EmailCos Security Fact Sheet

Version 2026.08 - emailcos.com/security

1. Data handling

Email bodies are processed in memory only. No volumes are mounted in production; machines auto-stop and RAM is wiped. Retention: 0 days email body, 30 days metadata, 60 second analysis purge. We do not train models on customer mail.

2. Encryption

AES-256-GCM at rest for tokens, app passwords and derived metadata, with rotated keys. TLS 1.3 in transit between browser, edge and provider APIs.

3. Authentication and isolation

OAuth2 for Gmail, Outlook 365, Yahoo and Zoho. Encrypted app passwords for the other 23 providers. Short-lived JWT session tokens. Multi-tenant isolation enforced by row-level security; every query is scoped to the authenticated account.

4. Safety guardrails

Deterministic validator checks every amount extraction in code, not the LLM.
Human-in-the-loop approval is mandatory above R500 or any L3 high-risk classification.
EmailCos reads and drafts; it never transacts.

5. Audit and compliance

Tamper-evident SHA-256 hash-chained audit log of every action, approval and access event.
Architected against POPIA, GDPR and SOC 2 principles. Framework alignment, not certification.
Primary region jnb (Johannesburg). EU / UK / ZA residency options.
Information Officer: Xoli Dlabantu - dpa@emailcos.com

6. Contractual

DPA available on request and pre-signed for Partnership Deployment customers.
Security disclosure: security@emailcos.com