Technische en organisatorische maatregelen (TOM's)

Status	Geldend leveranciersdocument
Versie / uitgiftedatum	1.0 / 28 augustus 2026
Documenteigenaar	Schmeitzke, handelend onder de namen Summa en Summa Labs
Classificatie	Publiek / due diligence

1. Reikwijdte

Deze maatregelen beschrijven het aantoonbare beveiligingsniveau van de actuele Summa-dienst. Zij zijn bedoeld als AVG artikel 32-bijlage, leveranciersbewijs en basis voor gemeentelijke securityreviews. Een maatregel wordt alleen als geïmplementeerd beschreven wanneer deze in de huidige code/configuratie aantoonbaar aanwezig is; gewenste verbeteringen staan expliciet als open actie.

2. Identiteit en authenticatie

- Authenticatie verloopt via een zelfgehoste ZITADEL-identityservice binnen de Summa-infrastructuur.
- Unieke accounts en rolgebaseerde autorisatie zijn verplicht voor werkruimten en beheerfuncties.
- Het eigenaar-/platformbeheervlak is uitsluitend bereikbaar op een private Tailscale-host, vereist de platform_admin-rol en dwingt MFA af.
- Platformbrede MFA-enforcement voor alle gewone accounts staat op uitgiftdatum uit. Zakelijke/overheidsproductie moet daarom MFA via het gekozen identity-/SSO-profiel verplicht stellen voordat gevoelige data wordt toegelaten.
- Development login is in productie uitgeschakeld.

3. Tenantisolatie en autorisatie

- De FastAPI-backend is de beleidsgrens: browserclients krijgen geen directe toegang tot database/modelservers.
- PostgreSQL Row Level Security en tenantcontext beperken data tot de actuele tenant.
- Applicatielaagautoriteit controleert aanvullend gebruikers-, tenant-, workspace- en roomrechten.
- Gedeelde rooms gebruiken expliciete membership/roles; cross-tenant toegang wordt slechts via één gecontroleerde resolutieroute toegestaan.
- Connectoren vereisen waar van toepassing deployment featuregate, tenantbeleid, access profile en per-user providerautorisatie.

4. Versleuteling en sleutelbeheer

- Publieke verbindingen gebruiken TLS.
- Gevoelige velden en tenantgebonden gegevensklassen worden applicatief versleuteld; tenant-scoped encryption is in productie verplicht.
- Secrets worden niet in ConfigMaps geplaatst wanneer zij geheim zijn; productiecredentials worden via versleutelde Kubernetes/SOPS secretbestanden geïnjecteerd.
- CI genereert tijdelijke test-encryptiesleutels en weigert bekende credentialbestanden in de repository.
- Voor een volledige cryptografische lifecycle worden sleutelrotatie, noodrotatie, keycustody en periodieke review volgens document 13 uitgevoerd.

5. Netwerkbeveiliging

- Externe route: Leafcloud load balancer -> ingress-nginx -> Next.js -> FastAPI.
- Databases, caches, modelgateways en interne toolservices hebben geen gewone publieke browserroute.
- Kubernetes network policies beperken service-to-service verkeer; geïsoleerde Python jobs draaien in een afzonderlijke namespace met default-deny ingress/egress.
- De web-retrievalbroker concentreert internet-egress en blokkeert SSRF via schemecontrole, DNS/IP-validatie, private/metadata-adresblokkade, IP-pinning, redirectherbeoordeling, bodylimieten en timeouts.

6. Upload- en contentbeveiliging

- Uploads gaan via de geauthenticeerde applicatieboundary naar private objectstorage.
- ClamAV-scanning is in productie vereist voordat uploads worden gebruikt.
- Tika/OCR heeft limieten op bestandsgrootte, geëxtraheerde tekst, pagina's, OCR-pages en timeouts om decompression/parser denial-of-service te beperken.
- Archive-expansie en file-aantallen zijn begrensd.
- Externe/imported documenten worden als onbetrouwbare input behandeld; zij krijgen geen implicit tool-/systeemautoriteit.

