CIDENTIA SECURITY PROTOCOL

Version 1.0 - June 2025

Prepared by: The Cidentia Team

1. INTRODUCTION

The Cidentia platform operates at the intersection of digital identity, AI, finance, and public infrastructure. Security is foundational to our mission of building trust in a decentralized, AI-powered ecosystem. This protocol outlines the technical, procedural, and cryptographic measures in place to ensure the confidentiality, integrity, and availability of data and services within Cidentia.

2. SECURITY PRINCIPLES

- Zero Trust: Every user, device, and process must be authenticated and authorized.
- User Sovereignty: Users control their data and decide what is shared.
- Privacy by Design: All features are designed with data minimization and ZK (zero-knowledge) compliance in mind.
- End-to-End Encryption: Data is encrypted at rest and in transit.
- Open Source & Transparency: Core cryptographic code is published and independently auditable.

3. IDENTITY SECURITY

- Biometric Verification: Facial and eye-scan data is hashed, encrypted, and processed locally before submission.
- Face Match System: Uses AI-based comparison models with anti-spoofing measures (liveness detection).
- ZK-Proof Roadmap: Integration of zero-knowledge proofs to verify identity without revealing the biometric input.

- NFT Binding: ID records, documents, and avatars are bound to the verified Cidentia ID via signed NFT metadata.

4. WALLET & TRANSACTION SECURITY

- Multi-Sig Wallets: User wallets support optional multi-signature security.
- Ledger-Backed Logging: Every action (send, receive, connect) is recorded on-chain or in a secure audit trail.
- Address Whitelisting: Users can limit withdrawals to trusted addresses.
- AI Fraud Detection: Behavior models flag unusual transactions in real-time.
- Transaction Reversal Window: Optional 30-second cancellation buffer for accidental sends.

5. DATA PROTECTION

- Cloudinary (Media): Profile and biometric files are stored with signed upload presets and expiring URLs.
- MongoDB Atlas: Encrypted database with IP restrictions, audit logs, and automatic backups.
- Supabase (Auth): Secure JWT-based sessions, email verification, and role-based access control.
- Encryption Protocols:
  - AES-256 for storage
  - TLS 1.3 for transport
  - SHA-256 hashing for biometric and password data

6. BLOCKCHAIN SECURITY (CONCORDIA CHAIN)

- DPoS Validators: Run by regulated entities with KYC and reputation staking.
- Slashing & Audits: Misbehaving validators are slashed and publicly flagged.
- NFT Provenance: Each NFT is uniquely tied to verified metadata and timestamped.
- Smart Contract Security: All contracts are formally verified, tested, and subject to regular third-party audits.

- Cold Storage Reserves: $CONC backing funds held in multi-sig institutional custody.

7. INFRASTRUCTURE SECURITY

- CI/CD Pipeline: Secrets scanning, test automation, and staged deployments.
- Monitoring: Real-time alerts for intrusion detection, error spikes, and abnormal resource use.
- Disaster Recovery: Daily encrypted backups and multi-region deployment across cloud providers.
- Access Management:
  - MFA for all admin access
  - Role-based access enforcement
  - Session timeout and IP whitelisting

8. USER CONTROLS

- Privacy Dashboard: Users can view, download, and delete their data.
- Permissions: Explicit consent required for data linking or third-party API use.
- Identity Reset: If compromised, users can request reset via SafeLink and secondary biometrics.
- Session Management: Revoke tokens and see login history by device and location.

9. THIRD-PARTY INTEGRATIONS

- All third-party services (e.g., Cloudinary, Supabase) are vetted for SOC 2 / ISO 27001 compliance.
- Keys and API tokens are rotated every 30 days and scoped by least privilege.
- Zero data sharing without explicit user consent.

10. CONCLUSION

Security is not a feature - it is the backbone of the Cidentia ecosystem. We commit to continuous testing, transparency, ethical AI, and real human accountability. In a world filled with bots and breaches, Cidentia stands as a fortress of trust for Verified Citizens of the Internet.

For more details, visit https://cidentia.com/security or contact security@cidentia.com