Marqib — Answers to a standard security questionnaire

Version 1.0 · September 2026. The answers follow the usual headings of SIG-Lite / CAIQ-style vendor questionnaires. "Firm-hosted" means installed in the customer's own environment. "Hosted" means a dedicated pilot instance or the public sandbox run by Marqib.

Company and governance

Question	Answer
Legal entity	Nordera Works Teknoloji ve Danışmanlık A.Ş., Istanbul, Türkiye (company registration in progress)
Security contact	hello@marqib.com, subject "Security"; marqib.com/.well-known/security.txt
Certifications (ISO 27001, SOC 2)	None yet. Firm-hosted deployment keeps customer data inside the customer's certified environment. We will share our roadmap on request.
Written security policies	Secure development, access and incident handling practices are described in this pack. Formal policy set: in preparation.
Background checks / confidentiality	All staff and contractors with access sign confidentiality undertakings.

Data location and handling

Question	Answer
Where is customer data stored?	Firm-hosted: in the customer's account and region, and never with Marqib. Hosted pilot: a dedicated database in the customer's chosen region.
Does the vendor access production data?	Firm-hosted: no, except in a support session the customer grants and supervises. Hosted pilot: only named Marqib staff, for support, logged.
Data minimisation	Only the fields in the Architecture document. No identity documents or images.
Encryption in transit / at rest	TLS 1.2+. At rest: provider encryption (AES-256) for hosted databases; in firm-hosted installations, the customer's storage encryption applies.
Retention and deletion	Firm-hosted: the customer controls retention. Hosted pilot: deleted at pilot end, with written confirmation, unless a licence follows. Sandbox: deleted after 7 days.
Data used for training	Never.
Sub-processors	See the sub-processor list; none in firm-hosted installations.

Access control

Question	Answer
Authentication	Named user id and password. Sessions are HMAC-signed cookies (HttpOnly, SameSite) and expire after 12 h.
MFA / SSO	Planned (SAML/OIDC). In firm-hosted installations, we recommend placing the application behind the firm's identity-aware proxy or VPN, which provides MFA today.
Role separation	Analyst and MLRO roles; maker-checker enforced on the server. Nobody approves their own proposal.
Brute-force protection	Sign-in attempts are rate-limited per user and per IP.
Leaver process	Removing a user from the configuration invalidates their session immediately.

Application security

Question	Answer
Secure SDLC	Code review before every release; typed code (TypeScript); parameterised SQL only (no string-built queries from user input); dependency updates tracked.
OWASP controls	CSRF: Origin checks on state-changing requests. XSS: framework output encoding. SQL injection: parameterised queries. Open redirects: local-only paths. Rate limits on public endpoints.
Penetration test	Not yet performed by a third party. We welcome the customer's own test on a pilot instance.
Vulnerability disclosure	security.txt; acknowledgement within 2 business days.
Audit logging	Append-only, hash-chained log of every action, written in the same transaction as the change. Re-verified on view.

Operations

Question	Answer
Backups	Hosted: provider point-in-time recovery. Firm-hosted: the customer's backup policy.
Availability	End-of-day batch product; no real-time dependency in the firm's trading path.
Incident notification	We notify affected customers without undue delay and within 72 hours of becoming aware of a personal-data breach, with the facts known and the steps taken.
Business continuity	Firm-hosted installations keep running without Marqib. Source code escrow can be discussed for a production licence.

AI / model use

See the Model governance note:

- deterministic detection;
- optional drafting only;
- tokenisation before any call;
- sentence-level evidence citations;
- a model endpoint the firm chooses;
- no training on client data.