RegAlign®

CSA CAIQ v4 — Level 1 Self-Assessment

Entity: RegAlign Limited (Jersey company No. 165263), 9 Bond Street, St. Helier, JE2 3NP. Scope: RegAlign SaaS — multi-tenant pilot-stage GRC platform for JFSC-regulated firms. EU region only. Framework: CSA Cloud Controls Matrix v4 (197 controls across 17 domains). Assessment type: Self-assessment (CAIQ Level 1 — STAR Registry submission pending). Assessment date: 2026-07-04 Reviewer: Sabrina Stewart, Founder & DPO-equivalent. Next review: 2027-06-21 (or sooner on any change to RLS, encryption, audit-trail, sub-processors, retention, or auth controls).

How to read this document

Each row is one CSA CCM v4 control. The Answer column is one of:

- Yes — RegAlign currently meets the control.
- Partial — RegAlign meets part of the control; the gap is named.
- No — Control is in scope but not yet implemented; the plan is named.
- N/A — Control does not apply to RegAlign's deployment (managed-platform offload, no physical infra, no employee fleet, no mobile app, no IoT, no host OS we manage). The reason is named.

Honesty principle: no claim of an external certification we do not hold. Pen-test, SOC 2 and STAR Level 2 are on the roadmap; they are recorded as No here until the artefact exists.

Submission status. This self-assessment is the source of truth for the CAIQ v4 spreadsheet submitted to the CSA STAR Registry. Once listed, the registry entry URL will be added to the Trust Pack and `/trust/caiq`.

Cross-references. Every note points back to a public artefact: a section of the Trust Pack (`32_Trust_Pack.md`) or one of the other canonical documents in `docs/canonical/`.

Summary tally

Status	Count	% of 197
Yes	154	78%
Partial	11	6%
No	6	3%
N/A	26	13%

AA — Audit & Assurance

Control	Title	Answer	Notes
AA-01	Audit and Assurance Policy and Procedures	Yes	Audit policy documented in `docs/canonical/30_Chain_Verifier_Auditor_Runbook.md` and `31_Pilot_Ready_Attestation.md`. Single-founder operation; written policy maintained in `docs/canonical/` and reviewed at every release. No formal annual sign-off cycle yet — planned post first paying pilot.
AA-02	Independent Assessments	No	No third-party SOC 2 / ISO 27001 / STAR Level 2 yet. Pen-test SoW drafted (`19_Pen_Test_RFP.md`); execution planned post first paying pilot.
AA-03	Risk Based Planning Assessment	Yes	Risk register maintained internally; SWOT v2 published (`01_SWOT_v2.md`). Re-reviewed every release.
AA-04	Requirements Compliance	Yes	Compliance scope mapped in `25_Pilot_Prospectus.md` and `32_Trust_Pack.md` (JFSC AML/CFT/CPF, DPJL 2018, UK GDPR-aligned).
AA-05	Audit Management Process	Partial	Internal audit only (founder-led, evidenced via hash-chained audit trail). External audit programme not yet established.
AA-06	Remediation	Yes	Issues tracked in product `issues` table with status workflow, escalation, and audit-trailed remediation. See Trust Pack §6.

AIS — Application & Interface Security

Control	Title	Answer	Notes
AIS-01	Application and Interface Security Policy and Procedures	Yes	SDLC + interface security policy embedded in commit / review workflow; see `docs/canonical/architecture-overview.md`.
AIS-02	Application Security Baseline Requirements	Yes	Baseline: TypeScript strict, RLS-by-default, no service-role on user paths, signed webhooks, CSP. Enforced in code review.

Control	Title	Answer	Notes
AIS-03	Application Security Metrics	Partial	Dependency-scan + lint metrics in CI; no formal monthly metrics report yet.
AIS-04	Secure Application Design and Development	Yes	Threat modelling at architecture-change time; secure-by-default patterns documented in `architecture-overview.md`.
AIS-05	Automated Application Security Testing	Partial	Dependency-scan automated in CI; SAST coverage limited. DAST / pen-test deferred to `19_Pen_Test_RFP.md` engagement.
AIS-06	Automated Secure Application Deployment	Yes	Lovable-managed CI/CD; every deploy is git-tracked and reproducible; rollback by re-deploy of prior commit.
AIS-07	Application Vulnerability Remediation	Yes	Public Vulnerability Disclosure Policy at `regalign.app/vdp` (see `28_Vulnerability_Disclosure_Policy.md`); SLAs documented.

