Capital Investment Club

Logging and Monitoring Policy

Logging, monitoring, alerting, retention, review, and response controls for production and security events.

Last updated: 06/01/2026

Purpose

This policy defines CIC's requirements for logging, monitoring, alerting, retention, review, and response for systems that support the CIC platform, including applications, APIs, infrastructure, financial workflows, identity workflows, support tooling, and production integrations.

The goal is to detect, investigate, and respond to security, availability, integrity, privacy, and financial-risk events in a timely and auditable manner.

Scope

This policy applies to:

- Web applications, APIs, notification services, landing pages, and administrative portals.
- Production, staging, development, CI/CD, and cloud infrastructure.
- Authentication, authorization, organization context switching, KYC-adjacent workflows, support access, and administrative actions.
- Wallets, grants, pitches, investments, withdrawals, PFS ledgers, reporting, reconciliation, and financial API integrations.
- Databases, object storage, deployment systems, background jobs, queues, email/SMS services, and third-party providers.
- Employee, contractor, agent, service-account, and automated system activity.

Policy Statement

CIC must maintain logging and monitoring controls that support security operations, incident response, fraud detection, financial integrity, operational reliability, regulatory diligence, and audit readiness.

Logging and monitoring must be designed to:

- Capture meaningful events from critical systems.
- Protect logs from unauthorized access and tampering.
- Avoid logging secrets or unnecessary sensitive data.
- Generate actionable alerts for material risks.
- Preserve enough context for investigation.

- Support incident timelines, audit evidence, and post-incident review.

Logging Requirements

CIC systems should capture logs for:

- User authentication attempts, failures, lockouts, MFA events, and session changes.
- Privileged and administrative activity.
- Organization context switching and role-sensitive access.
- Support access, screen-sharing events, identity-verification code events, file requests, and agent actions.
- Data exports, downloads, profile visibility changes, public content actions, and report-profile workflows.
- Wallet, grant, pitch, investment, withdrawal, contribution, disbursement, ledger, and reconciliation events.
- API requests and responses for critical workflows, excluding sensitive payload values where not required.
- Webhook receipt, validation, retry, and failure handling.
- Database migrations, repair scripts, backfills, and data deletion jobs.
- CI/CD builds, deployments, failed deployments, environment-variable changes, and release activity.
- Security events, suspicious behavior, rate-limit triggers, file upload events, and access-denied outcomes.
- Vendor and financial API integration errors.

Log Content Standards

Logs should include enough context to support investigation without exposing sensitive data.

Expected fields include:

- Timestamp.
- Environment.
- Service or component.
- Event type.
- Actor type and actor ID where appropriate.
- Organization or account context where appropriate.
- Object or resource type and ID where appropriate.
- Stable reason code.
- Outcome.
- Correlation or request ID.
- Error category where applicable.

Logs must not intentionally include:

- Passwords.
- MFA codes.
- Full authentication tokens.
- Private keys.
- Full financial account numbers.
- Unnecessary sensitive personal data.
- Secrets or environment variable values.

Monitoring Requirements

CIC must monitor production systems for:

- Authentication abuse.
- Privileged access anomalies.
- Unauthorized access attempts.
- Unexpected data export or download activity.
- Wallet, grant, pitch, investment, withdrawal, ledger, and reconciliation anomalies.
- Payment, financial API, identity, webhook, and notification integration failures.
- Elevated API error rates.
- Queue backlogs.
- Deployment failures.
- Database errors.
- Infrastructure capacity and availability issues.
- Unexpected changes in traffic, application behavior, or system health.
- Security-control failures.

Alerting Requirements

Alerts must be actionable and assigned to an accountable response path.

Critical alert categories include:

- Production outage or severe degradation.
- Suspected unauthorized access.
- Privileged access misuse.
- Financial transaction integrity failure.
- Wallet or ledger imbalance.
- Failed or suspicious withdrawal activity.
- Data exposure or unauthorized export.
- High-severity vulnerability or exploit indicator.
- Critical vendor/API outage affecting user workflows.
- Failed deployment affecting production.

Each alert should define:

- Severity.
- Trigger condition.
- Owner or response queue.
- Expected triage time.
- Escalation path.
- Runbook or investigation steps.
- Evidence to retain.

Retention and Protection

Log retention must be proportionate to business, security, audit, privacy, and regulatory needs.

Minimum expectations:

- Critical security and administrative logs: at least 12 months where practical.
- Production application and API logs: at least 90 days where practical.
- Financial, ledger, wallet, and reconciliation evidence: retained according to financial operations and legal requirements.
- Incident evidence: retained through investigation and remediation closure.

Logs must be access-controlled, monitored, and protected from unauthorized deletion or alteration.

Review Cadence

CIC must review:

- Critical alerts as they occur.
- Security and production-health dashboards regularly.
- Open logging gaps at least quarterly.
- Alert quality and false positives at least quarterly.
- High-risk event coverage after material product, infrastructure, or vendor changes.
- Logging retention and access controls at least annually.

Evidence

Required evidence may include:

- Logging architecture or system inventory.
- Alert rules and thresholds.
- Monitoring dashboards.
- Alert history.
- Incident tickets and investigation timelines.
- Access reviews for log platforms.
- Log-retention configuration.
- Runbooks.
- Post-incident reviews.

Exceptions

Exceptions must be documented with:

- Scope.
- Reason.
- Risk.
- Compensating controls.

- Owner.
- Expiration date.
- Approval.

Review

This policy must be reviewed at least annually and after material incidents, major architecture changes, or changes to critical production integrations.