Capital Investment Club

Access Control Policy

Provisioning, privileged access, production access, support access, service accounts, and reviews.

Last updated: 03/17/2023

Purpose

This policy defines how CIC grants, reviews, changes, and removes access to systems and data.

Scope

This applies to CIC applications, administrative tools, cloud resources, source code repositories, CI/CD systems, databases, support tools, vendor systems, and any system that stores or processes CIC data.

Access Principles

- Least privilege.
- Need to know.
- Unique user identity.
- Separation of duties for sensitive actions where practical.
- Timely access removal.
- Privileged access review.
- No unmanaged shared accounts.

Access Types

CIC must manage:

- Standard employee access
- Contractor access
- Privileged administrative access
- Production access
- Support access
- Service account access
- Vendor access
- Break-glass access

Provisioning

Access requests must include:

- Requester
- User
- System
- Role or permission requested
- Business justification
- Approver
- Duration if temporary

Privileged access must require manager or system owner approval.

Role-Based Access Model

CIC should maintain role definitions for:

- Platform user.
- Organization member.
- Organization administrator.
- Support agent.
- KYC or verification reviewer.
- Financial operations user.
- Engineering production operator.
- Repository administrator.
- Cloud administrator.
- Security administrator.
- Governance administrator.

Each role should define permitted actions, prohibited actions, data access, approval authority, and review cadence.

Authentication

Requirements:

- Unique accounts for human users.
- MFA for privileged systems where supported.
- Strong password requirements where password-based authentication is used.
- Session timeout or reauthentication for sensitive workflows where practical.

Privileged Access

Privileged access includes production admin, database admin, cloud admin, repository admin, CI/CD admin, financial operations admin, KYC/support admin, and security admin.

Controls:

- Approved before provisioning.
- Reviewed quarterly.

- Logged where supported.
- Removed when no longer required.
- Elevated only for defined business need.

Production Access

Production access should be limited. Direct production data access should be avoided when operational tooling can accomplish the same task safely.

Production data access must be:

- Approved.
- Logged where practical.
- Time-bound when temporary.
- Limited to the required scope.

Support Access

Support access to user or organization data must be limited to authenticated support workflows and legitimate business need.

Support personnel must not access user data out of curiosity, for personal reasons, or without an operational purpose.

Service Accounts

Service accounts must:

- Have named owner.
- Have limited scope.
- Use managed secrets.
- Be reviewed at least annually.
- Not be used by humans except during documented break-glass procedures.

Access Reviews

Minimum cadence:

- Privileged access: quarterly.
- Standard access: annually.
- Vendor access: quarterly for critical vendors or annually for lower-risk vendors.
- Service accounts: annually.

Access reviews must document reviewer, date, systems reviewed, access retained, access removed, exceptions, and remediation.

Deprovisioning

Access must be removed promptly when personnel leave CIC, change roles, complete contractor work, or no longer need access.

High-risk access should be removed immediately upon termination or role change.

Context Switching and Organization Access

Where CIC allows users to switch between personal and organization contexts, the platform must avoid exposing stale data from a prior context. Context switch actions should reload relevant data, clear context-specific state, and enforce authorization server-side and front-end where practical.

Access Review Procedure

Access reviewers must:

1. Obtain current access export. 2. Compare access against current role and business need. 3. Confirm privileged and production access remains justified. 4. Identify access to remove or downgrade. 5. Track remediation to completion. 6. Retain reviewer, date, scope, results, and exceptions.

Break-Glass Procedure

Break-glass access must be restricted, logged where practical, approved after use if prior approval was impossible, and reviewed promptly after use.

Exceptions

Exceptions must be documented, approved, time-bound, and reviewed before expiration.

Evidence

Required evidence:

- Access request records
- Approval records
- Access review records
- Deprovisioning records
- Privileged access list
- Service account inventory
- Break-glass usage record

Review

This policy must be reviewed at least annually.