Capital Investment Club

Incident Response Policy

Incident severity, triage, containment, investigation, communication, remediation, and post-incident review.

Last updated: 06/07/2026

Purpose

This policy defines how CIC prepares for, detects, triages, responds to, communicates about, remediates, and learns from security, privacy, operational, and availability incidents.

Scope

This applies to incidents affecting CIC applications, APIs, databases, wallets, grants, pitches, marketplace activity, support workflows, cloud systems, repositories, vendors, customer data, employee data, and production operations.

Objectives

CIC's incident response objectives are to:

- Protect users, organizations, CIC systems, and sensitive data.
- Contain security, privacy, financial, and availability impact quickly.
- Preserve evidence for investigation, audit, and legal review.
- Restore safe service operation.
- Communicate accurately and proportionately.
- Meet contractual, legal, provider, and customer obligations.
- Identify root cause and remediate control failures.
- Improve engineering, support, monitoring, and governance controls after material incidents.

Incident Response Roles

Incident Commander

Coordinates response, assigns owners, maintains timeline discipline, approves containment plan, and manages status updates.

Technical Lead

Investigates affected systems, proposes containment and remediation, validates recovery, and preserves technical evidence.

Communications Owner

Coordinates internal, customer, vendor, regulator, partner, and public communications where needed.

Legal or Privacy Owner

Assesses notification obligations, data impact, privacy impact, legal constraints, and evidence preservation needs.

Business Owner

Assesses user, financial, product, operational, and customer impact.

Scribe

Maintains the incident timeline, decisions, action owners, evidence references, and follow-up items.

Incident Categories

- Unauthorized access
- Suspected data disclosure
- Account takeover
- Fraud or abuse
- Wallet or transaction integrity issue
- Production outage
- Security vulnerability exploitation
- Lost or exposed secrets
- Vendor breach
- Privacy incident
- Misconfiguration
- Malware or endpoint compromise

Incident Intake Channels

Incidents may be reported through:

- Internal employee escalation.
- Support tickets.
- User reports.
- Vendor notification.
- Monitoring alerts.
- Repository or cloud security alerts.
- Financial reconciliation anomalies.
- Privacy request or complaint.
- Automated error tracking.

Severity Levels

Critical

Severe customer impact, confirmed sensitive data exposure, major financial impact, active compromise, major outage, or regulatory notification likely.

Examples include confirmed restricted data exposure, unauthorized production admin access, compromised production secrets, incorrect wallet/equity/grant financial outcomes at scale, destructive production change, major outage, or an incident likely to require urgent external notification.

High

Material customer impact, suspected sensitive data exposure, significant service degradation, or high-risk vulnerability actively exploited.

Examples include limited but serious data exposure, exploitable authorization defect, high-risk dependency exploit, vendor incident affecting CIC data, major workflow integrity defect, or serious production misconfiguration.

Medium

Limited customer impact, contained security issue, or operational issue with workaround.

Examples include suspicious activity without confirmed compromise, localized data handling error, moderate availability degradation, or a defect that could cause limited user confusion or incorrect display.

Low

Minor issue with limited impact and low risk.

Examples include low-risk alerts, blocked attacks, minor logging gaps, or issues handled through routine maintenance.

Response Time Targets

Response targets should be adjusted based on actual risk, but CIC should use this baseline:

- Critical: triage within 1 hour, containment plan within 4 hours, leadership update the same day.
- High: triage within 4 business hours, containment plan within 1 business day.
- Medium: triage within 2 business days.
- Low: triage through routine operational review.

If target timelines cannot be met, the incident commander must document the reason and interim risk treatment.

Response Lifecycle

1. Prepare

Maintain contacts, runbooks, communication templates, logging, monitoring, backup procedures, and tabletop exercises.

2. Detect

Sources include alerts, user reports, support reports, vendor notifications, monitoring, logs, audits, and internal

discovery.

3. Triage

Determine severity, affected systems, data impact, active threat, customer impact, and immediate containment needs.

Triage must identify affected systems, users, organizations, data classes, vendors, business workflows, financial records, and whether active exploitation or ongoing exposure is suspected.

