding.

Hieronder een situatieschets voor de SOLL situatie.



Om de **SOLL-situatie** te bereiken, is onderstaande figuur opgenomen ter ondersteuning van het voorstel voor de mogelijke transitiepaden. Momenteel bevinden we ons in een overgangsfase naar een nieuw netwerk, gebaseerd op de **Cisco SDA-architectuur**. Tegelijkertijd verhuist de **Gemeente Amersfoort** naar een nieuw stadhuis. Zodra de **Storage- en Compute-omgeving** wordt opgeleverd, zullen deze worden geplaatst in

Leusden en Groenekan. De verwachting is dat zowel het netwerk als de locaties bekend en operationeel zullen zijn op het moment van gunning.

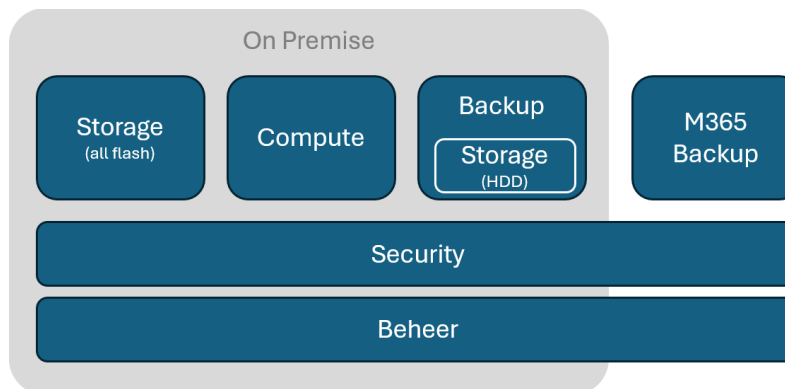
6.2 Architectuurprincipes

De volgende principes vormen de basis voor alle ontwerpkeuzes binnen deze aanbesteding.

Principe	Rationale	Implicaties
Modulaire bouwblokken	Vergroot flexibiliteit en vervangbaarheid.	Storage, Compute, Backup, en M365 backup Security en Beheer worden zelfstandig ontworpen.
Open standaarden	Voorkomt leveranciersafhankelijkheid.	Gebruik van gestandaardiseerde API's, protocollen en authenticatiemechanismen.
Security by Design	Beveiliging is integraal onderdeel van het ontwerp.	IAM, logging, encryptie, hardening en monitoring zijn onderdeel van ieder bouwblok.
Datasoevereiniteit	De gemeente behoudt regie over gegevens.	Bewuste keuzes voor opslaglocatie, encryptie en beheer.
Situationele regie	Niet ieder bouwblok vraagt dezelfde mate van uitbesteding.	Per bouwblok worden verantwoordelijkheden expliciet vastgelegd.
High Availability	Continuïteit van dienstverlening is essentieel.	Redundante Active - active inrichting en automatische failover.
Schaalbaarheid	Capaciteit moet kunnen meegroeien.	Modulaire uitbreiding zonder herontwerp.
Scheiding van verantwoordelijkheden	Duidelijke governance vermindert beheerlast.	Leverancier beheert infrastructuur; gemeente beheert platformgebruik en applicaties.
Meetbaarheid	Kwaliteit moet aantoonbaar zijn.	Monitoring, auditlogging en rapportages zijn onderdeel van de dienstverlening.

Deze architectuurprincipes vormen het toetsingskader voor de verdere uitwerking van de bouwblokken in de volgende hoofdstukken van de PSA en zijn leidend voor de vertaling naar het Programma van Eisen.

6.3 Bouwblokken



6.3.1 Bouwblok Storage

Centrale opslagvoorziening voor de OnPremise infrastructuur.

Rol binnen de architectuur

- Storage vormt de basis voor alle virtuele workloads en ondersteunt zowel bedrijfskritische applicaties als databases en bestanden.

Architectuuruitgangspunten

- Active - active storage verdeeld over twee datacenters.
- Synchrone replicatie tussen locaties.
- Ondersteuning voor NAS functionaliteit en bestaande NetApp functionaliteit tijdens de transitie.
- Opslagcapaciteit modulair uitbreidbaar met minimaal 100 TB zonder herontwerp.

Samenhang

- De oplossing sluit aan op de netwerkarchitectuur met redundante glasvezelverbindingen.

Ontwerpkeuzes

- Storage (All Flash) wordt logisch losgekoppeld van On Premise Compute en Storage (HDD) wordt logisch losgekoppeld van On Premise Backup, zodat beide bouwblokken onafhankelijk kunnen groeien of worden vervangen. De architectuur voorkomt productspecifieke afhankelijkheden waar mogelijk.

Relatie met PvE

- Het PvE werkt deze uitgangspunten uit in eisen voor prestaties, capaciteit, replicatie, beschikbaarheid en beheer.

6.3.2 Bouwblok Compute

Virtualisatie en reken capaciteit voor de gemeentelijke informatievoorziening.

Rol binnen de architectuur

- Compute levert de capaciteit waarop virtuele servers, databases en ondersteunende infrastructuur draaien.

Architectuuruitgangspunten

- Active - Active inrichting over twee datacenters.
- Automatische fail over bij uitval van één locatie.
- Ondersteuning voor bestaande SQL en Oracle workloads.
- Virtualisatieplatform centraal beheerd door de leverancier.
- Capaciteit modulair uitbreidbaar.

Samenhang

- Compute maakt gebruik van het Storage bouwblok en wordt beschermd door OnPremise Backup.

Ontwerpkeuzes

- Het virtualisatieplatform blijft generiek zodat toekomstige vervanging of uitbreiding mogelijk blijft zonder ingrijpende wijzigingen aan applicaties.

