CAIRL

Enterprise Security Packet

Security architecture, data handling, compliance posture, and infrastructure overview for partner and enterprise security review.

Prepared by:	reAPPlicate Incorporated
Document Version:	1.1
Last Updated:	March 25, 2026
Classification:	External — For Partner and Enterprise Security Review

Table of Contents

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™

1. Company Overview

CAIRL is a privacy-first identity verification platform operated by reAPPlicate Incorporated, a Florida corporation. The platform provides:

- Identity verification using government-issued documents and biometric matching
- Secure encrypted document storage
- OAuth 2.0-based verification claims delivery (PKCE enforced, no raw PII exposure)
- Proxy email services (CAIRL/mail)
- Passkey-first authentication (CAIRL/keys)

CAIRL provides verification signals and infrastructure, not legal identity certification. CAIRL does not act as a financial intermediary, data broker, or custodian of funds.

2. Data Handling Model

2.1 Data Minimization

CAIRL is designed to collect only the data necessary to verify identity, prevent fraud, and provide authorized services.

2.2 Claims-Based Architecture

Connected services receive verification claims only (e.g., "age_18_plus: true", "identity_verified: true"). No raw identity documents, biometric data, or full personal details are shared with connected services unless explicitly authorized by the user through a comparison claim.

CAIRL APIs do not expose raw identity documents or biometric data to connected services.

Claims are generated per request and are not reused across services without user authorization.

2.3 Pairwise Identifiers

Each integration receives a unique, non-correlatable identifier (HMAC-SHA256) for each user. Raw user IDs never leave the CAIRL platform. This prevents cross-platform user correlation.

2.4 Biometric Data Handling

Attribute	Detail
Collection trigger	User-initiated identity verification
Consent mechanism	Explicit UI consent screen, separate from ToS acceptance
Processor	AWS Rekognition (under CAIRL control and instruction)

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™

Attribute	Detail
AWS model training	AWS processes biometric data solely on CAIRL's behalf and under its instructions. CAIRL does not permit the use of this data for model training.
Session data retention	Not retained beyond what is required to complete the session
Biometric reference	May be retained for uniqueness enforcement and fraud prevention
Encryption	AES-256 at rest
Deletion trigger	Account closure, deletion request, or consent withdrawal
Deletion timeline	Within 30 days of trigger event
Sale/sharing	Not permitted and not part of CAIRL's data processing practices
Tracking/profiling	Not permitted and not part of CAIRL's data processing practices
AI/ML training	Not permitted and not part of CAIRL's data processing practices

3. Infrastructure

3.1 Architecture

Component	Provider	Purpose
Application hosting	Vercel	Edge-distributed hosting with DDoS protection
Cloud infrastructure	AWS	Compute, storage (S3), identity verification (Rekognition, Textract), serverless (Lambda)
Database	PostgreSQL (Supabase)	Primary data store
Caching / rate limiting	Upstash Redis	Session management, rate limiting, abuse prevention
Bot protection	Cloudflare	Turnstile challenge on sensitive flows
Payments	Stripe	Billing, subscription, wallet management
Bank linking	Plaid	Bank account verification
Email	Mailgun	Transactional email and proxy relay (CAIRL/mail)
Phone verification	Twilio	OTP delivery and phone number verification

3.2 Environment Isolation

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™

Environment	Database	Storage	URL
Development	cairl-dev	cairl-dev-documents	localhost / Vercel preview
Staging	cairl-staging	cairl-staging-documents	staging.cairl.app
Production	cairl-production	cairl-production-documents	cairl.app

Development, staging, and production environments are fully isolated with separate databases, storage buckets, credentials, and access controls. No development data touches production systems.

3.3 Shared Responsibility

Underlying infrastructure providers (AWS, Vercel) operate under a shared responsibility model. CAIRL secures application-layer systems and access controls, while providers secure the underlying cloud infrastructure.

4. Encryption

Layer	Standard	Detail
Data at rest	AES-256	All stored data including documents, biometric references, and database records
Data in transit	TLS 1.3	All connections between client, server, and third-party services
Key management	Dedicated KMS	Strict access controls, automatic rotation

5. Access Controls

5.1 Internal Access

Control	Implementation
Access model	Role-based access control (RBAC)
Privilege	Least privilege — minimum access required for task
Authentication	Multi-factor authentication required for all staff with data access
Logging	All access to user data is logged
Audit	Subject to periodic review
Data access scope	Need-to-know only — support, technical resolution, fraud investigation, legal compliance

5.2 User Access

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™

Control	Implementation
Password storage	Secure hash (never plain text)
Primary authentication	Passkey-first (WebAuthn) with password fallback
Session management	Scoped, time-limited, revocable
Consent enforcement	Platform-level — connected services cannot bypass user consent

6. Application Security

Control	Implementation
OAuth	PKCE with S256 enforcement on all flows
CSRF	Protection on all state-changing operations
Rate limiting	All sensitive and user-data endpoints
Token model	Short-lived, scoped tokens for integration endpoints
Bot protection	Cloudflare Turnstile on verification and login flows
Identifier isolation	Pairwise HMAC-SHA256 — no raw user IDs exposed to connected services

7. Incident Response

CAIRL maintains internal incident response procedures covering:

- **Detection** — Monitoring and alerting on anomalous access patterns
- **Containment** — Isolation of affected systems and credentials
- **Remediation** — Root cause analysis and patching
- **Post-incident review** — Documentation and process improvement

Incident response procedures are tested periodically as part of internal security practices.

