Capital Investment Club

Data Classification, Privacy, and Retention Policy

Data classes, handling rules, support data, logs, retention, deletion, and evidence.

Last updated: 09/23/2023

Purpose

This policy defines how CIC classifies, protects, uses, shares, stores, retains, and deletes data.

Scope

This applies to user data, organization data, pitch data, grant data, wallet and transaction data, assessment data, support data, uploaded files, logs, employee data, vendor data, and internal business data.

Data Classes

Public

Approved for public disclosure, such as public landingpage content and public profile information intentionally made public by users.

Internal

CIC business information not intended for public release.

Confidential

Sensitive business, customer, platform, or operational data that could cause harm if disclosed.

Restricted

Highly sensitive data requiring strict access control. Examples may include wallet-impacting data, sensitive identity data, support verification data, production secrets, security findings, and privileged logs.

CIC Data Type Mapping

Data type	Default classification
Public landingpage content	Public

Data type	Default classification
Public profile content intentionally published	Public
User account profile data	Confidential
Organization member and role data	Confidential
Wallet, transaction, ledger, and disbursement data	Restricted
KYC-adjacent and verification support data	Restricted
Security findings and incident records	Restricted
Source code and internal architecture	Confidential
Production secrets and credentials	Restricted
Support tickets and uploaded support files	Confidential or Restricted based on content

Data Inventory Requirements

CIC should maintain a data inventory that identifies:

- Data category.
- System of record.
- Business owner.
- Technical owner.
- Classification.
- Data subjects affected.
- Collection purpose.
- Public display status.
- Retention period.
- Deletion method.
- External sharing or subprocessors.
- Legal or contractual constraints.

The inventory should be reviewed at least annually and whenever CIC introduces a material new data field, upload flow, support workflow, financial workflow, or public profile feature.

Data Handling Requirements

Public

- Confirm content is approved for public release.
- Avoid accidentally publishing private user or organization data.

Internal

- Limit to CIC personnel and authorized contractors.
- Do not publish externally without approval.

Confidential

- Limit access by business need.
- Store in approved systems.
- Avoid unnecessary copying or local storage.
- Redact where practical in logs and support workflows.

Restricted

- Limit to explicitly authorized users.
- Review access periodically.
- Encrypt in transit and at rest where supported.
- Avoid logging except where security or audit requires it.
- Use heightened controls for access and retention.

Privacy Principles

CIC should:

- Collect data for legitimate business purposes.
- Limit data access to need-to-know.
- Communicate how data is used.
- Maintain support workflows that protect user privacy.
- Retain data only as needed for business, legal, security, operational, and audit purposes.
- Delete or de-identify data when no longer needed and legally permissible.

Collection and Use Review

Before introducing new data collection, CIC should confirm:

- The business purpose is clear.
- The field is necessary for the workflow.
- The classification is known.
- The field is not accidentally public.
- The retention period is known.
- Access can be limited by role and context.
- The privacy policy, terms, or user-facing notice remains accurate.

Support Data

Support workflows may include sensitive information, screenshots, files, phone numbers, identity verification context, or account details.

Requirements:

- Support access must be authenticated and role-limited.
- Support personnel must only access data for legitimate support purposes.
- Uploaded support files must be handled as confidential or restricted based on content.
- Support records must be retained based on operational and legal needs.

Logging

Logs should avoid sensitive data where practical. When sensitive logs are necessary for security, debugging, fraud prevention, or audit, access must be restricted.

Logs should not intentionally store passwords, one-time passwords, full payment credentials, private keys, unnecessary identity documents, or complete sensitive files. If sensitive data appears in logs, CIC should treat it as an incident or remediation item based on impact.

Retention

CIC must maintain a retention schedule for:

- User profile data
- Organization data
- Pitch and grant records
- Wallet and transaction records
- KYC-adjacent records
- Support records
- Security logs
- Audit evidence
- Employee and contractor records
- Vendor records

Retention periods should reflect legal, financial, security, fraud prevention, customer support, and business requirements.

Baseline Retention Schedule

Final retention periods should be approved by CIC leadership and counsel, but the following baseline should guide program operations.

Data category	Baseline retention	Notes
User account and profile data	Life of account plus approved retention period	Preserve records needed for disputes, fraud prevention, and legal obligations.
Public profile content	Until removed by user or account closure, subject to legal retention	Public visibility must honor profile settings.
Organization membership and governance records	Life of organization plus approved retention period	Needed for authority and dispute history.

Data category	Baseline retention	Notes
Wallet, transaction, ledger, grant, pitch, project, and disbursement records	At least 7 years unless counsel approves otherwise	Financial integrity and audit trail.
Support tickets	3 years unless sensitive or legally required longer	Sensitive attachments may have shorter retention if not needed.
Security logs	1 year where practical for critical systems	Longer for incidents or investigations.
Incident records	7 years or legal requirement	Preserve timeline, impact, and remediation.
Vendor reviews and contracts	Contract life plus 7 years	Preserve diligence and obligations.
Policy evidence and control testing	At least 3 years	Longer if required for audit or contract.

Data Minimization

CIC should avoid collecting unnecessary sensitive data. Product teams should review new fields, uploads, and support requests for necessity, retention impact, public visibility risk, and access requirements.

Public Display Review

Before displaying profile, credential, evidence, wallet, grant, pitch, or organization data publicly, CIC should confirm the information is intended for public display and does not expose private evidence, sensitive verification details, private contact details, or misleading verification status.

Retention Schedule Administration

The retention schedule should identify owner, data category, system of record, retention period, deletion method, legal hold process, and evidence of deletion or archival.

Deletion

Deletion requests must be reviewed against legal, security, financial, fraud, contractual, and operational retention requirements.

Deletion Workflow

Deletion or de-identification should follow a controlled workflow:

- Verify requester identity and authority.
- Identify systems and data categories in scope.
- Check legal hold, financial record, fraud, security, and dispute constraints.
- Delete, de-identify, or restrict data where approved.
- Record systems searched and action taken.
- Notify requester of outcome when required.
- Retain the request record and legal basis for any denial or limitation.

Data Sharing

CIC should share data with vendors, partners, service providers, or legal recipients only when there is a business purpose, approved contractual basis, access limitation, and retention expectation. External sharing of restricted data requires heightened review.

Legal Hold

When litigation, investigation, audit, dispute, or regulatory inquiry requires preservation, CIC must suspend deletion for affected records until the hold is released by authorized leadership or counsel.

Evidence

Required evidence:

- Data classification inventory
- Retention schedule
- Access review records
- Support access records
- Data deletion records
- Privacy review records

Review

This policy must be reviewed at least annually.