BCR — Business Continuity Management & Operational Resilience

Control	Title	Answer	Notes
BCR-01	Business Continuity Management Policy and Procedures	Yes	BCP outline at `07_BCP_Outline.md`. Reviewed at every major release.
BCR-02	Risk Assessment and Impact Analysis	Yes	BIA documented in BCP outline; RTO 8h / RPO 24h for tenant data (mirrors Trust Pack §8).
BCR-03	Business Continuity Strategy	Yes	Strategy: rely on managed-platform multi-AZ + daily DB snapshots; founder-led incident response. See `07_BCP_Outline.md`.
BCR-04	Business Continuity Planning	Yes	Plan documented; named successor scoped in `16_Successor_Role_Spec.md`.
BCR-05	Documentation	Yes	All BCP/DR docs in `docs/canonical/`; published Trust Pack §7.
BCR-06	Business Continuity Exercises	No	No live BCP exercise executed yet. Tabletop scheduled for Q3 2026 once first pilot live.

Control	Title	Answer	Notes
BCR-07	Communication	Yes	Status page at `regalign.app/status`; incident communication via direct email to tenant admins.
BCR-08	Backup	Yes	Lovable Cloud (Supabase EU) daily automated backups; point-in-time recovery enabled. See Trust Pack §2.
BCR-09	Disaster Response Plan	Yes	DR plan documented in `07_BCP_Outline.md`; relies on managed-platform multi-AZ failover.
BCR-10	Response Plan Exercise	No	Not yet exercised; planned alongside BCR-06.
BCR-11	Equipment Redundancy	N/A	Managed platform (Cloudflare + Supabase EU) provides infrastructure redundancy. RegAlign owns no physical equipment.

CCC — Change Control & Configuration Management

Control	Title	Answer	Notes
CCC-01	Change Management Policy and Procedures	Yes	Every change is a git commit with reviewer + deploy audit trail. Lovable-managed deploys.
CCC-02	Quality Testing	Yes	Type-check + lint + Vitest required on every change; visual QA before publish.
CCC-03	Change Management Technology	Yes	Git + Lovable CI/CD. Append-only audit-trail with SHA-256 hash chain; per-page verifier at `regalign.app/verify`. See Trust Pack §6.
CCC-04	Unauthorized Change Protection	Yes	Only the founder can deploy; MFA-enforced on Lovable account. Branch protection on `main`.
CCC-05	Change Agreements	Yes	Pilot Agreement (`05_Pilot_Agreement_Scaffold.md`) covers change-notification cadence.
CCC-06	Change Management Baseline	Yes	Baseline = current `main` branch + last deployed commit SHA; reproducible by checkout.

Control	Title	Answer	Notes
CCC-07	Detection of Baseline Deviation	Partial	Git tracks code drift; runtime config drift caught manually. Automated config-drift alerting deferred.
CCC-08	Exception Management	Yes	Exceptions logged as issues; require sign-off + audit-trail entry.
CCC-09	Change Restoration	Yes	Rollback by re-deploying prior commit; DB rollback via Supabase PITR. RTO < 1h.

