Capital Investment Club

Configuration Management Process

Configuration baselines, environment variables, secrets, cloud configuration, endpoint configuration, and review practices.

Last updated: 03/29/2026

Purpose

This process defines how CIC manages configuration for assets, applications, cloud resources, environments, CI/CD workflows, secrets, monitoring, and production integrations.

The objective is to ensure CIC assets are configured consistently, securely, and traceably.

Scope

This process applies to:

- Production, staging, development, and CI/CD environments.
- Web applications, APIs, notification services, landing pages, and administrative portals.
- Cloud infrastructure, databases, storage, queues, and networking.
- Identity, payment, financial API, support, monitoring, and notification integrations.
- Secrets, environment variables, feature flags, deployment settings, and runtime configuration.
- Endpoint security and corporate asset configuration.

Configuration Standards

CIC must define baseline configuration expectations for critical systems.

Baselines should cover:

- Authentication and MFA.
- Least-privilege access.
- Encryption in transit.
- Encryption at rest where supported.
- Logging and monitoring.
- Backup and recovery.
- Secure network exposure.
- Secret storage.
- Dependency and runtime versions.
- Deployment packaging rules.
- File upload limits and allowed types.

- Data retention settings.

Change Control

Configuration changes must follow the Change Management Policy when they affect production, security, privacy, financial workflows, user access, customer data, deployment behavior, or critical integrations.

Configuration changes must capture:

- Change owner.
- Reason.
- Affected environment.
- Before and after value where safe to record.
- Validation evidence.
- Rollback plan.
- Approval where required.

Secrets must not be recorded in tickets, pull requests, logs, screenshots, or documentation.

Environment Variables and Secrets

CIC must manage secrets through approved secret-management or environment-configuration systems.

Requirements:

- Secrets must not be committed to code repositories.
- Production secrets must have restricted access.
- Secrets must be rotated after exposure, suspected exposure, or role change where required.
- Environment-variable additions must be documented.
- Required variables for deployment must be tracked.
- Failed deployments caused by missing variables must be remediated at the environment level or source configuration level.

Infrastructure and Cloud Configuration

Cloud configuration should use:

- Tagged resources.
- Named owners.
- Approved regions.
- Least-privilege service accounts.
- Monitored deployment pipelines.
- Restricted administrative access.
- Logging enabled for critical resources.
- Backup and retention controls for data stores.

Manual console changes to production should be avoided unless approved or required for an emergency. Emergency console changes must be documented after the fact.

Endpoint Configuration

Corporate endpoints should be configured to support:

- Device inventory.
- Endpoint security tooling where available.
- Disk encryption where supported.
- Screen lock.
- Secure update settings.
- Removal of access when users leave CIC.

Review Cadence

CIC should review:

- Production configuration baselines at least annually.
- High-risk environment variables and secrets access at least quarterly.
- Critical cloud configuration at least quarterly.
- Endpoint configuration at least quarterly.
- CI/CD configuration after material workflow or deployment changes.

Evidence

Evidence may include:

- Configuration baseline records.
- Environment-variable register.
- Secret access review.
- Cloud configuration review.
- Deployment logs.
- Endpoint configuration evidence.
- Exception register.
- Remediation tracker.

Review

This process must be reviewed at least annually and after major incidents or infrastructure changes.