

## Contents

<b>SOUTHGATE TERMINAL</b>	<b>1</b>
<b>## Port Operations Security Documentation</b>	<b>1</b>
<b>Crisis and Incident Management – Incident Log Closure Protocol</b>	<b>1</b>
Required When:	1
Closure Checklist	1
Final Log Contents Should Include:	2
Debrief Use	3
Reminder:	3

## SOUTHGATE TERMINAL

### ## Port Operations Security Documentation

### Crisis and Incident Management – Incident Log Closure Protocol

#### Purpose:

To ensure all incident-related activity is formally logged, tagged, and closed in a way that supports audit, debrief, legal, and insurer requirements. This protocol applies to the Incident Coordinator and team leads as the crisis response winds down.

#### Required When:

Use this protocol when:

- The incident is being de-escalated (as confirmed by the Executive or Crisis Lead)
- The final 15–30 minutes of the response window has been reached
- Final outputs (media, legal, insurer, ops) are being prepared

#### Closure Checklist

##### 1. Final Log Review & Tagging

- Review full inject list and timeline
- Ensure each inject is tagged with:
  - Time received
  - Team(s) impacted
  - Action(s) taken
  - Decision point (if applicable)

- Tag all major actions/decisions with final timestamps
- Highlight unresolved or delayed responses (for scoring)

## **2. Cross-Check with Teams**

- Coordinate with Tech, Legal, Ops, Media, and CEO:
- Confirm each has logged their major actions and responses
- Identify any “silent” or undocumented activity
- Capture cross-role communications (e.g. joint decisions, escalations)

## **3. Format Log for Export**

- Ensure the master log is readable and structured:
- Sort by timestamp
- Group by phase (e.g. T+0 to T+30)
- Use standard format: [Timestamp] [Team] [Action] [Outcome]
- Save as:
- Internal archive version (.xlsx or .csv)
- Briefing version (.pdf for Board, Debrief, and Insurance)

## **4. Flag Key Learning Moments**

- Identify entries where:
- Teams took proactive or creative action
- Escalation was delayed or debated
- Policy conflicts or constraints arose
- Role confusion or comms breakdowns occurred
- Tag these for the debrief summary

## **Final Log Contents Should Include:**

- Inject responses (time, action, outcome)
- Decision records (formal and informal)
- Major communications (internal and external)
- Cross-role handoffs or miscommunications
- System state transitions (e.g. isolation, containment, restore)

## **Debrief Use**

The final log will be used to:

- Support the internal post-incident review process
- Identify opportunities for improvement in incident detection, escalation, and response
- Inform legal or regulatory reporting where applicable
- Preserve an evidence trail to support policy and operational reform

## **Reminder:**

Logs that are incomplete, disorganised, or missing timestamps reduce learning value and undermine the incident response narrative.

**Owner:** Incident Coordinator

**Reference:** CIM-03

**Version:** 1.0

**Approved by:** Workshop Planning Team