Information Security Policy

PersonaBlocks - Sovereign Identity Verification

Published: April 7, 2026

Version 1.0

Persona Blocks LLC
privacy@personablocks.io
https://www.personablocks.io

1. Purpose

This Information Security Policy establishes the security principles, controls, and practices that PersonaBlocks implements to protect user data, platform infrastructure, and identity verification services. This policy applies to all systems, employees, contractors, and third-party partners involved in the operation of the PersonaBlocks platform.

2. Scope

This policy covers:

- All PersonaBlocks production and development systems
- Identity verification data (biometrics, documents, compliance records)
- Blockchain infrastructure and smart contract operations
- IPFS storage and encryption key management
- Third-party service integrations
- Internal access controls and administrative operations

3. Security Architecture

3.1 Sovereign Encryption Model

PersonaBlocks employs a client-side encryption architecture where users retain sole control of their identity data:

- Key Derivation: Encryption keys are derived from the user's wallet signature using keccak256 hashing, producing a secp256k1 keypair. The platform never stores or transmits private keys.
- Encryption Standard: All identity documents are encrypted using eccrypto AES-256-CBC with ECIES (Elliptic Curve Integrated Encryption Scheme) before leaving the user's browser.
- Zero-Knowledge Storage: The server processes identity data during verification, then encrypts and uploads to IPFS. After encryption, plaintext data is purged from server memory.

3.2 Data Classification

- Critical: Biometric data (facial geometry, selfies, video), government identification documents, encryption private keys
- Sensitive: Compliance screening results, sanctions matches, SAR filings, KYC scores
- Confidential: Wallet addresses, VIC metadata, merchant configurations, audit logs
- Public: On-chain VIC registrations, IPFS content hashes, smart contract addresses

4. Access Controls

4.1 Authentication

- User Authentication: Wallet-based authentication using EIP-191 signed messages. No passwords are stored or transmitted.
- Admin Authentication: EIP-191 wallet signature with 24-hour session tokens. Admin wallets are registered on-chain via the AdminManager smart contract.

- Merchant Authentication: EIP-191 wallet signature with 24-hour session tokens. Merchant registration requires on-chain approval by platform administrators.

4.2 Authorization

- Smart Contract Enforcement: Access control rules are enforced on-chain through the AccessControl smart contract.
- Minimum Privilege: Merchants can only access documents explicitly approved by the customer.
- Session Management: Sessions stored in browser sessionStorage (per-tab isolation). Sessions expire after 24 hours or when the tab is closed.

5. Infrastructure Security

5.1 Transport Security

- All communications use TLS 1.2+ (HTTPS enforced via HSTS)
- CORS restricted to authorized origins only
- Security headers: X-Content-Type-Options, X-Frame-Options DENY, X-XSS-Protection, Referrer-Policy, Permissions-Policy
- Server identification headers (X-Powered-By) disabled

5.2 Application Security

- Input Validation: All API inputs are validated and sanitized server-side
- Error Handling: 5xx error responses are sanitized to prevent internal information leakage
- API Key Protection: Timing-safe comparison for all API key validations
- Rate Limiting: Applied to authentication endpoints and API calls
- Frontend Security: No sensitive data logged to browser console in production

5.3 Blockchain Security

- Smart Contracts: Deployed on Polygon with UUPS upgradeable proxy pattern for critical bug fixes
- Admin Operations: Contract admin functions restricted to registered admin wallets
- Immutability: Document hashes recorded on-chain cannot be altered

6. Data Protection

6.1 Encryption at Rest

- All identity documents stored on IPFS are encrypted with user-controlled AES-256-CBC keys
- Compliance databases (SQLite) are stored on encrypted volumes
- Sanctions screening data is stored locally and not transmitted to third parties

6.2 Encryption in Transit

- All API communications encrypted via TLS 1.2+
- Blockchain transactions signed client-side and submitted over HTTPS RPC endpoints
- IPFS uploads use encrypted HTTPS connections to pinning services (Pinata, Filebase)

6.3 Digital Watermarking & Forensics

- Invisible Watermarking: All decrypted identity images are embedded with cryptographic steganographic watermarks for forensic traceability
- Layered Provenance: Watermarks encode the viewing context (KYC capture, customer view, merchant share, ROI delivery)
- Perceptual Hashing: Document fingerprints enable detection of unauthorized copies, including cropped or reformatted versions

7. Compliance & Regulatory

7.1 Sanctions Screening

- All users screened against OFAC SDN, UN Security Council, EU Financial Sanctions, and Canadian sanctions lists
- Multi-stage name matching: exact match, full-text search, Jaro-Winkler fuzzy matching, DOB boosting
- Matches at or above 0.85 confidence automatically generate SARs
- SAR reports generated in BSA XML 2.0 format for regulatory filing

7.2 Audit Logging

- All document access events are logged with timestamp, actor, action, and document type
- Admin and merchant operations generate immutable audit trail entries
- ROI requests tracked with multi-signature approval workflows
- Audit logs include IPFS hashes and watermark IDs for forensic cross-referencing

7.3 Utah S.B. 275 Compliance

PersonaBlocks is designed to comply with Utah Senate Bill 275 (effective May 6, 2026), which mandates selective disclosure, minimum attribute access, and state-of-the-art safeguards for credential protection.

8. Incident Response

8.1 Detection

- Server-side error monitoring and alerting for anomalous activity
- Authentication failure tracking with automatic session invalidation
- Blockchain event monitoring for unauthorized contract interactions

8.2 Response Procedures

- Identification: Classify incident severity (Critical, High, Medium, Low)
- Containment: Isolate affected systems, revoke compromised sessions or API keys
- Notification: Affected users and merchants notified within 72 hours of confirmed breach
- Recovery: Restore from verified backups, rotate credentials, deploy patches
- Post-Incident: Root cause analysis, policy updates, and preventive measures documented

8.3 Customer Protections

Because PersonaBlocks uses client-side encryption, a server compromise does not expose user identity documents. An

attacker who gains server access would only obtain encrypted blobs that require the user's wallet private key to decrypt.

9. Third-Party Security

- IPFS Pinning Services (Pinata, Filebase): Receive only encrypted data. Cannot access plaintext documents.
- Polygon Network: Public blockchain. Only content hashes and access control metadata are recorded on-chain.
- AI Services (Claude API): Used for liveness analysis. Images processed in-memory and not retained after processing.

10. Physical Security

- Production servers hosted on AWS EC2 with industry-standard physical security controls
- Access restricted to authorized personnel via SSH key authentication (no password access)
- No identity data is stored on local workstations or portable devices

11. Business Continuity

- Data Durability: Identity documents stored on IPFS are pinned across multiple providers for redundancy
- Blockchain Permanence: VIC registrations and document hashes are permanently recorded on Polygon
- User Self-Sovereignty: Users can independently verify and access their encrypted data through IPFS and on-chain records

12. Policy Updates

This Information Security Policy is reviewed and updated at least annually, or whenever significant changes are made to platform architecture, compliance requirements, or threat landscape. Material changes will be communicated through the PersonaBlocks website.

13. Contact

For security concerns, vulnerability reports, or questions about this policy:

PersonaBlocks

Email: privacy@personablocks.io

Website: https://www.personablocks.io