CEK — Cryptography, Encryption & Key Management

Control	Title	Answer	Notes
CEK-01	Encryption and Key Management Policy and Procedures	Yes	TLS 1.2+ in transit, AES-256 at rest (Lovable Cloud managed). Key custody is sub-processor side — see Trust Pack §2/§3.
CEK-02	CEK Roles and Responsibilities	Yes	Founder owns key-lifecycle decisions; day-to-day key custody is delegated to sub-processors (Cloudflare, Supabase).
CEK-03	Data Encryption	Yes	TLS 1.2+ in transit, AES-256 at rest (Lovable Cloud managed). Key custody is sub-processor side — see Trust Pack §2/§3.
CEK-04	Encryption Algorithm	Yes	AES-256 at rest, TLS 1.2+ (incl. TLS 1.3) in transit. No proprietary crypto.
CEK-05	Encryption Change Management	Yes	Crypto changes flow through normal CCC change process; sub-processor crypto changes tracked via vendor advisories.
CEK-06	Encryption Change Cost Benefit Analysis	Yes	Documented when crypto is changed; default = use sub-processor managed crypto, which has independent CBA.
CEK-07	Encryption Risk Management	Yes	Crypto-risk reviewed at architecture-change time; logged in risk register.
CEK-08	CSC Key Management Capability	No	Bring-your-own-key not supported. Single-tenant CMK on roadmap (post-Series-A).

Control	Title	Answer	Notes
CEK-09	Encryption and Key Management Audit	Partial	Internal review only; relies on sub-processor SOC 2 / ISO 27001 attestations.
CEK-10	Key Generation	Yes	Keys generated by sub-processors (Cloudflare, Supabase); no founder-managed long-lived keys other than API/webhook secrets.
CEK-11	Key Purpose	Yes	Each key has a single purpose (TLS cert, DB encryption, webhook HMAC, API key signing).
CEK-12	Key Rotation	Yes	Sub-processor keys rotated per their published schedule. Tenant API keys / webhook secrets rotatable on demand via `/admin/api-keys`.
CEK-13	Key Revocation	Yes	API keys revocable instantly via operator UI; HTTP 401 returned on next call.
CEK-14	Key Destruction	Yes	Revoked keys are deleted, not just disabled; sub-processor key destruction per their procedures.
CEK-15	Key Activation	Yes	API keys active on creation; sub-processor keys per their lifecycle.
CEK-16	Key Suspension	Yes	API keys can be disabled (suspended) before deletion via operator UI.
CEK-17	Key Deactivation	Yes	Deactivation is identical to revocation for API keys; sub-processor lifecycle per their controls.
CEK-18	Key Archival	N/A	RegAlign-issued keys are not archived (no need: re-issue is one click). Sub-processor practice per their controls.
CEK-19	Key Compromise	Yes	Suspected compromise -> revoke + re-issue + audit-trail entry + tenant-admin notification.
CEK-20	Key Recovery	N/A	Tenant API keys cannot be recovered after revocation; sub-processor key recovery per their controls.

Control	Title	Answer	Notes
CEK-21	Key Inventory Management	Yes	Active keys listed at `/admin/api-keys` per tenant; webhook secrets at `/admin/regulator-endpoints`.

DCS — Datacenter Security

Control	Title	Answer	Notes
DCS-01	Off-Site Equipment Disposal Policy and Procedures	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-02	Off-Site Transfer Authorization Policy and Procedures	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-03	Secure Area Policy and Procedures	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-04	Secure Media Transportation Policy and Procedures	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-05	Assets Classification	Yes	Logical asset classification (data classification at table level, sensitivity tagged via `data_classification` column). Physical-asset classification N/A.

Control	Title	Answer	Notes
DCS-06	Assets Cataloguing and Tracking	Yes	Logical asset inventory in `data-model-map.md` and `architecture-overview.md`. Physical assets N/A.
DCS-07	Controlled Access Points	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-08	Equipment Identification	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-09	Secure Area Authorization	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-10	Surveillance System	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-11	Unauthorized Access Response Training	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

Control	Title	Answer	Notes
DCS-12	Cabling Security	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-13	Environmental Systems	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-14	Secure Utilities	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.
DCS-15	Equipment Location	N/A	N/A — RegAlign operates no physical data-centre, network cabling, surveillance or utility infrastructure. Hosting is managed by Cloudflare Workers and Lovable Cloud (Supabase EU); their published certifications apply to this domain.

DSP — Data Security & Privacy Lifecycle Management

Control	Title	Answer	Notes
DSP-01	Security and Privacy Policy and Procedures	Yes	Published privacy notice + DPIA template (`06_DPIA_Template.md`); JOIC-registered controller/processor (No. 103914).
DSP-02	Secure Disposal	Yes	Tenant deletion = hard delete + audit-trail entry. Backups expire per `15_Data_Retention_and_Deletion.md`.

