Capital Investment Club

Information Security Policy

Security baseline for assets, data, access, engineering, vendors, incidents, and monitoring.

Last updated: 07/23/2024

Purpose

This policy defines CIC's baseline information security requirements for protecting customer data, platform data, employee data, source code, infrastructure, financial operations, and business systems.

Scope

This applies to CIC personnel, contractors, administrators, service accounts, vendors, cloud environments, repositories, production services, support workflows, and administrative tools.

Security Objectives

- Protect confidentiality, integrity, and availability of CIC systems and data.
- Reduce unauthorized access, data leakage, fraud, abuse, and service disruption.
- Maintain evidence of operating controls.
- Support production API access, customer diligence, partner diligence, and audit readiness.

Information Security Governance

CIC must maintain:

- Information security policy and procedures
- Security risk register
- Asset inventory for critical systems
- Control register
- Incident register
- Access review tracker
- Vulnerability and remediation tracker
- Vendor security review records
- Audit and internal assessment evidence

Security Ownership

- Executive owner: accountable for security risk acceptance.
- Security owner: accountable for policy administration, risk tracking, incident coordination, and evidence

readiness.
- Engineering owner: accountable for secure architecture, SDLC controls, code review, CI/CD controls, and remediation.
- Operations owner: accountable for customer support security, KYC-adjacent handling, support access, and operational controls.
- Finance owner: accountable for wallet, reconciliation, ledger, transaction, and payment-related controls.

Asset Management

CIC must maintain an inventory of critical assets:

- Production applications
- APIs
- Databases
- Cloud services
- Repositories
- CI/CD systems
- Monitoring systems
- Identity providers
- Admin tools
- Vendor systems
- Support tools

Each critical asset must have an owner, purpose, data classification, access model, and recovery expectation.

Asset Criticality

Assets should be tiered by impact:

- Tier 1: Production systems or records that affect authentication, wallets, ledger, grants, pitches, transactions, KYC-adjacent workflows, security monitoring, or customer data.
- Tier 2: Important internal systems that support operations, support, deployments, reporting, or administration.
- Tier 3: Low-risk internal tools with no sensitive data or production impact.

Tier 1 assets require named owners, access review, backup or recovery expectations, monitoring, and change traceability.

Data Protection

CIC must protect:

- User identity and profile data
- Organization data
- Pitch and grant data
- Wallet and transaction data
- Assessment data
- KYC-adjacent workflow data

- Support data and uploaded files
- Security logs
- Source code and secrets

Controls:

- Encrypt sensitive data in transit.
- Encrypt sensitive data at rest where supported by infrastructure.
- Restrict access by role and least privilege.
- Do not store secrets in source code.
- Redact sensitive data from logs where practical.
- Review privileged access quarterly.
- Review standard access at least annually.

Authentication and Access

CIC systems must require authenticated access for non-public functions. Administrative access must be limited to authorized personnel and reviewed on a defined cadence.

Requirements:

- Unique user accounts.
- No shared human accounts except documented break-glass accounts.
- Strong password and session controls.
- MFA for privileged systems where supported.
- Least privilege access.
- Timely removal after role changes or termination.
- Quarterly privileged access review.

Secure Engineering

Engineering teams must follow secure SDLC practices:

- Code review before merge.
- Automated tests for material changes.
- Dependency review for material changes.
- Secrets must not be committed.
- Security-sensitive changes require additional scrutiny.
- Production releases must be traceable to approved changes.

Vulnerability Management

CIC must identify, triage, prioritize, and remediate vulnerabilities.

Minimum remediation targets:

- Critical: immediate triage and remediation plan within 2 business days.
- High: remediation plan within 7 business days.

- Medium: remediation plan within 30 days.
- Low: risk-based remediation.

Exceptions require documented risk acceptance.

Logging and Monitoring

CIC must log security-relevant activity for critical systems where practical:

- Authentication events
- Administrative actions
- Permission changes
- Financial or wallet-impacting actions
- KYC-adjacent actions
- Security configuration changes
- Failed access attempts
- Critical API errors

Logs must be protected against unauthorized alteration and retained based on business, legal, and operational needs.

Configuration and Hardening

CIC should maintain hardened configurations for critical systems:

- Disable unused accounts, ports, services, and integrations where practical.
- Require secure transport for production services.
- Restrict production administration to approved users.
- Maintain environment separation between development, staging, and production.
- Protect production secrets and environment variables.
- Review high-risk configuration changes before release.

Security Monitoring Signals

CIC should monitor or periodically review:

- Failed login spikes.
- Privileged access changes.
- Production configuration changes.
- Suspicious support access.
- Wallet, grant, pitch, or ledger anomalies.
- Unusual API errors.
- Dependency or vulnerability alerts.
- Cloud or repository security alerts.

Encryption and Key Management

CIC should use encryption in transit for production communications and encryption at rest where supported by managed services. Secrets, tokens, and private keys must be stored in approved secret stores or restricted environment configuration. Keys and secrets must be rotated after suspected exposure.

Security Exceptions

Any exception to this policy must define scope, reason, owner, compensating controls, approval, and expiration date.

Incident Response

Suspected security incidents must be escalated promptly. Incident handling must include triage, containment, investigation, remediation, communication, and post-incident review.

Vendor Security

Critical vendors must be reviewed before onboarding and at least annually. Reviews should consider data access, security posture, availability, compliance, breach history, contract terms, and exit risk.

Training and Awareness

Personnel with access to CIC systems must receive security expectations during onboarding and periodic reminders. Privileged users and support personnel require additional training on data handling and account safety.

Evidence

Required evidence:

- Approved policy
- Asset inventory
- Access review records
- Vulnerability tracker
- Incident register
- Vendor reviews
- Security risk register
- Change records
- Training or acknowledgement records
- Internal assessment results

Review

This policy must be reviewed at least annually.