Bijlage 1C – Nadere eisen Azure landingzone

1. Inleiding
De Opdrachtnemer ontwikkelt, beheert en onderhoudt de software binnen een Azure landingzone die deel uitmaakt van een hub-spoke-architectuur. Binnen deze architectuur worden de infrastructurele voorzieningen centraal, binnen de hub, gefaciliteerd onder beheer van de Koninklijke Bibliotheek (KB). Het betreft onder andere Identity & Access Management (IAM), routering, firewalling, DNS en mailvoorzieningen. De Opdrachtnemer dient met de eigen landingzone en inrichting hierop aan te sluiten en binnen deze kaders te opereren.

Voordat een landingzone wordt uitgerold vindt een intake plaats met de Opdrachtnemer. Tijdens deze intake worden de indeling van de landingzone, de benodigde functionaliteiten, en de aansluiting op de centrale voorzieningen afgestemd. Daarnaast worden onder meer de toegangsvoorzieningen, het IP-plan en de benodigde stappen voor firewallregels besproken. Deze afstemming is bedoeld om te waarborgen dat de inrichting aansluit op de beveiligings- en beheerstandaarden van de organisatie.

In de volgende paragrafen worden de eisen en uitgangspunten ten aanzien van de Azure-landingzone en de onderliggende infrastructuur beschreven, geordend per logisch onderdeel. Deze eisen vormen het kader waarbinnen de Opdrachtnemer de omgeving dient te realiseren en te beheren.

2. Algemeen
De Opdrachtnemer host, ontwikkelt, beheert en onderhoudt software binnen een Azure landingzone die deel uitmaakt van een hub-spoke architectuur.

De KB levert en beheert de centrale infrastructurele voorzieningen (IAM, routering, firewalling, DNS, mailvoorziening). De Opdrachtnemer sluit hierbij aan op de centrale voorzieningen van KB.

3. Governance en Toegangsbeheer
Er wordt op basis van Azure Privileged Identity Management (PIM) en RBAC-rollen toegang verleend tot de landingzone binnen de relevante subscripties waarin de applicatie-infrastructuur wordt gehost en beheerd. De KB beheert de rechten tot de landingzone en gebruikers worden via een goedkeuringsflow toegevoegd.

- De Opdrachtnemer ontvangt van de KB specifieke admin accounts, indien de KB nog geen volwassen alternatief heeft (bijvoorbeeld Azure LightHouse).
- De Opdrachtnemer ontvangt minimaal Contributor-rechten binnen de subscriptie die relevant is voor het beheren en hosten van de applicatie-infrastructuur.

4. Security & Compliance
- De Opdrachtnemer krijgt via PIM toegang tot de beheerrollen binnen Azure, voor auditing- en logging doeleinden.
- Opdrachtnemer wordt geacht gebruik te maken van een keystore voor opslaan van wachtwoorden/secrets en certificaten.
- Opdrachtnemer maakt gebruik van door KB verstrekte certificaten (OV) voor publieke domeinen.
- Opdrachtnemer wordt geacht gebruik te maken van centraal beschikbaar gestelde log analytics workspace voor aggregeren en raadplegen applicatie en systeemlogging.
- Vanuit beveiligingsoogpunt zorgt de Opdrachtnemer ervoor dat de laatste stabiele versies en patches worden toegepast van de onderliggende software. Denk hierbij aan bijvoorbeeld webserver, database of operating system. Onderliggende software met een end-of-Life status wordt door Opdrachtnemer vermeden. Indien een oudere, of end-of-Life, versie van onderliggende software wordt toegepast dan levert fabrikant/ uitgever, in overleg met de KB, een roadmap aan waarin duidelijk wordt aangegeven in welke versie en op welk moment wordt overgegaan op de laatste versie of een alternatief product.

- Opdrachtnemer past controle op bekende kwetsbaarheden op haar source code toe (bv SAST voor statische code en DAST voor draaiende applicaties).
- De dienst doorstaat succesvol een (pen)test langs de lijnen van de OWASP Application Security Verification Standard (ASVS) c.q. Certified Secure Checklists.
- Opdrachtnemer versleutelt alle data-in-transit conform de 'Ict-beveiligingsrichtlijnen-voor-transport-layer-security-2025-05' van het NCSC.
- Opdrachtnemer past lifecycle management toe op software.
- Opdrachtnemer zorgt ervoor dat Microsoft Defender en Azure Policies periodiek worden gecontroleerd en aanbevelingen geïmplementeerd.
- KB controleert naleving via periodieke policies en Defender aanbevelingen.

5. Netwerk & Connectiviteit

- Hub/spoke model wordt gevolgd en inkomend en uitgaand verkeer loopt via de Hub wat in beheer is van de KB.
- KB beheert de API Management Service en Application Gateway, hiervoordient de Opdrachtnemer aanvraag te moeten doen om hier gebruik van te maken.
- De Opdrachtnemer zet de API Management Service in wanneer de API vanuit het internet toegankelijk moet zijn of wanneer deze over meerdere landingzones heen wordt gebruikt.
- De Opdrachtnemer houdt er rekening mee of de applicatie alleen toegankelijk is voor de KB en zorgt ervoor dat deze uitsluitend via de IP-adressen van de KB bereikbaar is.