4. Contain

Containment may include disabling accounts, rotating secrets, blocking traffic, disabling features, isolating systems, revoking tokens, or pausing risky workflows.

5. Investigate

Preserve relevant logs and evidence. Determine root cause, scope, timeline, affected users, affected data, and control gaps.

Investigation should use logs, deployment history, repository history, access records, monitoring data, screenshots, database records, support reports, vendor notices, user reports, and financial reconciliation data where relevant.

6. Remediate

Apply fixes, rotate credentials, patch systems, restore services, improve monitoring, and close control gaps.

Remediation must include validation that the issue is fixed in the affected environment and that adjacent workflows have not regressed.

7. Communicate

Communications must be accurate, timely, and approved by appropriate leadership. Legal review is required for potential customer, regulator, partner, or public communications.

8. Post-Incident Review

Document lessons learned, root cause, timeline, impact, remediation, control improvements, and follow-up owners.

Required Incident Record

- Incident ID
- Date/time detected
- Reporter
- Severity
- Systems affected
- Data affected
- Users affected
- Timeline

- Root cause
- Containment actions
- Remediation actions
- Communications
- Evidence
- Post-incident actions
- Closure approval

Notification

Potential legal, regulatory, customer, or partner notification must be escalated to leadership and legal counsel.

Notification decisions must be documented even when CIC determines notice is not required. Notices should be accurate, timely, and approved by the appropriate owner before being sent.

Notification Decision Factors

CIC should consider:

- Whether personal information, restricted data, or confidential organization data was accessed, acquired, disclosed, altered, or lost.
- Whether wallet, transaction, grant, pitch, equity, assessment, or ledger integrity was affected.
- Whether users need to take protective action.
- Whether law, contract, API-provider terms, or vendor terms require notice.
- Whether a regulator, platform provider, or law enforcement contact is needed.
- Whether public communications are necessary to preserve trust or reduce harm.

Communications Matrix

Incident communications should define:

- Internal incident commander.
- Technical lead.
- Customer support lead.
- Legal or privacy lead.
- Executive approver.
- Vendor contact where applicable.
- Customer or partner communication owner.

No external incident communication should be sent without approval from the incident commander and appropriate leadership.

Evidence Preservation

During an incident, CIC should preserve relevant logs, tickets, screenshots, configuration, deployment history, user reports, access records, transaction records, and communication history.

Evidence should be stored in an approved location with restricted access for sensitive incidents. Destructive cleanup should not occur before reasonable evidence preservation unless immediate containment requires it.

Containment Playbooks

CIC should maintain or be prepared to execute containment steps for:

- Compromised user or admin account.
- Compromised service account or API key.
- Exposed secret in repository, logs, or deployment.
- Authorization or organization-context data leak.
- Public profile privacy incident.
- Wallet, grant, equity, or transaction integrity incident.
- File upload or document exposure.
- Vendor incident.
- Production outage or failed deployment.
- Malicious or abusive user-generated content.

Post-Incident Corrective Actions

Post-incident actions should be tracked in the remediation tracker and assigned owners, severity, due dates, and closure evidence.

Corrective actions should address root cause, detection gaps, prevention gaps, documentation gaps, test gaps, and owner accountability. High and critical incidents require management review before closure.

Tabletop Exercises

CIC should perform at least one incident response tabletop annually.

Exercise scenarios should include at least one security/data incident and one financial or platform integrity incident relevant to CIC's operating model.

Post-Incident Review Requirements

High and critical incidents require a post-incident review covering:

- What happened.
- Timeline.
- Root cause.
- Detection effectiveness.
- User/customer impact.
- Data or financial impact.
- What worked.
- What failed.
- Corrective actions.

- Control updates.
- Evidence retained.
- Closure approval.

Evidence

Required evidence:

- Incident register
- Incident tickets
- Communications
- Root cause analysis
- Remediation evidence
- Tabletop records
- Post-incident review
- Notification decision record
- Containment evidence
- Closure validation

Review

This policy must be reviewed at least annually and after major incidents.