Capital Investment Club

Financial API Production Access Readiness Policy

Production readiness for financial, identity, banking, payment, verification, and related API providers.

Last updated: 02/22/2024

Purpose

This policy defines how CIC prepares for and maintains production access to financial, identity, banking, payment, verification, and related APIs that require security, privacy, operational, and compliance readiness.

Scope

This applies to API providers used for bank account connectivity, wallet funding, payments, identity verification, transaction data, risk screening, notifications tied to financial activity, or other regulated or high-trust workflows.

Readiness Objectives

CIC must be able to demonstrate:

- A legitimate production use case.
- A published privacy policy.
- Clear user consent and data use notices.
- Data minimization and retention controls.
- Secure handling of tokens, secrets, webhooks, logs, and API responses.
- Access control over production dashboards and API credentials.
- Incident response and user notification process.
- Vendor and subprocessor governance.
- Support and data rights request handling.
- Testing evidence for critical user flows.

Production Access Intake

Before requesting production access from a financial API provider, CIC should document:

- Provider name.
- Products or APIs requested.
- Business use case.
- User data involved.

- Data classification.
- User consent flow.
- Systems receiving provider data.
- Storage and retention approach.
- Security controls.
- Support and escalation owner.
- Provider-specific requirements and evidence.

User Consent and Transparency

User-facing flows must explain what CIC is asking the user to connect or authorize, why it is needed, what data may be accessed, how data is used, and how the user can disconnect or request support.

Consent records should be retained where practical and tied to account, organization, or wallet context.

Data Handling Requirements

Financial API data should be classified as Confidential or Restricted depending on sensitivity.

CIC must:

- Store only what is needed.
- Avoid logging sensitive API payloads unless necessary for security or debugging.
- Restrict access to API data by role and business need.
- Encrypt data in transit and at rest where supported.
- Protect API tokens, refresh tokens, webhooks, and secrets.
- Retain and delete provider data according to user commitments, provider terms, and legal requirements.

Production Credential Controls

Production credentials must:

- Be stored in approved secret management or environment configuration.
- Not be committed to source code.
- Have a named owner.
- Be rotated after suspected exposure, personnel changes, or provider requirement.
- Be limited by environment where supported.
- Be reviewed at least quarterly for privileged access.

Webhook and Integration Controls

Provider webhooks and callbacks must be validated where supported.

Controls should include:

- Signature or token verification.
- Idempotent processing.

- Replay protection where practical.
- Error logging without sensitive data exposure.
- Alerting for repeated failures.
- Reconciliation where financial state is affected.

Testing Requirements

Before production launch, CIC should test:

- Connection or authorization flow.
- Revocation or disconnect flow.
- Error handling for expired, revoked, or failed provider access.
- Permission-denied and unauthorized access cases.
- Webhook processing and retry behavior.
- Data minimization and public display controls.
- Support flow for user questions.
- Data rights request handling where provider data is involved.

Provider Review Evidence

CIC should maintain evidence commonly requested by production API providers:

- Privacy Policy.
- Terms of Service.
- Security policy and access control policy.
- Data retention and deletion policy.
- Incident response policy.
- Vendor and subprocessor register.
- Support policy.
- Screenshots of consent and user-facing flows.
- Test results for integration flows.
- Production credential control record.
- Contact details for security and support escalation.

Ongoing Monitoring

Production integrations should be monitored for:

- API errors.
- Webhook failures.
- Authentication or authorization failures.
- Unexpected data volume.
- Provider incidents or deprecations.
- User complaints.
- Support escalations.

- Security alerts.

Change Management

Material changes to financial API integrations require review before release, including changes to requested permissions, user consent text, data storage, webhook handling, public display, financial posting, or deletion behavior.

Evidence

Required evidence:

- Production access intake record
- Provider review evidence package
- Credential owner record
- Integration test results
- Consent flow screenshots
- Webhook validation evidence
- Data retention mapping
- Vendor review record
- Incident and support escalation records

Review

This policy must be reviewed at least annually and whenever CIC adds a new financial API provider or materially changes an existing integration.