6. Resource Management & Deployment

- Applicatie en infrastructuur componenten dienen obv Terraform met CI/CD pipelines naar gescheiden T, A en P omgevingen te worden uitgerold.
- Opdrachtnemer zorgt ervoor dat CI/CD pipelines worden gebruikt, voor het bouwen, testen en deployen van de applicatie.
- Opdrachtnemer voert vóór iedere deployment een vulnerability scan uit op alle gebruikte code, dependencies en componenten (inclusief container images) om ten minste bekende kwetsbaarheden (known vulnerabilities) te detecteren en te rapporteren. Geconstateerde kwetsbaarheden worden vervolgens opgelost conform de afspraken in de SLA.
- Opdrachtnemer gebruikt KB naamconventies voor Azure Resources die beschikbaar zullen worden gesteld.
- Opdrachtnemer zorgt ervoor dat de applicatie portable is door middel van containers.
- Azure-resources worden zorgvuldig gekozen waarbij rekening wordt gehouden met voldoende schaling, fouttolerantie, kostenefficiëntie, beveiliging rekening houden met specifieke eisen van bedrijfs- en applicatiekritische onderdelen. Uitgangspunt bij de keuze van resources is het streven naar een zo hoog mogelijk PaaS-niveau, zodat beschikbaarheid, beheerbaarheid en continuïteit optimaal zijn geborgd. Zie ook: https://learn.microsoft.com/en-us/azure/architecture/guide/technology-choices/technology-choices-overview.
- De Opdrachtnemer zorgt samen met de KB voor een synchronisatie van de git repositories naar de KB GitLab omgeving.

7. Dataverwering

- Opdrachtnemer verwerkt data AVG/GDPR-compliant.
- Opdrachtnemer houdt zich aan het dataclassificatiebeleid en residencyeisen.
- KB levert dataclassificatiebeleid en residencyeisen.

8. Operationeel werken

- Opdrachtnemer richt eigen alerting en monitoring in op applicatiekritische delen.
- Opdrachtnemer is in control over de incidenten en volgt deze op.
- Opdrachtnemer zorgt voor back-ups en Disaster recovery scenario's en deze worden getest en geborgd in het ontwerp.

9. Eigenaarschap en Exit-strategie

- Opdrachtnemer zorgt ervoor dat duidelijke en overdraagbare documentatie beschikbaar is.
- Opdrachtnemer zorgt voor documentatie en overdraagbaarheid van code wordt geborgd.
- De Opdrachtnemer zorgt ervoor dat de KB de intellectuele eigendomsrechten op de gemaakte code krijgt of behoudt.

10. Rapportage & Audit

- De KB houdt toezicht op de naleving van dit eisendocument door de Opdrachtnemer.
- De Opdrachtnemer dient volledige transparantie te bieden met betrekking tot de inrichting van de landingzone zodat de KB, wanneer nodig, gevraagd of ongevraagd aanbevelingen kan doen dan wel zaken bespreekbaar kan maken met de Opdrachtnemer over de inrichting en het beheer van de landingzone.

11. Eisen aan Opdrachtnemersorganisatie

- In het ontwerpen van de Azure landingzone is minimaal een “Microsoft Certified: Azure Solutions Architect” betrokken.
- Beschikt over aantoonbare ervaring met Cloud Native architectuurprincipes, waaronder containerization, microservices, CI/CD en Infrastructure as Code

12. Best Practices

- We werken volgens het CAF (Cloud Adoption Framework) als leidraad voor inrichting, governance en lifecycle management van workloads binnen Azure.
- PaaS en SaaS diensten hebben nadrukkelijk de voorkeur boven IaaS. IaaS wordt alleen toegepast als PaaS of SaaS geen passend alternatief biedt.
- App Services worden gebruikt voor hosting van webapplicaties waar mogelijk, om onderhoud, schaalbaarheid en security te vereenvoudigen.
- Container Registry wordt ingezet voor het veilig beheren en distribueren van container images.
- Managed identiteiten worden standaard toegepast voor authenticatie van applicaties en services binnen Azure, waarbij credentials niet handmatig worden beheerd.
- Federated Credentials worden gebruikt voor geautomatiseerde en veilige authenticatie zonder secrets of service principals met lange geldigheid. (bijvoorbeeld voor CI/CD pipelines)
- Infrastructure as Code (IaC) wordt consequent toegepast voor het uitrollen van infrastructuur en applicaties, inclusief governance en security policies.
- GitOps principes worden toegepast voor een transparante, controleerbare en reproduceerbare deployment pipeline.
- CI/CD pipelines worden ingericht volgens een shift-left security principe, waarbij securitychecks (zoals SAST, DAST en dependency scanning) zo vroeg mogelijk in het ontwikkelproces plaatsvinden.
- Logging en monitoring worden centraal georganiseerd via Log Analytics, Application Insights en Defender for Cloud om proactief beheer en incidentrespons te ondersteunen.
- Secrets worden nooit in code of pipelines opgenomen, maar altijd beheerd via Key Vault.
- Netwerktoegang tot resources is standaard minimaal (least privilege, zero trust).
- Vulnerability scanning en compliance checks worden geautomatiseerd uitgevoerd en nagevolgd.
- Back-ups en disaster recovery scenario’s worden getest en geborgd in het ontwerp.
- Er wordt gestreefd naar kostenoptimalisatie via reserveringen, autoscaling en het minimaliseren van onnodige resources.
- Documentatie over architectuur, implementaties en procedures blijft actueel en wordt opgeslagen in een centrale repository.
- Architectuurbesluiten worden volgens ADR (Architectural Decision Records) opgeslagen in een centrale repository.