Breach Notification

Obligation	Detail
User notification	As required by applicable law, without unreasonable delay
Controller notification (DPA)	Within 72 hours of becoming aware of the breach
Regulatory notification	As required by applicable federal and state law

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™

Obligation	Detail
Content	Nature of breach, data types affected, approximate scope, mitigation steps

8. Compliance Posture

Framework	Status	Detail
SOC 2 Type II	In preparation	Actively preparing for first formal audit engagement
GDPR	Active	Data controller / processor hybrid model. Consent (biometric) and legitimate interest (service delivery) as legal bases. SCCs in place for international transfers.
CCPA	Active	No sale of personal data. Authorized agent support. Non-discrimination.
BIPA (Illinois)	Active	Explicit consent, published retention/destruction schedule, deletion on request, private right of action acknowledged
Texas CUBI	Active	Biometric consent and deletion practices in place
Washington	Active	Biometric identifier practices in place
COPPA	Active	Guardian-managed participation for minors through circles with verifiable parental consent
HIPAA	Not applicable	CAIRL is not a covered entity or business associate unless explicitly contracted under a BAA

CAIRL does not claim certification until audits are complete and the auditor's report is received.

9. Payments

Attribute	Detail
Payment processor	Stripe
Card storage	CAIRL does not store full card numbers
Financial role	Not a financial intermediary, payment processor, or custodian of funds
Wallet	Prepaid service balance only — not a deposit account or stored value instrument

10. Data Retention

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™

Data Type	Retention	User Control
Raw identity documents	Until user deletes or account closure + 30 days	User-deletable subject to applicable legal, security, and fraud prevention requirements
Biometric session data	Duration of verification session only	Ephemeral
Biometric reference (embedding)	Until deletion request or account closure + 30 days	User-deletable subject to applicable legal, security, and fraud prevention requirements
Verification records	Up to 7 years (regulatory/audit/fraud)	Cannot be deleted due to legal retention
Usage logs	90 days	Automatic expiry
Account information	Until account deletion	User-deletable
Proxy email metadata	90 days	Automatic expiry

11. Third-Party Subprocessors

Subprocessor	Purpose	Role	Location
AWS	Infrastructure, Rekognition, Textract, Lambda, S3	Data processor / subprocessor	United States
Stripe	Payments and billing	Data processor	United States
Vercel	Hosting and content delivery	Data processor	United States (global edge)
Plaid	Bank account verification	Data processor	United States
Mailgun	Email delivery and proxy relay	Data processor	United States
Twilio	Phone verification (OTP delivery)	Data processor	United States
Cloudflare	Bot protection (Turnstile)	Data processor	United States (global edge)
Upstash	Rate limiting and caching	Data processor	United States
Supabase	Primary database (PostgreSQL)	Data processor	United States

All subprocessors operate under contractual and security obligations consistent with CAIRL's Privacy Policy and Data Processing Agreement. CAIRL remains responsible for the performance of its subprocessors. Material subprocessor changes are communicated with 30 days' notice.

12. Available Documentation

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™

Document	Location
Privacy Policy	cairl.app/legal/privacy
Terms of Service	cairl.app/legal/terms
Security Overview	cairl.app/security
Cookie Policy	cairl.app/legal/cookies
Refund Policy	cairl.app/legal/refund
Acceptable Use Policy	cairl.app/legal/acceptable-use
Data Processing Agreement	cairl.app/legal/dpa
Trust Center	cairl.app/trust

13. Contact

Purpose	Contact
Enterprise security inquiries	security@cairl.app
Legal and DPA inquiries	legal@cairl.app
Privacy and data rights	privacy@cairl.app
General	info@cairl.app

Address: reAPPlicate Incorporated, 3200 NW 62nd Avenue #22, Margate, FL 33063

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™

Confidentiality Notice

This document is provided for security review purposes in connection with a potential or existing business relationship with CAIRL. It contains information about CAIRL's security practices and infrastructure. Recipients should treat this document as confidential and not distribute it beyond the individuals and teams directly involved in the security review.

© 2026 reAPPlicate Incorporated. All rights reserved. CAIRL™