Control	Title	Answer	Notes
DSP-03	Data Inventory	Yes	Full data inventory in `data-model-map.md`; per-table sensitivity tagging.
DSP-04	Data Classification	Yes	`data_classification` column on tenant rows; `live_PROHIBITED` on pilot/sandbox tenants until uplift.
DSP-05	Data Flow Documentation	Yes	Data flow diagram + sub-processor map in `architecture-overview.md` and `14_Sub_Processor_List.md`.
DSP-06	Data Ownership and Stewardship	Yes	Tenant = data owner; RegAlign = processor for tenant data, controller for account data. Documented in Pilot Agreement §3.
DSP-07	Data Protection by Design and Default	Yes	RLS-by-default on every table; tenant isolation enforced at query layer.
DSP-08	Data Privacy by Design and Default	Yes	Minimum-necessary data collection; no special-category data accepted (enforced via upload guards).
DSP-09	Data Protection Impact Assessment	Yes	DPIA template provided to every tenant (`06_DPIA_Template.md`); founder DPIA performed at architecture-change time.
DSP-10	Sensitive Data Transfer	Yes	All transfers TLS 1.2+; EU-only sub-processors for data path.
DSP-11	Personal Data Access, Reversal, Rectification and Deletion	Yes	Operator UI supports DSAR / rectification / erasure via the public REST API (`public-api-contract.md`) and tenant Settings -> Data (`/settings/data`).
DSP-12	Limitation of Purpose in Personal Data Processing	Yes	Documented in Pilot Agreement §3; tenant data not used for product improvement without explicit consent.
DSP-13	Personal Data Sub-processing	Yes	Public sub-processor list at `regalign.app/trust` and in `14_Sub_Processor_List.md`; changes notified 30 days in advance per Pilot Agreement §7.

Control	Title	Answer	Notes
DSP-14	Disclosure of Data Sub-processors	Yes	Public sub-processor list at `regalign.app/trust` and in `14_Sub_Processor_List.md`; changes notified 30 days in advance per Pilot Agreement §7.
DSP-15	Limitation of Production Data Use	Yes	Production data never used in dev/test; pilot/sandbox tenants flagged with `live_PROHIBITED` and enforce upload guards.
DSP-16	Data Retention and Deletion	Yes	Published policy at `15_Data_Retention_and_Deletion.md`; tenant-level retention overrideable per Pilot Agreement.
DSP-17	Sensitive Data Protection	Yes	No special-category data accepted; enforced by upload guards + onboarding checklist.
DSP-18	Disclosure Notification	Yes	Breach-notification SLA: 24h to tenant + JOIC per DPJL 2018; documented in BCP outline and Pilot Agreement §8.
DSP-19	Data Location	Yes	All tenant data resides in EU (Lovable Cloud EU region). Cloudflare edge does not persist tenant data.

GRC — Governance, Risk & Compliance

Control	Title	Answer	Notes
GRC-01	Governance Program Policy and Procedures	Yes	Governance documented in `docs/canonical/` (Trust Pack, Sub-processor list, BCP, DPIA, Retention, VDP, AI-use disclosure).
GRC-02	Risk Management Program	Yes	Internal risk register + SWOT (`01_SWOT_v2.md`); reviewed every release.
GRC-03	Organizational Policy Reviews	Yes	Canonical docs reviewed at every release; review log in `.lovable/handover/`.
GRC-04	Policy Exception Process	Yes	Exceptions logged in `issues` with sign-off + audit-trail; documented in Pilot Agreement §6.
GRC-05	Information Security Program	Yes	Trust Pack (`32_Trust_Pack.md`) is the published programme summary.

Control	Title	Answer	Notes
GRC-06	Governance Responsibility Model	Yes	Founder is accountable owner; successor role scoped in `16_Successor_Role_Spec.md`.
GRC-07	Information System Regulatory Mapping	Yes	Regulatory mapping per `25_Pilot_Prospectus.md` (JFSC AML/CFT/CPF, DPJL 2018) and the in-product Compass methodology.
GRC-08	Special Interest Groups	Yes	Founder participates in CSA / FCA / JFSC discussion channels; subscribes to ENISA + NCSC advisories.