Relatie met PvE

- Het PvE beschrijft de eisen voor capaciteit, beschikbaarheid, prestaties, lifecycle en beheer.

6.3.3 Bouwblok OnPremise Backup

Bescherming van alle OnPremise workloads.

Rol binnen de architectuur

- Waarborgt herstel na calamiteiten en ondersteunt de continuïteit van de gemeentelijke dienstverlening.

Architectuuruitgangspunten

- 3-2-1 Backup principe, en daarop verschillende varianten.
- Replicatie tussen beide datacenters.
- Encryptie tijdens transport en opslag.
- Regelmatige restoretesten.
- Retentie conform gemeentelijk beleid en VNG richtlijnen.

Samenhang

- Beschermt alle workloads binnen het Compute en Storage bouwblok.

Ontwerpkeuzes

- Backup is een zelfstandig bouwblok zodat toekomstige vervanging onafhankelijk van Storage of Compute mogelijk blijft.

Relatie met PvE

- Het PvE bevat de functionele eisen voor retentie, monitoring, herstelpunten, rapportages en dienstverlening.

6.3.4 Bouwblok Microsoft 365 Backup

Bescherming van Microsoft 365 SaaS data.

Rol binnen de architectuur

- Beschermt gegevens binnen Exchange Online, SharePoint Online, OneDrive en Microsoft Teams tegen verwijdering, corruptie en ransomware.

Architectuuruitgangspunten

- Volledige dekking van Microsoft 365 diensten.

- Granulaire herstelmogelijkheden.
- Ondersteuning voor retentiebeleid.
- Veilige authenticatie via moderne standaarden.
- API ondersteuning voor monitoring en rapportages.

Samenhang

- Vormt een zelfstandig SaaS bouwblok naast de OnPremise Backup voorziening.

Ontwerpkeuzes

- De Microsoft 365 Backup wordt als managed dienst geleverd en sluit aan op het centrale Identity & Access Management.

Relatie met PvE

- Het PvE specificeert de eisen voor beveiliging, retentie, herstel, rapportages, schaalbaarheid en compliance.

6.3.5 Bouwblok Security

Security is een generiek bouwblok dat alle overige bouwblokken ondersteunt. De beveiliging wordt vanaf het ontwerp geïntegreerd (Security by Design) en voldoet minimaal aan BIO, AVG en relevante NIS2 uitgangspunten.

Identity & Access Management

- Authenticatie via moderne standaarden (SAML, OpenID Connect).
- Ondersteuning voor MFA en centrale IAM integratie.
- Rolgebaseerde autorisatie (RBAC) en least privilege.

Platformbeveiliging

- CIS hardening waar toepasbaar.
- Patchmanagement en lifecyclebeheer.
- Encryptie van data tijdens transport en opslag.
- Zero trust als uitgangspunt.

Monitoring & Detectie

- Centrale logging en audittrail.
- Koppeling mogelijk met SIEM/monitoringplatform.
- Periodieke vulnerability scans en pentesten.

Continuïteit & Compliance

- Ondersteuning voor restoretesten.
- Rapportages voor audits en ENSIA.
- Voldoen aan gemeentelijke beveiligingsrichtlijnen.

6.3.6 Bouwblok Beheer

Het beheer wordt ingericht volgens een duidelijke scheiding van verantwoordelijkheden tussen leverancier en gemeente.

Onderdeel	Leverancier	Gemeente
Hardware	Beheer, onderhoud, firmware	Toezicht

Storage & Compute	Technisch beheer t/m virtualisatie	OS en applicatiebeheer
Backup	Backup dienst en platform	Restore, retentiebeleid
Security	Platform hardening en updates	IAM, autorisaties, beleid
Monitoring	Technische monitoring	Operationele opvolging

7. Afhankelijkheden en randvoorwaarden

De architectuur kent de volgende randvoorwaarden:

- Twee geografisch gescheiden datacenters met redundante verbindingen.
- Gefaseerde migratie zonder verstoring van de dienstverlening.
- Opschaling van Storage en Compute zonder herontwerp.
- Ondersteuning voor bestaande SQL , Oracle en VMware workloads gedurende de transitie.
- Open standaarden en API's waar mogelijk.
- Documentatie, kennisoverdracht en beheerprocessen maken onderdeel uit van de dienstverlening.

8. Relatie met het Programma van Eisen

Deze PSA beschrijft de architectuurkaders en ontwerpprincipes. Het Programma van Eisen vertaalt deze uitgangspunten naar objectief toetsbare eisen voor leveranciers. Wijzigingen in functionele eisen leiden niet automatisch tot wijzigingen van de architectuur, tenzij de doelarchitectuur verandert.

Traceability per bouwblok:

Bouwblok	PvE bevat o.a.
Storage	Capaciteit, prestaties, replicatie, beschikbaarheid
Compute	Virtualisatie, capaciteit, lifecycle
OnPremise Backup	Retentie, herstel, monitoring
Microsoft 365 Backup	SaaS Backup, retentie, security
Security	IAM, logging, encryptie, compliance
Beheer	SLA, dienstverlening, verantwoordelijkheden

9. Tot slot

De doelarchitectuur bestaat uit zelfstandige bouwblokken voor Storage, Compute, OnPremise Backup, Microsoft 365 Backup, Security en Beheer. Deze modulaire opzet ondersteunt een toekomstbestendige, veilige en schaalbare infrastructuur. De PSA vormt het architectuurkader voor de aanbesteding; het PvE werkt deze uitgangspunten uit in concrete eisen.