Capital Investment Club

Financial Operations and Reconciliation Policy

Wallets, grants, pitches, ledgers, journal postings, duplicate prevention, reconciliation, and financial access.

Last updated: 03/31/2024

Purpose

This policy defines governance requirements for CIC financial workflows, including wallets, grants, pitches, ledger postings, disbursements, fees, reconciliations, and financial operations access.

Scope

This applies to wallet balances, deposits in trust, grant wallets, pitch wallets, project wallets, user wallets, organization wallets, transaction records, ledger entries, journal postings, assessment fees, investment flows, grant funding, disbursements, and financial reporting.

Financial Control Objectives

- Preserve transaction integrity.
- Prevent unauthorized financial actions.
- Maintain accurate user, organization, grant, pitch, and project balances.
- Ensure journal entries and ledger postings are traceable.
- Detect duplicate postings, missing postings, and reconciliation differences.
- Restrict financial operations access.
- Maintain evidence for audit and investigation.

Access Controls

Financial operations access must be:

- Approved before provisioning.
- Limited by role and need.
- Reviewed at least quarterly for privileged financial access.
- Logged where supported.
- Removed promptly when no longer needed.

Financial Roles and Segregation

Financial workflows should separate duties where practical.

Role	Typical responsibilities	Restrictions
Finance operator	Review reconciliations, prepare corrections, monitor exceptions	Should not approve own high-risk correction
Finance approver	Approve high-risk corrections, disbursements, and repair activity	Should not directly prepare all supporting evidence
Engineering owner	Build and maintain financial workflow logic	Should not execute production repairs without approval
Support owner	Intake user-facing wallet or transaction issues	Should not independently change balances
Governance admin	Review access and evidence	Should not initiate financial postings

If full segregation is not practical because of team size, CIC must retain compensating evidence such as independent review, pull request approval, before-and-after reconciliation, and leadership approval.

Transaction Integrity

Wallet, grant, pitch, project, investment, disbursement, and ledger operations should be designed to avoid:

- Duplicate postings
- Missing postings
- Mismatched wallet and ledger balances
- Overfunding
- Unauthorized disbursement
- Incorrect equity or ownership calculations
- Incorrect currency display or conversion
- Stale draft funding records

Financial Event Inventory

CIC should maintain an inventory of financial events and expected accounting behavior.

Examples include:

- Wallet top-up or deposit.
- Wallet withdrawal.
- Grant draft creation.
- Grant publication and creator contribution.
- Co-grantor invitation acceptance and contribution.
- Grant disbursement.
- Pitch investment.
- Equity allocation.

- Assessment fee setting and settlement.
- Refund, reversal, or correction.
- Platform fee recognition.

Each event should identify source system, trigger, actor, expected wallet movement, expected ledger movement, idempotency key, reversal path, and audit evidence.

Change Review

Changes affecting financial workflows require heightened review and testing.

Examples:

- Grant funding and contribution logic
- Wallet transfers
- Disbursements
- Pitch investment and equity calculations
- Ledger posting
- Currency conversion
- Fee calculation
- Reconciliation reports

Reconciliation

CIC should maintain reconciliation procedures for:

- User wallet balances
- Organization wallet balances
- Grant wallets
- Pitch wallets
- Project wallets
- Ledger entries
- Journal postings
- External payment or banking provider records where applicable

Reconciliation differences must be documented, investigated, assigned, and resolved.

Reconciliation Procedure

1. Identify population and period. 2. Pull wallet, ledger, transaction, and external provider records. 3. Compare opening balance, movements, and ending balance. 4. Identify duplicates, missing records, stale draft funding, currency mismatch, and failed postings. 5. Assign exceptions to an owner. 6. Correct through approved repair process. 7. Retain evidence before and after repair. 8. Review recurring exceptions for root cause.

Reconciliation Frequency

Reconciliation	Minimum frequency	Owner	Required evidence
User and organization wallets to transaction ledger	Monthly	Finance owner	Reconciliation workbook or report
Grant wallets to grant funding records	Monthly	Finance owner	Grant wallet reconciliation
Pitch/project wallets to investment records	Monthly	Finance owner	Investment reconciliation
Journal entries to ledger report	Monthly	Finance owner	Posted journal report
External payment or banking provider to CIC ledger	Monthly when provider is active	Finance owner	Provider statement tie-out
High-risk repair or migration result	Per event	Finance and engineering owners	Before and after evidence

Exception Thresholds

Financial exceptions should be escalated based on impact.

- Any unexplained user-fund discrepancy must be treated at least High severity.
- Any repeat duplicate posting pattern must be escalated for engineering root-cause review.
- Any equity allocation discrepancy must be reviewed before related investment workflows continue.
- Any production repair touching more than one account, grant, pitch, or wallet pool requires documented approval.
- Any stale draft funding record must be corrected or justified before relying on grant funding reports.

Journal Posting Controls

Journal postings should include:

- Document number
- Posting date
- Company
- Currency
- Ledger type
- Debit and credit lines
- Profit area or stewardship metadata where applicable
- User who posted
- Status
- Supporting explanation

Posted entries should be viewable and auditable. Reversals must be traceable to original entries.

Idempotency and Duplicate Prevention

Financial posting services should use idempotency keys, transaction references, reservation group IDs, or equivalent safeguards to prevent duplicate ledger and wallet postings. Historical repair scripts must be idempotent

and should be tested on representative data before execution.

Repair and Backfill Controls

Repair scripts and backfills must:

- Have a documented purpose and scope.
- Be reviewed before execution.
- Be tested against representative data where practical.
- Be idempotent or explicitly protected against duplicate execution.
- Record dry-run results when supported.
- Retain before-and-after counts and affected record identifiers.
- Be tied to a remediation item, incident, or approved change.

User-Facing Accuracy

Financial data displayed to users must not overstate or misrepresent balances, funding state, contribution state, equity, fees, due dates, or public grant status. User-facing labels should distinguish draft, pending, posted, reserved, contributed, funded, disbursed, reversed, and failed states.

Exception Severity

Financial exceptions should be rated:

- Critical: user funds, grant funds, investment equity, or ledger integrity materially wrong.
- High: financial report or balance materially inaccurate but contained.
- Medium: delayed or incomplete posting with no user harm.
- Low: display or metadata issue with no financial impact.

Evidence

Required evidence:

- Financial access review
- Transaction logs
- Reconciliation records
- Exception records
- Journal posting records
- Duplicate prevention test evidence
- Financial workflow change reviews
- Remediation tracker

Review

This policy must be reviewed at least annually.