HRS — Human Resources Security

Control	Title	Answer	Notes
HRS-01	Background Screening Policy and Procedures	N/A	N/A — single founder; no employees. Will adopt policy at first hire.
HRS-02	Acceptable Use of Technology Policy and Procedures	Yes	Acceptable-use embedded in founder operating procedure; will formalise at first hire.
HRS-03	Clean Desk Policy and Procedures	Yes	Founder operates browser-only; no printed customer data; locked workspace when away.
HRS-04	Remote and Home Working Policy and Procedures	Yes	Single home-office; disk-encrypted laptop; MFA on every privileged account.
HRS-05	Asset returns	N/A	N/A — no employees / no issued assets.
HRS-06	Employment Termination	N/A	N/A — no employees yet.
HRS-07	Employment Agreement Process	N/A	N/A — no employees yet.
HRS-08	Employment Agreement Content	N/A	N/A — no employees yet. Sub-processor contracts cover equivalent obligations.
HRS-09	Personnel Roles and Responsibilities	Yes	Founder role + successor role spec in `16_Successor_Role_Spec.md`. Second-operator brief in `17_Second_Operator_Brief.md`.
HRS-10	Non-Disclosure Agreements	Yes	Mutual NDA template available; signed with every pilot prospect before sharing diligence pack.

Control	Title	Answer	Notes
HRS-11	Security Awareness Training	Yes	Founder maintains CPD; will formalise programme at first hire.
HRS-12	Personal and Sensitive Data Awareness and Training	Yes	Founder DPO-equivalent; maintains data-protection CPD.
HRS-13	Compliance User Responsibility	Yes	Tenant user responsibilities documented in Pilot Agreement §4 and the in-product onboarding checklist.

IAM — Identity & Access Management

Control	Title	Answer	Notes
IAM-01	Identity and Access Management Policy and Procedures	Yes	Row-level security on every tenant table; least-privilege role model (admin / cco / mlro / board / user). See Trust Pack §4.
IAM-02	Strong Password Policy and Procedures	Yes	Supabase Auth password policy: min 12 chars, breach-list check via HIBP, no max length.
IAM-03	Identity Inventory	Yes	All identities in `auth.users` + `public.tenant_users`; operator review at `/settings/users`.
IAM-04	Separation of Duties	Yes	Maker-checker workflow on regulatory adoption; admin / cco / mlro / board roles separated. Row-level security on every tenant table; least-privilege role model (admin / cco / mlro / board / user). See Trust Pack §4.
IAM-05	Least Privilege	Yes	Row-level security on every tenant table; least-privilege role model (admin / cco / mlro / board / user). See Trust Pack §4.
IAM-06	User Access Provisioning	Yes	Tenant-admin invites + named roles; audit-trailed.
IAM-07	User Access Changes and Revocation	Yes	Role changes + offboarding via `/settings/users`; immediate effect; audit-trailed.
IAM-08	User Access Review	Yes	Quarterly access review prompt on `/settings/users`; results captured in audit trail.

Control	Title	Answer	Notes
IAM-09	Segregation of Privileged Access Roles	Yes	`sandbox_admin` (founder cross-tenant) is separate from per-tenant `admin`.
IAM-10	Management of Privileged Access Roles	Yes	Privileged roles grant logged in `user_roles` + audit-trailed; manual approval required.
IAM-11	CSCs Approval for Agreed Privileged Access Roles	Yes	Founder cross-tenant access is documented in Pilot Agreement §5; tenant can revoke at any time.
IAM-12	Safeguard Logs Integrity	Yes	Append-only audit-trail with SHA-256 hash chain; per-page verifier at `regalign.app/verify`. See Trust Pack §6.
IAM-13	Uniquely Identifiable Users	Yes	Every action stamped with `auth.uid()` + tenant; no shared accounts.
IAM-14	Strong Authentication	Yes	MFA (TOTP) enforced for all elevated roles (admin, cco, mlro) on production hosts via `requireMfaForElevatedRoles` middleware; enrolment nudged in `/today` and hard-required in `/settings/security`. Founder accounts MFA-enforced manually. See handover 243.
IAM-15	Passwords Management	Yes	Supabase Auth; bcrypt-hashed; reset via verified email; no plaintext storage.
IAM-16	Authorization Mechanisms	Yes	RLS + has_role() security-definer functions; documented in `architecture-overview.md`.

