

Unabated Products - Security Overview

For enterprise procurement / IT Security review. Version 1.0 | Last updated: 2026-06-24

Contact: security@unabatedproducts.com

Compliance & data protection

- Unabated Products does not currently hold its own SOC 2 attestation. The service runs entirely on SOC 2 Type II and ISO 27001 certified infrastructure (Supabase, Netlify, GitHub), so the underlying compute, storage, and network controls are independently audited.
- GDPR: Data Processing Agreement (DPA) available on request; standard SCCs included.
- CCPA: compliant; California data subject requests honored within 45 days.

Data we handle

- Customer-provided: name, work email, role/title, company name (optional), in-product interaction transcripts.
- We do not collect or process payment card data (handled by Stripe), health data, biometric data, or children's data.
- Residency: all customer data is stored in US-East via Supabase (AWS us-east-1). No cross-region replication without contractual amendment.

Architecture & encryption

- Application: React + TypeScript SPA delivered via Netlify global CDN.
- Backend: Supabase managed Postgres + serverless edge functions.
- In transit: TLS 1.2+ (TLS 1.3 preferred) on all endpoints; HSTS enforced.
- At rest: AES-256 on Postgres volumes (Supabase platform); Supabase maintains its own SOC 2 Type II report.
- Secrets: stored in Supabase Vault and Netlify environment variables; never committed to source control.

Access controls

- Customer access: email-based auth with JWT session tokens (Supabase Auth). Optional SAML SSO on enterprise tier.
- Internal access: all production access requires MFA; quarterly access reviews; service-role keys scoped to specific edge functions.
- Row Level Security: Postgres RLS enforces per-tenant isolation. Customers cannot access another tenant's data even with valid credentials.

Monitoring & incident response

- Application logs: production-safe logger sanitizes PII before write; debug logs suppressed in production builds.
- Incident response: documented IR plan; customer notification within 72 hours of confirmed material incident (GDPR Art. 33).
- Security contact: security@unabatedproducts.com (one business-day response SLA).

Backup & continuity

- Backups: daily automated Postgres backups via Supabase; point-in-time recovery enabled.

- Retention: 7 days minimum on standard tier; 30 days on enterprise tier.
- RTO: 4 hours (target). RPO: 24 hours (daily backup) or 1 minute (PITR).
- Disaster recovery: multi-AZ Postgres failover handled by Supabase platform.

Subprocessors

- Supabase, Inc. - Database, auth, edge functions - US (AWS us-east-1) - SOC 2 Type II.
- Netlify, Inc. - Static hosting, CDN - Global (edge POPs) - SOC 2 Type II.
- Resend - Transactional email - US - SOC 2 Type II.
- GitHub, Inc. - Source code management - US - SOC 2 Type II, ISO 27001.
- Stripe, Inc. (planned) - Payments - US/EU - PCI DSS Level 1, SOC 2.

Updated subprocessor list maintained at unabatedproducts.com/trust.

Secure development

- All code changes require pull-request review before merging to main.
- Dependency vulnerability scanning on every build (npm audit + Dependabot).
- Production deploys only from main via CI; no direct manual deploys.
- Third-party penetration testing (starting 2026 Q3).

Customer rights & data portability

- Export: customers can export their data in JSON/CSV via in-product UI or by request to security@unabatedproducts.com.
- Deletion: account deletion removes all customer data within 30 days; backups purge within an additional 90 days.
- Subprocessor changes: 30 days advance notice; right to object per DPA.

Questions?

- Security & compliance: security@unabatedproducts.com
- Pre-sales technical review: sales@unabatedproducts.com
- Privacy / data subject requests: privacy@unabatedproducts.com

This document is provided for informational purposes during procurement evaluation. Binding security commitments are in the executed Master Services Agreement (MSA) and Data Processing Agreement (DPA).