



AdaptivMapr Security one-pager

Single-page summary of the controls AdaptivMapr operates. Full posture at adaptivmapr.com/legal/security.

PLATFORM & DATA RESIDENCY

Hosting	Cloudflare Workers (EU PoPs preferred) for compute + edge; Supabase Postgres for the account database.
Data residency	Supabase EU (Ireland) with PITR; Cloudflare edge region preference is configurable. Full-data PHI calls route through phi-cloud with in-region routing.
Storage	Cloudflare KV (rate-limit + stats), R2 (assets). Stateless mapping engine — uploads in-process with hard 24-hour TTL.

ENCRYPTION

In transit	TLS 1.3, AEAD-only ciphers; TLS 1.0/1.1 disabled at the edge; HSTS with preload.
At rest	AES-256 (GCM) for persisted state — account database, audit logs, encrypted BYO-LLM credentials.
Key management	Envelope encryption with KMS-managed root keys; BYO-LLM creds encrypted per-workspace with a unique DEK wrapped by the KMS root.

AUTHENTICATION & ACCESS

API keys	HMAC-signed self-contained keys (signed with MAPR_KEY_SECRET). Revocation via server-side deny-list checked every request.
Dashboard auth	Magic-link sign-in + JWT sessions. RBAC: Owner / Admin / Developer / Viewer, workspace-scoped and audit-logged.
MFA & SSO	TOTP MFA on all plans (enforced for Owner/Admin on Pro+Enterprise). SAML 2.0 + OIDC SSO and SCIM on Enterprise.
IP restrictions	Pro and Enterprise can bind API keys to CIDR allow-lists enforced at the edge.

AUDIT & MONITORING

Audit log	Append-only audit via Chainlog — authn, authz, config changes, mapping commits. Retention: 7 years.
Observability	Cloudflare Workers logs + structured request tracing. Status at status.adaptivmapr.com .

COMPLIANCE POSTURE

SOC 2 Type II	Observation window in progress; first attestation report expected before end of the current fiscal year.
GDPR / nFADP	GDPR-aligned with SCCs incorporated in DPA (adaptivmapr.com/legal/dpa). Swiss nFADP treated as equivalent.
HIPAA	HIPAA-eligible via phi-cloud BAA — customers route full-data calls through phi-cloud; the BAA covers AdaptivMapr as a downstream agent.
CCPA / CPRA	AdaptivMapr does not sell or share personal data within the meaning of California law.

INCIDENT RESPONSE

RTO / RPO	RTO 4h for the public API and dashboard. RPO 1h for the account database; near-zero for stateless API requests (idempotent retries supported).
Breach notification	Customers notified within 72 hours of any confirmed Personal Data Breach, per DPA Article 11.
Contact	security@adaptivmapr.com for security disclosures and incident contact. dpo@adaptivmapr.com for data protection requests.