IPY — Interoperability & Portability

Control	Title	Answer	Notes
IPY-01	Interoperability and Portability Policy and Procedures	Yes	Documented data-export commitment in Pilot Agreement §9.
IPY-02	Application Interface Availability	Yes	Public REST API v1 at `/api/public/v1/*`; contract PDF in `public/downloads/canonical/public-api-contract.pdf`.
IPY-03	Secure Interoperability and Portability Management	Yes	API authenticated with bearer tokens; webhooks signed HMAC-SHA256.

Control	Title	Answer	Notes
IPY-04	Data Portability Contractual Obligations	Yes	Pilot Agreement §9 commits to CSV/JSON export of all tenant data on request, format documented in `public-api-contract.md`.

IVS — Infrastructure & Virtualization Security

Control	Title	Answer	Notes
IVS-01	Infrastructure and Virtualization Security Policy and Procedures	Yes	Infrastructure offloaded to Cloudflare Workers + Lovable Cloud (Supabase EU). RegAlign-side policy in `architecture-overview.md`.
IVS-02	Capacity and Resource Planning	Yes	Managed-platform auto-scale (Cloudflare Workers, Supabase). Capacity review at every architecture change.
IVS-03	Network Security	Yes	Cloudflare WAF + DDoS protection; TLS-only ingress; egress to known sub-processors only.
IVS-04	OS Hardening and Base Controls	N/A	N/A — no host OS managed by RegAlign. Workers + managed Postgres.
IVS-05	Production and Non-Production Environments	Yes	Separate Lovable preview + published environments; pilot/sandbox tenants flagged `live_PROHIBITED`.
IVS-06	Segmentation and Segregation	Yes	Multi-tenant logical segregation via RLS; no shared schema for tenant data without `tenant_id` scoping.
IVS-07	Migration to Cloud Environments	N/A	N/A — cloud-native since inception; no on-prem migration.
IVS-08	Network Architecture Documentation	Yes	Documented in `architecture-overview.md` and `data-model-map.md`.
IVS-09	Network Defense	Yes	Cloudflare WAF + bot mitigation; Sentry alerting on server errors; rate-limiting on `/api/public/*`.

LOG — Logging & Monitoring

Control	Title	Answer	Notes
LOG-01	Logging and Monitoring Policy and Procedures	Yes	Logging policy: every state-changing action audit-trailed; security events to Sentry. Append-only audit-trail with SHA-256 hash chain; per-page verifier at `regalign.app/verify`. See Trust Pack §6.
LOG-02	Audit Logs Protection	Yes	Append-only + SHA-256 hash chain (sealed). Tampering detectable at `/verify`.
LOG-03	Security Monitoring and Alerting	Yes	Sentry (browser + server); founder receives alert on errors and suspicious patterns.
LOG-04	Audit Logs Access and Accountability	Yes	Audit-trail read scoped by RLS to tenant admins + sandbox_admin; every read is itself audit-trailed for privileged roles.
LOG-05	Audit Logs Monitoring and Response	Yes	Founder reviews critical audit events daily; alerts via Sentry.
LOG-06	Clock Synchronization	Yes	All timestamps from managed-platform NTP (Cloudflare, Supabase). UTC stored, UI localises.
LOG-07	Logging Scope	Yes	Audit scope: auth events, role changes, data CRUD, exports, adoptions, escalations, attestation pack composition, key issuance/revocation.
LOG-08	Log Records	Yes	Per-event record: actor (`auth.uid()`), tenant, entity, action, timestamp, prior-hash, current-hash.
LOG-09	Log Protection	Yes	Append-only audit-trail with SHA-256 hash chain; per-page verifier at `regalign.app/verify`. See Trust Pack §6.
LOG-10	Encryption Monitoring and Reporting	Partial	TLS health monitored by Cloudflare; at-rest encryption status reported by Supabase. No internal crypto-monitoring dashboard yet.

