SAMPLE RESPONSE RUNBOOK

High Withdrawal Velocity

Public example of a versioned operational runbook for validation, routing, decision capture, and escalation.

RUNBOOK
OCO-RB-001
VERSION 1.0
PUBLIC TEMPLATE

> Template boundary
> This is not protocol-specific advice or authorization to pause, sign, transfer, disclose, or change production systems. A real runbook must name actual owners, authority, tools, thresholds, secure channels, and legal requirements.

1. Purpose and trigger

Use this runbook when a trusted monitor identifies withdrawal velocity, concentration, or net outflow materially above the protocol's documented baseline. A monitor event starts validation; it does not prove an exploit.

Trigger input	Required record	Do not assume
Alert ID, source, time, severity, affected asset	Original payload, normalized incident record, evidence link	That the alert is correct, malicious, or protocol-wide
Change versus baseline	Window, amount, counterparties, transaction hashes	That every unusual withdrawal has the same cause

2. Named roles

- Triage owner - validates the signal and opens the incident record.
- Protocol decision owner - owns production-state decisions within documented authority.
- Security owner - assesses exploit indicators and coordinates existing security partners.
- Communications owner - prepares approved internal and external communication.
- Scribe - records facts, hypotheses, decisions, evidence, timestamps, and unresolved questions.

3. First ten minutes

1. Record the alert without editing the original payload.
2. Validate transaction, block, contract, and amount against an independent RPC or explorer.
3. Check for a known migration, rebalance, liquidation, market event, or approved action.
4. Identify affected assets and dependencies; separate verified facts from hypotheses.
5. Notify primary triage and protocol decision owners through the documented secure channel.
6. Open the incident timeline and record acknowledgement times.

4. Severity decision

State	Example evidence	Operating response
EXPECTED	Approved transaction, known migration, or documented market behavior	Close with evidence and tune the monitor if needed
INVESTIGATE	Confirmed movement, unclear cause, no exploit indicator yet	Engage owners and increase observation
CRITICAL	Unauthorized control change, invariant break, exploit trace, or continuing loss	Activate the separately approved critical-incident procedure

5. Decision record

For every material decision, capture:

- time and named decision owner;
- verified facts available at that time;
- known unknowns and competing hypotheses;
- options considered and authority required;
- decision, rationale, expected consequence, and review time;
- evidence links and communication approvals.

6. Escalation and outside resources

Use the protocol's current escalation matrix. Contact audit, monitoring, legal, insurance, emergency-response, exchange, custodian, and law-enforcement partners only through pre-approved channels and named authority. Do not disclose sensitive details in unverified direct messages.

7. Closure criteria

- The signal is explained or transferred into a protocol-specific critical-incident process.
- All material facts and decisions have evidence links and owners.
- Required communications were approved and recorded.
- Open remediation items have owners and due dates.
- The alert rule and runbook receive a documented post-event review.

8. Test record

A production runbook should record the last tabletop or routing test, participants, acknowledgement times, failed steps, remediations, approver, and next review date.

Build a protocol-specific version
Start at https://onchainoncall.com/start/ or explore the workspace at https://onchainoncall.com/demo/.