Security Document

How we keep your business data safe

Version 1.0 · 10 May 2026 · tradesmind.ai

This document describes the technical and organisational security measures TradesMind AI Ltd has in place to protect your data. Effective: 10 May 2026.

1. Our Security Commitment

TradesMind AI Ltd is committed to the security of your personal and business data. We have implemented a layered security architecture designed to protect your data against unauthorised access, disclosure, alteration, and destruction. Our security practices comply with UK GDPR Article 32, which requires appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

2. Infrastructure Security

The TradesMind AI platform runs on enterprise-grade infrastructure:

- Cloud hosting: DigitalOcean London region (UK data residency for all core data).
- Server hardening: Ubuntu 24.04 LTS, automatic security updates, minimal attack surface.
- Firewall: UFW configured to allow only ports 22 (SSH), 80 (HTTP), and 443 (HTTPS). All other inbound traffic is blocked.
- SSH access: key-based authentication only. Password SSH authentication is disabled.
- Process management: pm2 manages the brain API server with automatic restart on failure.
- SSL/TLS: all traffic is encrypted via Let's Encrypt certificates. HTTP is automatically redirected to HTTPS.
- Reverse proxy: nginx handles all public traffic and terminates SSL before forwarding to the internal API.

3. Application Security

- Authentication: Supabase Auth handles all user authentication. Passwords are never stored in plaintext — Supabase uses bcrypt hashing.
- Session management: sessions are stored as JSON Web Tokens (JWTs). JWTs are cryptographically verified and expire after a limited period.
- API authentication: all internal API calls require a secure bearer token. Tokens are stored as environment variables and never in code.
- Row-level security (RLS): all database tables have RLS enabled. Users can only ever read or write their own data.
- Token limits: AI processing is capped at 2,000 tokens per API call.
- Webhook validation: inbound webhooks from VAPI and other providers are validated using HMAC signatures before processing.
- HTTPS enforced: all platform URLs are served over HTTPS. Mixed content is blocked.
- Input sanitisation: user-supplied inputs are sanitised before processing to mitigate injection attacks.

4. Data Security

- Encryption in transit: all data in transit is encrypted using TLS 1.2 or higher.
- Encryption at rest: Supabase database storage is encrypted at rest using AES-256.
- Payment data: card numbers are handled exclusively by Stripe (PCI DSS Level 1 compliant). TradesMind never stores card data.

- Credential storage: SMTP passwords and other sensitive credentials are stored in encrypted form.
- Voice recordings: conversation transcripts are stored in the UK/EU.
- Email data: emails accessed via OAuth are processed in memory only and stored only where explicitly saved.
- Backup: regular automated backups are maintained, encrypted and stored separately from the primary database.

5. Access Controls

- Principle of least privilege: each system component accesses only the data and resources it needs.
- Staff access: access to production systems is restricted to the founder and authorised technical contractors under NDA.
- Third-party access: sub-processors are given only the minimum access necessary to deliver their specific service.
- Database access: direct database access is not exposed to any frontend page. All operations go through the brain API.
- Audit logging: API requests are logged for security monitoring and incident response.

6. GDPR & UK Data Protection Compliance

- Data Controller: TradesMind AI Ltd is registered as a Data Controller with the ICO.
- Data Processing Agreements: DPAs are in place with all sub-processors.
- Data minimisation: we collect only the data necessary for the purposes described in our Privacy Policy.
- Breach notification: we will notify the ICO within 72 hours of a confirmed personal data breach.
- Data subject rights: requests handled within 30 days. Contact: privacy@tradesmind.ai
- Data residency: core personal data is stored in UK/EU infrastructure.

7. Third-Party Security

We rely on the following sub-processors:

- Supabase — Database: SOC 2 Type II, GDPR compliant.
- DigitalOcean — Server hosting: SOC 2 Type II, ISO 27001.
- Anthropic — AI processing: Enterprise DPA, US-based (SCCs apply).
- VAPI — Voice AI telephony: Enterprise DPA.
- Stripe — Payments: PCI DSS Level 1.
- SendGrid — Email delivery: SOC 2 Type II.
- Vercel — Web hosting: SOC 2 Type II.
- Google / Microsoft — Gmail / Outlook OAuth: OAuth only, user-granted access.

8. Incident Response

In the event of a security incident, TradesMind will:

- Identify and contain the incident as quickly as possible.
- Assess the scope, cause, and impact of the incident.
- Notify the ICO within 72 hours if the incident constitutes a personal data breach.
- Notify affected users without undue delay where there is high risk to their rights.
- Document the incident and remediation steps taken.
- Review and update security measures to prevent recurrence.
- To report a security concern: security@tradesmind.ai

9. Security Roadmap

As TradesMind grows, we will implement additional measures:

- Independent penetration testing (scheduled once the platform has paying users).
- Hardware security keys for all staff with production access.
- SOC 2 / ISO 27001 audit (relevant when selling to enterprise customers).
- Bug bounty programme for responsible disclosure.
- Multi-region failover for high availability.

10. Contact

- Security reports: security@tradesmind.ai
- Data protection: privacy@tradesmind.ai
- General: support@tradesmind.ai
- Post: TradesMind AI Ltd, 67a Main Avenue, Enfield, EN1 1DS