Control	Title	Answer	Notes
LOG-11	Transaction/Activity Logging	Yes	Append-only audit-trail with SHA-256 hash chain; per-page verifier at `regalign.app/verify`. See Trust Pack §6.
LOG-12	Access Control Logs	Yes	Role grants/revocations + auth events captured in audit trail + Supabase Auth logs.
LOG-13	Failures and Anomalies Reporting	Yes	Sentry captures errors; weekly review by founder; high-severity alerts immediate.

SEF — Security Incident Management, E-Discovery & Cloud Forensics

Control	Title	Answer	Notes
SEF-01	Security Incident Management Policy and Procedures	Yes	Documented in BCP outline; 24h tenant notification SLA per Pilot Agreement §8.
SEF-02	Service Management Policy and Procedures	Yes	Status page + incident comms via direct tenant-admin email.
SEF-03	Incident Response Plans	Yes	IR plan in `07_BCP_Outline.md`; founder = on-call; successor role spec in `16_Successor_Role_Spec.md`.
SEF-04	Incident Response Testing	No	Not yet tested live. Tabletop exercise scheduled Q3 2026.
SEF-05	Incident Response Metrics	Partial	Sentry MTTA/MTTR available; formal monthly metric report deferred.
SEF-06	Event Triage Processes	Yes	Sentry severity -> founder triage within 1 business hour during working hours.
SEF-07	Security Breach Notification	Yes	DPJL 2018 / UK GDPR-aligned: 72h to JOIC, 24h to tenants. Documented in Pilot Agreement §8.
SEF-08	Points of Contact Maintenance	Yes	Security contact published at `regalign.app/vdp` and `regalign.app/trust`; tenant emergency contact captured at onboarding.

STA — Supply Chain Management, Transparency & Accountability

Control	Title	Answer	Notes
STA-01	SSRM Policy and Procedures	Yes	Shared-responsibility model documented in Trust Pack §3 and `architecture-overview.md`.
STA-02	SSRM Supply Chain	Yes	Public sub-processor list at `regalign.app/trust` and in `14_Sub_Processor_List.md`; changes notified 30 days in advance per Pilot Agreement §7.
STA-03	SSRM Guidance	Yes	Pilot Agreement §3 + Trust Pack §3 spell out what RegAlign vs the tenant is responsible for.
STA-04	SSRM Control Ownership	Yes	RACI documented in Trust Pack §3.
STA-05	SSRM Documentation Review	Yes	Reviewed at every release + every sub-processor change.
STA-06	SSRM Control Implementation	Yes	Controls implemented per Trust Pack §4–§7; evidence in `docs/canonical/`.
STA-07	Supply Chain Inventory	Yes	Public sub-processor list at `regalign.app/trust` and in `14_Sub_Processor_List.md`; changes notified 30 days in advance per Pilot Agreement §7.
STA-08	Supply Chain Risk Management	Yes	Sub-processor risk reviewed before onboarding; certifications + region + SLAs captured in `14_Sub_Processor_List.md`.
STA-09	Primary Service and Contractual Agreement	Yes	Pilot Agreement scaffold at `05_Pilot_Agreement_Scaffold.md`.
STA-10	Supply Chain Agreement Review	Yes	Sub-processor contracts reviewed at renewal; security addenda in place where required.
STA-11	Internal Compliance Testing	Partial	Internal self-assessment (this document). External testing per AA-02.
STA-12	Supply Chain Service Agreement Compliance	Yes	Sub-processor SLAs monitored via status pages + Sentry.
STA-13	Supply Chain Governance Review	Yes	Sub-processor list reviewed quarterly; changes notified 30 days in advance per Pilot Agreement §7.

Control	Title	Answer	Notes
STA-14	Supply Chain Data Security Assessment	Yes	Sub-processor security posture captured in `14_Sub_Processor_List.md`; only EU-region processors on data path.

