Capital Investment Club

Personnel Screening and Background Check Process

Role-based screening and background check practices for employees, contractors, agents, and privileged users.

Last updated: 11/10/2025

Purpose

This process defines CIC's approach to personnel screening and background checks for employees, contractors, and privileged service providers who may access CIC systems, customer data, production environments, financial workflows, or sensitive internal operations.

Scope

This process applies to:

- Employees.
- Contractors.
- Temporary staff.
- Support agents.
- Administrators.
- Engineers and operators with access to production systems.
- Finance, reconciliation, PFS, wallet, payment, or withdrawal workflows.
- Individuals with access to consumer financial data or sensitive personal data.

Screening Requirements

CIC should perform screening proportionate to role risk and local legal requirements.

Screening may include:

- Identity verification.
- Employment or engagement verification.
- Reference checks.
- Criminal background check where legally permitted and role-appropriate.
- Education or credential verification where relevant.
- Sanctions or restricted-party screening where relevant.
- Conflict-of-interest acknowledgement.

- Confidentiality and acceptable-use acknowledgement.

Role-Based Risk

Higher-risk roles include personnel with:

- Production system access.
- Administrative or privileged access.
- Access to consumer financial data.
- Access to wallet, withdrawal, ledger, grant, pitch, or investment workflows.
- Access to support identity verification, screen-sharing, or file-request functions.
- Ability to approve payments, change bank information, or alter user permissions.

Timing

Screening should occur before access is granted to sensitive systems or data, unless a documented exception is approved.

Re-screening or additional review may be required when:

- A person moves into a higher-risk role.
- Access expands materially.
- A policy violation occurs.
- A legal or contractual requirement changes.
- CIC receives credible risk information.

Privacy and Fairness

Personnel screening must be conducted in a manner consistent with applicable law and privacy commitments.

Requirements:

- Collect only information necessary for the screening purpose.
- Restrict access to screening results.
- Retain screening records according to applicable retention requirements.
- Provide notices and authorizations where required.
- Apply screening requirements consistently for comparable roles.

Evidence

CIC should retain:

- Screening completion record.
- Role-risk classification.
- Access approval record.
- Confidentiality or acceptable-use acknowledgement.
- Exception approvals.

- Review records for privileged role changes.

Exceptions

Exceptions must be documented with:

- Reason.
- Role.
- Access requested.
- Risk acceptance.
- Compensating control.
- Expiration.
- Approval.

Review

This process must be reviewed at least annually.