7. Geïsoleerde code-uitvoering

De Python tool draait in een tijdelijke runtime zonder netwerktoegang, persistent volume, secrets, Kubernetes token, runtime package-installatie of schrijfbare root filesystem. CPU, geheugen, looptijd, stdout/stderr en tijdelijke opslag zijn begrensd. De controller heeft alleen namespaced RBAC dat nodig is om deze tijdelijke pods te beheren; runtimepods gebruiken Restricted Pod Security en default-deny netwerkbeleid.

8. Secure development en CI

- Pull/push-CI lint, typecheckt en test relevante backend/frontend/microservices.
- Database-migraties en schema compatibility worden geverifieerd vóór imagepromotie.
- Gitleaks scant volledige relevante Git-historie op secrets.
- pip-audit en npm audit controleren dependencykwetsbaarheden.
- Trivy scant repository en productieimages op HIGH/CRITICAL kwetsbaarheden en faalt de build bij toepasselijke findings.
- CycloneDX-SBOM's worden voor backend/frontend-images gegenereerd en 365 dagen als CI-artifact bewaard.
- OSV Scanner vormt een tweede CVE-gate op de SBOM's.
- Container/images worden waar in manifests zichtbaar via digests gepind.

9. Logging en audit

- Security- en beheeracties worden gelogd; prompt/responsecontent wordt niet als gewone observabilitypayload gelogd.
- Auditrecords zijn tenantgebonden en gevoelige details kunnen versleuteld zijn.
- De applicatie ondersteunt een auditketen; externe digest-signing staat op uitgiftedatum uit. Daarom wordt geen extern cryptografisch onveranderlijk auditbewijs geclaimd.
- Ruwe cookieless websiteanalytics bewaren geen IP en geen identifier die langer dan de dag voortleeft volgens de huidige implementatie; ruwe events maximaal 90 dagen.

10. Malware-, vulnerability- en patchmanagement

Nieuwe HIGH/CRITICAL dependency-/imagekwetsbaarheden blokkeren de CI waar de workflow ze als fixable/relevant detecteert. Productiepatches worden op ernst, exploitability, exposure en beschikbaarheid van fix beoordeeld. Kritieke actief misbruikte kwetsbaarheden krijgen voorrang boven gewone releaseplanning. Zie document 14.

11. Incidentrespons

Securitymeldingen: security@summalabs.ai. Incidenten worden geregistreerd, geclassificeerd, ingedamd, onderzocht en afgesloten met root cause en corrective actions. Processorincidenten krijgen een interne klantmeldingsdoelstelling van 24 uur na bevestiging; wettelijke termijnen blijven leidend. Zie document 15.

12. Beschikbaarheid, backup en herstel

Er is op 28 augustus 2026 geen operationele off-cluster backup in de live deployment. Daardoor claimt Summa geen productie-RPO/RTO en mag de omgeving niet de enige opslag zijn van informatie die niet verloren mag gaan.

Na productieactivering moeten backups versleuteld, logisch gescheiden en herstelbaar zijn; een echte restore drill is de acceptatievoorwaarde. Zie document 15.

13. Verwijdering

Account-/tenantverwijdering gebruikt een durable erasure-receipt met retries voor componenten zoals PostgreSQL, Redis, identity en observability. Bestanden worden via deletion queues uit objectstorage verwijderd. Retentiepurges zijn tenantaware en tijdelijke chats hebben een aparte max-24h purge.

14. Security-openpunten vóór gemeentelijke productie

- operationele off-cluster backup + restorebewijs;
- MFA voor het afgesproken gemeentelijke identityprofiel;
- onafhankelijke penetratietest met tenantisolatiescope en gesloten kritieke/high findings;
- jaarlijkse onafhankelijke assurance volgens GIBIT artikel 38 of geaccepteerde equivalent;
- extern bewijs van beroeps-/bedrijfsaansprakelijkheidsverzekering;
- volledige runtime-SBOM voor alle productiecomponenten, niet alleen backend/frontend;
- formele verificatie van provider-DPA's en doorgifteposities, inclusief Leafcloud als infrastructuur- en inferenceprovider.