Capital Investment Club

Cookie Policy

Public-facing cookie and similar technology notice for authentication, preferences, analytics, and security.

Last updated: 06/07/2026

Purpose

This Cookie Policy explains how Capital Investment Club may use cookies and similar technologies on CIC websites and applications.

Scope

This policy applies to CIC public websites, authenticated platform applications, admin portals, help or support widgets, analytics tooling, embedded media, security tooling, and any mobile or browser-based experience that stores identifiers on a user's device. It covers first-party cookies set by CIC and third-party cookies or similar storage set through providers that CIC configures.

What Cookies Are

Cookies are small files or records stored by a browser or device. Similar technologies may include local storage, session storage, pixels, tags, and SDK-provided storage.

How CIC Uses Cookies

CIC may use cookies and similar technologies for:

- Authentication and session management.
- Security and fraud prevention.
- Remembering user preferences.
- Platform functionality.
- Analytics and performance measurement.
- Error monitoring and debugging.
- Product improvement.

Cookie Categories

Strictly Necessary

Required for login, security, routing, session management, and core platform functionality.

Examples may include authentication session identifiers, CSRF protection tokens, load-balancing state, fraud-prevention state, and selected account context needed to prevent users from seeing data for the wrong user or organization.

Functional

Used to remember settings such as preferences, selected account context, display choices, or workflow state.

Examples may include currency preference, saved filters, accessibility settings, support widget state, and whether a user has dismissed non-critical notices.

Analytics and Performance

Used to understand usage, performance, errors, and feature effectiveness.

Analytics should be configured to avoid collecting sensitive profile, wallet, payment, message, support, or document contents unless a specific approved business need and privacy review exists.

Security

Used to detect suspicious activity, protect accounts, and support incident investigation.

Security technologies may support bot detection, abuse prevention, rate limiting, device or browser fingerprint risk signals, suspicious-login detection, and incident forensics.

Advertising or Marketing

CIC should not deploy advertising or retargeting cookies by default. If CIC later deploys marketing cookies, they must be added to the cookie register, classified as non-essential, disclosed to users, and controlled through an appropriate consent or preference workflow where required.

Third-Party Cookies

CIC may use third-party providers for hosting, analytics, security, support, payment, or communication features. These providers may use cookies or similar technologies according to their own policies and CIC's configuration.

Third-party technologies must have an assigned business owner and must be reviewed before implementation when they can process personal information, track users across sessions, support customer support interactions, or affect authentication, payments, wallets, public profiles, grants, pitches, marketplace activity, or messaging.

User Choices

Users may control cookies through browser settings. Blocking cookies may affect authentication, account access, security, and platform functionality.

Where CIC provides an in-product cookie preference tool, users should be able to change non-essential choices without creating a support ticket. Preference choices should be recorded with timestamp, browser or device context where practical, policy version, and consent state.

Operational Cookie Register

CIC should maintain an internal cookie and tracking technology register with:

- Cookie or technology name.
- Provider.
- Category.
- Purpose.
- Data collected.
- Duration.
- Whether it is first-party or third-party.
- Whether it is strictly necessary.
- Link to provider policy where applicable.

Consent and Preference Management

Where required, CIC should provide a cookie notice or preference workflow that allows users to understand non-essential cookies and manage choices. Strictly necessary cookies may remain active because they are required for authentication, security, and platform operation.

The consent workflow should:

- Avoid pre-selecting non-essential categories where opt-in consent is required.
- Explain the purpose of each category in plain language.
- Preserve access to strictly necessary platform functions.
- Record the user's choice and policy version.
- Provide a way to update choices later.
- Avoid dark patterns that make rejection materially harder than acceptance.

Implementation Controls

Before adding or changing cookies or similar technologies, the owner must:

1. Identify the provider, cookie names, data elements, purpose, and retention. 2. Classify the technology as strictly necessary or non-essential. 3. Confirm whether the provider receives personal information. 4. Confirm whether a DPA, security review, or vendor review is required. 5. Update the cookie register and public disclosure. 6. Test that preference choices are honored. 7. Confirm that sensitive values are not stored in browser-accessible storage.

Prohibited Cookie Practices

CIC must not:

- Store passwords, full authentication secrets, payment credentials, KYC evidence, wallet transaction details, or sensitive uploaded document contents in cookies or browser storage.
- Use non-essential tracking before required consent is obtained.
- Deploy third-party tracking that conflicts with CIC's Privacy Policy or user choices.
- Reuse security or authentication cookies for marketing analytics.
- Keep obsolete cookies active after the related provider or feature is removed.

Retention and Expiration

Cookies should expire no later than needed for their stated purpose. Session cookies should expire when the session ends unless persistent login or security requirements justify a longer duration. Long-lived identifiers require privacy review and documented business justification.

Testing and Monitoring

CIC should test cookie behavior after releases that affect authentication, analytics, support, security, public pages, or account-context switching. Testing should verify that:

- Essential cookies are present only as needed.
- Non-essential cookies respect preferences.
- Login, logout, and context switching clear or refresh relevant state.
- Browser storage does not expose sensitive content.
- Cookie disclosures match actual runtime behavior.

Review Cadence

Cookie usage should be reviewed when CIC changes analytics, advertising, support, security, authentication, or monitoring providers and at least annually.

Changes

CIC may update this Cookie Policy as platform features and providers change.

Contact

Questions should be sent through CIC's support or governance contact channels.