MAEVE HQ · SECURITY OVERVIEW

How MAEVE Protects The Most Personal Data In Your Professional Life.

Version 1.0 · Private Beta · Last updated 2026

MAEVE is a relationship intelligence layer for founders, operators and investors. This document summarises how we handle, store, isolate and protect the data you entrust to us during the private beta.

1. Data We Handle

MAEVE ingests only the sources you explicitly connect. Typical categories include calendar events, message metadata (headers, cadence, participants), contact records, and any notes you author inside MAEVE. Message contents are never read unless you opt in per-source, per-thread.

2. Encryption

In transit	TLS 1.3 across every network hop, HSTS enforced.
At rest	AES-256, keys managed via the platform KMS.
Key rotation	Data-encryption keys rotated on a defined cadence.
Tenant isolation	One relationship graph per account; no cross-tenant reads.

3. Access Controls

- Least-privilege by default: engineers do not have standing access to production data.
- Any privileged access is time-bound, ticket-linked and reviewed by a second engineer.
- Every access event is logged; logs are immutable and retained for audit.
- Multi-factor authentication is mandatory for all internal systems.

4. AI & Model Use

Your data is never used to train models that touch anyone else's account, including ours. MAEVE composes drafts and recommendations; it never sends messages on your behalf without an explicit, in-context confirmation. Every recommendation is explainable — you can inspect the signals that produced it, and correct them.

5. Retention & Deletion

You can export everything MAEVE holds about you as a portable file at any time. On deletion, we remove your relationship graph, notes and derived signals within 24 hours; backup copies are purged on our defined backup rotation.

6. Integrations & Third Parties

Nothing MAEVE ingests is ever passed to another integration without your explicit direction. For a live, per-source list of what we read and what we don't, see maevehq.com/integrations.

7. Incident Response

We maintain a written incident-response runbook, rehearsed on a recurring schedule. If a verified security incident affects your data, we will notify you within 72 hours of confirmation, with the facts we know, the mitigations we have taken, and the next steps we owe you.

8. What You Can Expect During Private Beta

- Direct access to a founding-team contact for security or trust questions.
- Any feature that changes what MAEVE reads is announced in advance, opt-in, and reversible.
- You can disconnect any source and delete your account at any time — no support ticket required.
- This document evolves. Material changes are posted at maevehq.com/security.

9. Responsible Disclosure

If you believe you have found a security issue, write to security@maevehq.com. A human will reply within one business day. We commit to good-faith engagement, no legal action against researchers acting in good faith, and public credit where you want it.