# SOUTHGATE TERMINAL

## Port Operations Security Documentation

# Crisis and Incident Management – Incident Reporting Guide (Technical)

# Purpose:

To guide technical teams through the accurate and timely reporting of anomalies, indicators of compromise, system degradations, or cyber-physical disruptions during an active incident. This guide ensures reports are usable for operational decision-making, post-incident review, and legal/regulatory requirements.

## Who Should Use This Guide:

- Technical or Cybersecurity Team Leads
- · On-call engineers or analysts assigned during the incident
- Any team member investigating log data, system health, or dashboard anomalies

## When to Report

An incident report should be submitted if any of the following are observed:

- System anomalies affecting operations (e.g. container scheduler manipulation, AIS signal loss)
- Security-related indicators (e.g. spoofing, jamming, unauthorised access, persistence mechanisms)
- · Service degradation (e.g. communication latency, system unavailability)
- · Evidence of tampering or configuration changes
- · Log data suggesting policy breach, intrusion, or suspicious patterns

## What to Include in a Technical Incident Report

Each report should be concise but comprehensive. Use the following structure:

- 1. Summary
  - What was observed?
  - When and where (system/VM)?
  - · Is it still active or resolved?

## 2. Detection Method

- How was it discovered? (e.g. dashboard alert, log scan, external report)
- · Time of first indication

#### 3. Technical Detail

- Relevant log entries (include timestamped lines)
- · Affected systems, services, or ports
- · Any actions taken to isolate or mitigate
- · Whether escalation to other teams has occurred

#### 4. Assessment

- Confidence level: Confirmed / Suspected / Needs Further Investigation
- Severity: Low / Moderate / High / Critical
- · Potential business or safety impact

# 5. Supporting Artefacts

- File paths (e.g. /var/log/sim/container\_sched.log)
- · Dashboard screenshots (if applicable)
- Extracted indicators (e.g. IPs, timestamps, anomaly signatures)

### Where to Submit

- Upload or send report to the shared incident log system or Coordinator
- Notify Legal if indicators suggest potential breach
- · Notify Ops if physical systems are impacted
- Confirm upload via Slack/email to Incident Coordination Channel (or designated comms system)

# Format Template (Recommended)

Title: [Brief Issue Title]

Reported By: [Your Name / Team]

Date/Time: [DD/MM/YYYY HH:MM]

System/VM Affected: [e.g. VM-RF, VM-ContainerCtrl]

Summary:

[2-3 sentences describing the issue]

Detection:

[Describe how it was found, with times]

Log Evidence:

[Paste relevant entries here]

Impact Assessment:

[Risk/Severity, Current Status, Confidence Level]

Actions Taken:

[What has been done so far]

Recommendations:

[Next steps or actions required]

# Reminder:

All technical reports should be timestamped, factual, and as objective as possible. Speculation should be clearly labelled as such. Include context, but avoid unnecessary narrative.

Owner: Technical Team Lead

Reference: CIM-04

Version: 1.0

Approved by: Workshop Planning Team