Capital Investment Club

Acceptable Use and Personnel Security Policy

Personnel expectations, acceptable use, prohibited activity, training, and access safety.

Last updated: 02/07/2023

Purpose

This policy defines how CIC personnel, contractors, and authorized users must use CIC systems, devices, data, tools, and accounts.

Scope

This applies to CIC employees, contractors, administrators, support users, engineers, reviewers, finance operators, and anyone with authorized access to CIC systems or data.

Acceptable Use Requirements

Users must:

- Use CIC systems only for authorized business purposes.
- Protect account credentials.
- Use approved communication and storage systems for CIC work.
- Report suspected security incidents promptly.
- Avoid accessing customer or platform data without a business need.
- Avoid bypassing access controls or monitoring.
- Avoid storing CIC secrets, customer data, or restricted information in unapproved locations.

Prohibited Activities

Users must not:

- Share passwords or authentication tokens.
- Use shared accounts unless formally approved.
- Access user, organization, wallet, grant, pitch, assessment, KYC-adjacent, or support data out of curiosity.
- Exfiltrate CIC data.
- Disable security controls without approval.
- Commit secrets to repositories.
- Use unauthorized tools to process sensitive data.

- Perform unauthorized scanning, testing, or data extraction against production systems.

Personnel Security

Before granting access, CIC should confirm:

- Business need.
- Appropriate role.
- Required confidentiality obligation.
- Required training or acknowledgement.

Access must be removed promptly when personnel leave CIC or no longer need the access.

Workforce Risk Tiers

CIC should apply additional oversight based on the type of access.

Tier	Access type	Additional expectation
Standard	Internal business tools with no production or sensitive customer access	Policy acknowledgement and manager approval
Privileged	Admin, repository, cloud, support, production, or financial workflow access	Formal approval, role justification, periodic review
Restricted	Wallet, ledger, KYC-adjacent, incident, security, or highly sensitive support access	Heightened approval, need-to-know validation, additional monitoring where practical

Onboarding Requirements

Onboarding should include:

- Confidentiality obligation.
- Role-based access approval.
- Security and privacy policy acknowledgement.
- Acceptable use acknowledgement.
- Support data handling expectations where applicable.
- Secure development expectations for engineers.
- Financial data handling expectations for finance operators.

Access Grant Procedure

Access grants should record requester, user, system, role, business justification, approver, date granted, whether access is temporary, and review frequency. Privileged access should not be granted solely through informal chat approval unless the approval is copied into the official access record.

Offboarding Requirements

Offboarding should include:

- Disable identity provider access.
- Remove repository, cloud, admin, support, and vendor access.
- Recover or revoke devices, tokens, keys, and credentials.
- Transfer ownership of open tasks, support tickets, vendor relationships, and controls.
- Record completion evidence.

Transfer and Role Change Procedure

When personnel change role or responsibility, CIC should review whether existing access is still required. Access no longer needed must be removed, and new access must be approved before provisioning.

Device and Workspace Security

Personnel must protect work devices and workspaces. Devices used for CIC work should use reasonable protections such as screen lock, disk encryption where available, secure network use, and current security updates.

Device Baseline

Devices used for CIC work should meet the following baseline where practical:

- Unique user account.
- Screen lock enabled.
- Operating system updates applied.
- Disk encryption enabled where supported.
- Browser and password manager kept current.
- No shared storage of CIC secrets.
- Lost or stolen devices reported promptly.

Remote Work Expectations

Remote personnel must protect CIC information from unauthorized viewing or access, use secure networks, avoid sharing devices for CIC work where practical, and promptly report lost devices or suspected compromise.

AI and Automation Tool Use

Personnel may use AI or automation tools for CIC work only when the tool is approved for the data being processed. Restricted information, production secrets, private keys, customer identity documents, wallet data, and sensitive support files must not be placed into unapproved AI tools.

When AI tools are used for code, content, testing, or analysis, personnel remain responsible for validating accuracy, security, privacy, and production readiness.

Security Reporting

Personnel must promptly report suspected phishing, credential compromise, accidental data exposure, unauthorized access, lost devices, suspicious production behavior, and security control failures.

Training and Acknowledgement

Personnel with access to CIC systems must acknowledge relevant policies and receive security expectations during onboarding. Privileged users and support personnel should receive additional guidance.

Training should cover acceptable use, phishing awareness, data classification, support data handling, incident reporting, secure development expectations where relevant, and financial data handling where relevant.

Violations

Violations may lead to access removal, management escalation, contract review, disciplinary action, or legal action.

Monitoring and Privacy

CIC may monitor use of CIC systems, repositories, production environments, and support tools for security, compliance, quality, and operational purposes. Monitoring should be proportionate, business-relevant, and handled according to CIC privacy and data classification requirements.

Evidence

Required evidence:

- Policy acknowledgement records
- Onboarding access records
- Offboarding records
- Security training records
- Violation or exception records

Review

This policy must be reviewed at least annually.