Security Policy

Organization: Caliber Technologies Inc. (Calimatic Mail) **Document Version:** 1.0 **Effective Date:** February 14, 2026 **Last Reviewed:** February 14, 2026 **Classification:** Confidential

---

1. Purpose

This policy establishes security controls and practices for the Calimatic Mail platform to protect customer data, maintain service availability, and comply with regulatory requirements.

2. Scope

This policy applies to all Calimatic Mail systems, including:

- Production infrastructure and services
- Application code and configurations
- Employee and contractor access
- Third-party integrations and vendor relationships

3. Infrastructure Security

3.1 Network Security

- All public traffic is encrypted using TLS 1.3 via Let's Encrypt certificates.
- HSTS is enforced with a 1-year max-age, includeSubDomains, and preload directives.
- Traefik reverse proxy handles TLS termination and enforces security headers.
- Internal service communication occurs within isolated Docker networks.
- No services are directly exposed to the internet; all traffic routes through the reverse proxy.

3.2 Container Security

- Applications run in Docker containers with minimal Alpine-based images.
- Multi-stage builds separate build dependencies from production runtime.
- Containers run with limited privileges; no containers run as root in production.
- Container images are built from locked dependency files for reproducibility.

3.3 Database Security

- PostgreSQL database is accessible only within the internal Docker network.
- Database credentials are managed via environment variables, not hardcoded.
- Connection pooling via PgBouncer limits concurrent database connections.
- Unique indexes and constraints enforce data integrity at the schema level.

4. Application Security

4.1 Authentication

- **User Authentication:** JWT tokens with HS256 signing, configurable expiration, and refresh token rotation.
- **API Authentication:** API key-based authentication with role-scoped permissions.
- **OAuth 2.0:** Third-party integrations (Zoom, Google) use OAuth 2.0 with state parameter verification for CSRF protection.
- **Brute-Force Protection:** Account lockout after repeated failed authentication attempts.

4.2 Authorization

- Role-based access control (RBAC) with three tiers: user, admin, and super-admin.
- API routes enforce authorization via Fastify preHandler hooks.
- Multi-tenancy isolation ensures users can only access their own organization's data.

4.3 Input Validation

- All API inputs are validated using Zod schemas with strict type definitions.
- SQL injection is prevented through Drizzle ORM with parameterized queries.
- XSS protection is provided by Content Security Policy headers and React's built-in escaping.

4.4 Security Headers

All HTTP responses include the following security headers:

Header	Value
Strict-Transport-Security	max-age=31536000; includeSubDomains; preload
X-Content-Type-Options	nosniff
X-Frame-Options	DENY
Content-Security-Policy	Restrictive policy allowing only known origins
Referrer-Policy	strict-origin-when-cross-origin
Permissions-Policy	camera=(), microphone=(), geolocation=()
X-XSS-Protection	1; mode=block

4.5 Rate Limiting

- Redis-backed distributed rate limiting across all API endpoints.
- Configurable limits per endpoint category (read, write, sensitive, auth).
- Rate limit headers included in all responses for client-side handling.
- Logging at 80% threshold for proactive monitoring.

4.6 Sensitive Data Handling

- OAuth tokens are stored server-side and never included in HTTP responses to clients.
- An `onSend` hook actively strips sensitive fields from all integration endpoint responses.
- Cache-Control: no-store headers prevent caching of sensitive data (meeting links, IDs, tokens).
- Passwords are hashed with bcrypt; plaintext passwords are never stored or logged.

5. Third-Party Integration Security

5.1 OAuth Integration (Zoom, Google)

- **Principle of Least Privilege:** Only minimum required OAuth scopes are requested.
- **Token Management:** Access tokens and refresh tokens are encrypted at rest in the database.
- **Token Lifecycle:** Automatic refresh with 5-minute expiration buffer; revocation on disconnect.
- **Deauthorization:** Webhook endpoint handles Zoom's `app_deauthorized` event and submits data compliance confirmation.
- **State Verification:** OAuth flow uses base64url-encoded state with userId, provider, timestamp, and nonce.

5.2 Vendor Assessment

Third-party services used (Zoom, Google) are assessed for:

- SOC 2 Type II compliance
- Data processing agreements (DPA)
- Data residency and jurisdiction

6. Access Control

- Production server access is restricted to authorized engineering personnel.
- SSH key-based authentication is required for server access.
- Environment variables and secrets are not committed to version control.

- Principle of least privilege is applied to all system access.

7. Monitoring and Logging

- Structured JSON logging for all API requests and responses.
- Prometheus metrics collection for performance monitoring.
- Grafana dashboards for real-time system health visualization.
- Loki for centralized log aggregation.
- Promtail for log shipping from all containers.

8. Data Encryption

- **In Transit:** TLS 1.3 for all external communications.
- **At Rest:** AES-256 encryption for sensitive data stored in the database.
- **Internal:** Docker network encryption for inter-service communication.

9. Business Continuity

- Database backups are performed regularly.
- Container orchestration enables rapid recovery from failures.
- Health check endpoints enable automatic container restart on failure.
- Multi-service architecture allows individual component recovery without full system downtime.

10. Review Cycle

This Security Policy is reviewed and updated at minimum annually, or when:

- Significant infrastructure changes occur
- New security threats are identified
- Regulatory requirements change
- After any security incident

Approved by: Engineering Team, Caliber Technologies Inc. **Contact:** security@calimatic.app