AlertOwl

Information Security Policy

Version 1.0 | March 2026
Friday Surprise LLC
CONFIDENTIAL

1. Purpose

This policy establishes the information security framework for AlertOwl, operated by Friday Surprise LLC. It defines the security controls, responsibilities, and procedures for protecting customer data, system integrity, and service availability.

AlertOwl processes business email content and metadata from customer Gmail and Outlook accounts. Given the sensitivity of this data, this policy sets the minimum security standards for all systems, personnel, and processes.

2. Scope

This policy applies to all AlertOwl infrastructure, applications, data, and personnel, including:

- Production systems: n8n workflow engine (DigitalOcean), Supabase PostgreSQL database, Netlify frontend
- Third-party services: Twilio (WhatsApp), Anthropic Claude API, Resend (email), Stripe (billing), Cloudflare (DNS/CDN)
- All personnel with access to production systems or customer data
- All customer data including email metadata, message content, OAuth tokens, and account information

3. Data Classification

Classification	Description	Examples	Handling
Critical	Data that if exposed would cause severe harm	OAuth tokens, API keys, database credentials	Encrypted at rest and in transit. Access restricted to founder only. Never logged.
Confidential	Customer data requiring protection	Email content, sender addresses, WhatsApp numbers, classification results	Encrypted in transit. RLS enforced. Retained per customer settings (default 30 days).
Internal	Business operations data	Workflow logs, error reports, usage analytics	Access restricted to authorized personnel.
Public	Information intended for public access	Marketing content, pricing, documentation	No restrictions.

4. Access Control

4.1 Principle of Least Privilege

All access is granted on a need-to-know basis. No user or system receives more access than required for their role.

4.2 Current Access Matrix

System	Ali (Founder)	Yasir (Associate)	Customers
DigitalOcean (n8n server)	Full SSH + console	No access	No access
Supabase Dashboard	Full admin	No access	No access
Supabase Database (via RLS)	Service role (full)	Own data only	Own data only
n8n Workflow Editor	Full admin	No access	No access
Netlify (frontend deploy)	Full admin	No access	No access
Stripe Dashboard	Full admin	No access	No access
Twilio Console	Full admin	No access	No access
Cloudflare DNS	Full admin	No access	No access
Meta Business Portfolio	Full admin	Admin access	No access
Azure Portal (Entra ID)	Global Admin	No access	No access
AlertOwl Dashboard	Admin + customer view	Customer view	Own data only (RLS)

4.3 Authentication Requirements

- All admin accounts use strong passwords (16+ characters) and MFA where supported
- Customer authentication via Supabase Auth (email + password, bcrypt hashed)
- Email OAuth connections use OAuth 2.0 tokens (no passwords stored)
- API keys stored in environment variables, never in code or version control

4.4 Access Reviews

Access rights are reviewed quarterly by the founder. Any change in personnel triggers an immediate access review and revocation of unnecessary privileges.

5. Encryption

5.1 In Transit

- All external connections use TLS 1.2+ (HTTPS enforced by Caddy reverse proxy and Cloudflare)
- Database connections to Supabase use SSL/TLS
- API calls to Twilio, Anthropic, Resend, and Stripe use HTTPS

5.2 At Rest

- Supabase PostgreSQL: AES-256 encryption at rest (managed by Supabase Pro)
- DigitalOcean droplet: encrypted block storage
- Backups: encrypted via Supabase managed daily backups (7-day retention)

5.3 Known Gap: OAuth Token Encryption

OAuth access_token and refresh_token values in the customer_connections table are currently stored in plaintext. This is identified as a priority remediation item. Plan: implement AES-256-GCM application-layer encryption with key stored in n8n environment variables. Target completion: Phase 9 (post-launch).

6. Network Security

- n8n server is behind Caddy reverse proxy with automatic TLS certificate management
- DigitalOcean firewall restricts inbound access to ports 80, 443, and SSH (key-based only)
- Webhook endpoints validate signatures (Twilio HMAC, Stripe event verification via API callback)
- Content Security Policy (CSP) headers enforced on all frontend pages
- Rate limiting implemented on authentication endpoints

7. Data Retention and Disposal

- Email message content: masked immediately after AI classification (content replaced with "[Content removed for privacy]")
- Email metadata (sender, subject, timestamps): retained per customer setting (default 30 days)
- Classification results: retained with metadata
- Audit logs: retained for 90 days
- Account deletion: soft delete with 7-day grace period, then hard delete cascading all customer data
- OAuth tokens: revoked on account deletion or connection disconnect

8. Logging and Monitoring

- Sentry: real-time error tracking across all n8n workflows and frontend
- n8n execution logs: all workflow runs logged with input/output (sensitive content masked)
- Supabase logs: database query logs retained by Supabase
- Audit log table: records all significant actions (login, data access, settings changes, deletions)

- API usage tracking: daily usage counts per service (Claude, Twilio, Resend) in api_usage_daily table

9. Vendor Management

All third-party services processing customer data are evaluated for security posture:

Vendor	Data Processed	Security Posture	DPA Status
Supabase	All customer data, messages, tokens	SOC 2 Type II, HIPAA ready, encryption at rest	Covered by Supabase ToS + DPA
DigitalOcean	n8n server hosting	SOC 2 Type II, ISO 27001	Covered by DO ToS + DPA
Twilio	WhatsApp numbers, alert message content	SOC 2 Type II, ISO 27001, GDPR compliant	Covered by Twilio DPA
Anthropic (Claude)	Email content for classification (transient)	SOC 2 Type II, zero retention on API	Covered by Anthropic API Terms
Cloudflare	DNS, email routing	SOC 2 Type II, ISO 27001	Covered by Cloudflare DPA
Resend	Email addresses, digest content	SOC 2 Type II	Covered by Resend DPA
Stripe	Billing data, email	PCI DSS Level 1, SOC 2 Type II	Covered by Stripe DPA
Netlify	Frontend hosting (no customer data)	SOC 2 Type II	N/A (static hosting)

10. Acceptable Use

Production systems are used solely for AlertOwl service operations. Personal use, unauthorized software installation, and access from untrusted networks are prohibited.

11. Policy Review

This policy is reviewed annually or upon any significant change in infrastructure, personnel, or business operations. The founder is responsible for policy maintenance and enforcement.

Document Control

Version	Date	Author	Changes
1.0	March 2026	Ali Munir (Founder)	Initial version