Capital Investment Club

Customer Support and Identity Verification Policy

Authenticated support, call-back codes, agent codes, file requests, screen sharing, and queue governance.

Last updated: 08/16/2023

Purpose

This policy defines how CIC support teams authenticate users, handle support requests, protect support data, request evidence, share screens, and document support outcomes.

Scope

This applies to authenticated support workflows, call-back support, chat support, file requests, screen sharing, account troubleshooting, organization support, wallet-related support, grant support, pitch support, and KYC-adjacent help.

Support Principles

- Support must be provided only for authenticated users unless the workflow is explicitly designed for pre-authentication support.
- Support access must be limited to legitimate support purposes.
- Support personnel must verify user identity before discussing sensitive account details.
- Support data must be treated as confidential or restricted based on content.
- Support interactions should be logged enough to support quality, security, audit, and dispute resolution.

Identity Verification

For sensitive support actions, CIC should verify the user through one or more approved methods:

- Logged-in session context.
- One-time user verification code.
- Agent identification code shown to the user.
- Verified phone number or email.
- Organization membership validation.
- Additional checks for wallet-impacting or identity-sensitive actions.

Sensitive Support Actions

Sensitive actions include:

- Changing account email, phone, password, or authentication settings.
- Discussing wallet, transaction, grant funding, investment, or disbursement details.
- Updating organization owner or administrator access.
- Accessing KYC-adjacent or verification information.
- Handling uploaded identity, financial, or legal documents.
- Troubleshooting public profile visibility or impersonation reports.
- Reopening, withdrawing, or modifying high-impact platform workflows.

Call-Back Support

When CIC calls a user:

- The user should see a user verification code.
- The agent should provide an agent identification code.
- Codes should expire after a short period.
- Support session metadata should be retained.

Screen Sharing

Screen sharing must be user-initiated or user-approved. Support agents should remind users not to expose passwords, secrets, private keys, payment credentials, or other sensitive information.

File Requests

Support agents may request files only when needed. Requests must state what is needed and why.

File handling requirements:

- Classify uploaded files based on content.
- Restrict access to support personnel with need-to-know.
- Do not request more information than needed.
- Retain files according to retention schedule.
- Delete or archive files when no longer required and legally permissible.

Prohibited Support Actions

Support personnel must not:

- Ask users for passwords.
- Ask users for full payment credentials unless handled through approved secure workflows.
- Access unrelated account data.
- Change sensitive account settings without authorization.

- Share private user data with unauthorized parties.

Support Queue Governance

Support queues should track:

- Requester
- Account or organization context
- Issue category
- Priority
- Assigned agent
- Status
- Verification result
- Requested files
- Screen share indicator
- Resolution
- User rating
- Feedback

Queue Status Model

Support records should use clear statuses so requests can be governed and reported.

Recommended statuses:

- New: request submitted and not yet triaged.
- Triage: support is confirming scope, priority, and user context.
- Waiting for user: support requested information, file, or consent.
- Waiting for CIC: assigned owner is investigating or preparing response.
- Escalated: specialist, engineering, security, privacy, or finance support is required.
- Resolved: user-facing answer or action completed.
- Closed: ticket is complete and no further action is expected.

High-risk tickets should not be closed until verification evidence, action evidence, and disposition are recorded.

Priority Model

Priority	Examples	Target handling
Critical	Suspected account takeover, wallet-impacting issue, privacy incident, platform-wide outage	Immediate triage and escalation
High	Failed funding or disbursement, organization access issue, verification blocker, public impersonation report	Same business day triage
Medium	Workflow confusion, profile issue, grant or pitch setup issue	Standard support queue

Low	General question, feature request, cosmetic issue	Standard support queue

Agent Code Procedure

For call-back support:

1. User requests a call while authenticated. 2. CIC displays a user verification code and agent identification code. 3. Agent provides the agent identification code. 4. User provides the user verification code. 5. Agent records verification success or failure. 6. Codes expire automatically and must not be reused.

Screen Share Procedure

Before a screen share begins, support must:

- Confirm the user is authenticated.
- Explain the purpose of the session.
- Ask the user to close unrelated windows and hide sensitive information.
- Confirm whether the session is recorded.
- Record consent in the support ticket where practical.

During a screen share, support must not ask the user to reveal passwords, one-time passwords, private keys, complete payment credentials, or unrelated personal information. If sensitive information appears, the agent should pause and instruct the user to hide it.

File Request Procedure

File requests must be specific and proportional.

A valid file request should record:

- File requested.
- Reason the file is needed.
- Classification expectation.
- Retention expectation.
- Who can access it.
- Whether the file contains identity, financial, legal, or security-sensitive information.
- Disposition after the ticket is resolved.

Escalation Paths

Support must escalate:

- Security incidents to the security owner.
- Privacy requests to the privacy owner.
- Wallet, ledger, payment, and disbursement issues to the finance owner.
- Engineering defects to the engineering owner with reproduction steps and evidence.

- Organization governance disputes to the operations or governance owner.
- Legal or regulatory concerns to leadership or counsel.

Quality Review

CIC should periodically review support tickets for proper verification, minimum necessary data access, accurate disposition, and user satisfaction.

Quality review should sample tickets across normal support, call-back support, screen sharing, file requests, sensitive account actions, and escalated issues.

Customer Feedback

Support sessions should allow the user to rate the experience and leave feedback. CIC should periodically review ratings, reopened tickets, long-running queues, and unresolved escalations to improve support workflows.

Metrics

Support leadership should monitor:

- Volume by category and priority.
- First response time.
- Time to resolution.
- Reopened tickets.
- Verification failure rate.
- File request volume.
- Screen share volume.
- Escalation rate.
- User satisfaction rating.

Evidence

Required evidence:

- Support ticket records
- Verification records
- File request records
- Screen sharing consent records where practical
- Support outcome records
- Feedback and rating records
- Support access reviews

Review

This policy must be reviewed at least annually.