TVM — Threat & Vulnerability Management

Control	Title	Answer	Notes
TVM-01	Threat and Vulnerability Management Policy and Procedures	Yes	Public VDP at `regalign.app/vdp`; remediation SLAs documented in `28_Vulnerability_Disclosure_Policy.md`.
TVM-02	Malware Protection Policy and Procedures	N/A	N/A — no host OS managed by RegAlign; no user-uploaded executables; sub-processor anti-malware applies.
TVM-03	Vulnerability Remediation Schedule	Yes	Critical: 7 days; High: 30 days; Medium: 90 days; Low: best-effort. Per `28_Vulnerability_Disclosure_Policy.md`.
TVM-04	Detection Updates	Yes	Dependency-vulnerability scan in CI; managed-platform patching by sub-processors.
TVM-05	External Library Vulnerabilities	Yes	Dependency-scan on every build (npm audit + Lovable dependency scanner).
TVM-06	Penetration Testing	No	Not yet performed. RFP drafted at `19_Pen_Test_RFP.md`; engagement scheduled post first paying pilot.
TVM-07	Vulnerability Identification	Yes	Dependency scan in CI + VDP submissions + Sentry error patterns.
TVM-08	Vulnerability Prioritization	Yes	CVSS-aligned; remediation slotted per TVM-03 schedule.
TVM-09	Vulnerability Management Reporting	Partial	Internal reporting only; formal report cadence deferred until first paying pilot.
TVM-10	Vulnerability Management Metrics	Partial	MTTR captured per VDP submission; broader metric reporting deferred.

UEM — Universal Endpoint Management

Control	Title	Answer	Notes
UEM-01	Endpoint Devices Policy and Procedures	Yes	Founder laptop only — disk encryption (FileVault), screen lock, OS auto-update, MFA on every privileged login. Limited applicability — RegAlign has no employee fleet. Founder laptop only, with disk encryption + browser-only operator access. No MDM at this scale.
UEM-02	Application and Service Approval	Yes	Founder approves all software/services in use; documented in operating procedure.
UEM-03	Compatibility	Yes	Browser-only operator surface; supported in modern Chromium/Firefox/Safari.
UEM-04	Endpoint Inventory	Yes	Single founder endpoint inventoried. Tenant endpoints out-of-scope (tenant-managed).
UEM-05	Endpoint Management	Yes	Manual management on single founder endpoint. Limited applicability — RegAlign has no employee fleet. Founder laptop only, with disk encryption + browser-only operator access. No MDM at this scale.
UEM-06	Automatic Lock Screen	Yes	Founder laptop auto-locks after 5 min inactivity.
UEM-07	Operating Systems	Yes	macOS current major release; auto-update enabled.
UEM-08	Storage Encryption	Yes	FileVault enabled on founder laptop.
UEM-09	Anti-Malware Detection and Prevention	Yes	macOS Gatekeeper + XProtect + System Integrity Protection.
UEM-10	Software Firewall	Yes	macOS application firewall enabled.
UEM-11	Data Loss Prevention	Partial	Operator surface is browser-only; no bulk export from founder endpoint. Formal DLP tooling N/A at single-founder scale.

Control	Title	Answer	Notes
UEM-12	Remote Locate	N/A	N/A — single founder endpoint; Find My Mac enabled for personal device recovery.
UEM-13	Remote Wipe	Yes	Find My Mac remote wipe enabled on founder laptop.
UEM-14	Third-Party Endpoint Security Posture	N/A	N/A — no third-party endpoints provisioned by RegAlign.

Maintenance contract

This file is the canonical source. Update it the same turn any of these change:

- Row-level security model or `has_role()` definition.
- At-rest or in-transit encryption posture.
- Audit-trail / hash-chain mechanics.
- Sub-processor list (mirrors `14_Sub_Processor_List.md`).
- Data retention or deletion policy (mirrors `15_Data_Retention_and_Deletion.md`).
- Authentication controls (MFA scope, password policy).

Then rebuild the PDF with `python3 scripts/build-canonical-pdfs.py` and visually QA every page.