SOUTHGATE TERMINAL

Port Operations Security Documentation

Document Navigation Guide

Document Information

Purpose: Help teams quickly find the right documents for their situations Usage: Reference when you need detailed procedures beyond quick reference cards Companion to: QUICK_REFERENCE_CARDS.md (use cards first, then find detailed docs here)

TECHNICAL TEAM DOCUMENT NAVIGATOR

CRITICAL - Use Immediately

When systems are down or under active attack: - `VM_Specific_Investigation_Procedures.md` - Step-by-step VM analysis with trap warnings - `Evidence_Transfer_Chain_of_Custody.md` - Legal evidence preservation requirements - `Multi_System_Failure_Coordination_Guide.md` - Coordinating across multiple compromised systems

HIGH PRIORITY - Use Within 15 Minutes

For investigation and containment: - `Log_Deletion_Investigation.md` - Finding and analysing deleted log evidence - `AIS_Signal_Validation.md` - Verifying GPS/AIS system integrity - `CCTV_Blackout_Response.md` - Technical recovery procedures for camera systems - `Network_Diagnostics_SOP.md` - Network analysis and isolation procedures - `Service_Account_Authentication_Response.md` - Service account failure investigation

REFERENCE - Use When Time Permits

For comprehensive procedures: - `Technical Containment Guide.md` - Full system isolation and containment - `Node Isolation Procedure.md` - Network node isolation procedures - `Authentication_Failure_Response_SOP.md` - Authentication system troubleshooting - `Manual_Override_Authorisation.md` - Manual system override procedures - `Forensics Summary Template.md` - Evidence documentation templates

REPORTING - Use for Documentation

For reports and handoffs: - `Ops After-Action Checklist.md` - Post-incident technical analysis - `Access Control Summary.md` - Access control review procedures - `Downtime Impact Estimator.md` - Calculating system impact metrics

---

OPERATIONS TEAM DOCUMENT NAVIGATOR

SAFETY CRITICAL - Use Immediately

When safety systems are compromised: - `Container_Operations_Emergency_Procedures.md` - Safe container handling during incidents - `Multi_Berth_Emergency_Shutdown_Procedures.md` - Multi-terminal shutdown protocols - `Emergency_Response_Procedures.md` - General emergency response coordination

OPERATIONAL PRIORITY - Use Within 10 Minutes

For maintaining operations: - `CCTV_Blackout_Response.md` - Manual spotting and safety procedures - `Manual Ops SOP.md` - Manual operation procedures when systems down - `Authentication_Failure_Response_SOP.md` - Manual authorisation procedures - `Manual_Override_Authorisation.md` - Override procedures and documentation

COORDINATION - Use for Planning

For incident coordination: - `Multi_System_Failure_Coordination_Guide.md` - Cross-team coordination procedures - `Resource_Prioritization_and_Conflict_Resolution_Process.md` - Resource allocation during incidents - `Workforce_Safety_Communication_Protocol.md` - Crew communication during incidents

ASSESSMENT - Use for Analysis

For impact assessment: - `Downtime Impact Estimator.md` - Calculating operational impact - `Safety_Risk_Assessment_Template.md` - Risk assessment procedures - `Ops Closure Procedure (Part B).md` - Operations closure procedures

---

LEGAL TEAM DOCUMENT NAVIGATOR

TIME CRITICAL - Use Immediately

For regulatory deadlines: - `Breach_Classification_Decision_Tree.md` - Quick breach classification - `Regulatory_Timeline_Compliance.md` - Notification deadline tracker - `Legal Risk Escalation Flowchart.md` - Escalation decision matrix

COMPLIANCE PRIORITY - Use Within 2 Hours

For notifications and compliance: - `Breach Disclosure Checklist.md` - Step-by-step notification procedures - `Insurance_Clause_Interpretation.md` - Insurance coverage analysis - `Vendor_Incident_Coordination_Protocol.md` - Third-party vendor coordination

REFERENCE - Use for Guidance

For legal strategy: - `Legal Precedent Summary Sheet.md` - Legal precedent reference - `Post-Breach Reform Guidance.md` - Post-incident reform procedures - `Evidence_Transfer_Chain_of_Custody.md` - Legal evidence requirements

TEMPLATES - Use for Documentation

For legal communications: - `Insurance Communications Template.md` - Insurance notification templates - `Crisis_Communications_SOP.md` - Legal-approved communication procedures

---

MEDIA TEAM DOCUMENT NAVIGATOR

IMMEDIATE RESPONSE - Use Within 5 Minutes

For immediate media pressure: - `Rapid_Response_Media_Protocol.md` - Fast response procedures - `Internal_Information_Leak_Response.md` - Handling information leaks - `Final_Media_Deadline_Management.md` - TV crew and urgent deadline management

COMMUNICATION PRIORITY - Use Within 15 Minutes

For structured communication: - `Crisis Communications SOP.md` - Comprehensive crisis communication - `CEO Comms Briefing Template.md` - Executive

briefing procedures - `Public Messaging Templates.md` - Pre-approved message templates

COORDINATION - Use for Planning

For stakeholder coordination: - `Media SOP- Final Response.md` - Final statement procedures - `Comms Summary Template.md` - Communication summary procedures

---

EXECUTIVE TEAM DOCUMENT NAVIGATOR

STRATEGIC DECISIONS - Use Immediately

For critical business decisions: - `Crisis_Decision_Authority_Matrix.md` - Decision authority reference - `Executive Crisis Wrap Guide.md` - Executive crisis management - `Crisis Escalation Tree.md` - Escalation decision framework

COORDINATION PRIORITY - Use Within 15 Minutes

For team coordination: - `Executive_Briefing_Template_and_Schedule.md` - Team briefing procedures - `Resource_Prioritization_and_Conflict_Resolution_Process.md` - Resource allocation decisions - `Multi_System_Failure_Coordination_Guide.md` - Cross-team coordination oversight

GOVERNANCE - Use for Oversight

For organisational governance: - `Safety_Risk_Assessment_Template.md` - Risk assessment oversight - `Crisis_De_escalation_Criteria_and_Process.md` - De-escalation decision criteria - `Inter_Team_Communication_Protocol.md` - Communication governance

---

INCIDENT COORDINATOR DOCUMENT NAVIGATOR

COORDINATION CRITICAL - Use Immediately

For incident coordination: - `Inter_Team_Communication_Protocol.md` - Team coordination procedures - `Resource_Prioritization_and_Conflict_Resolution_Process.md`

- Conflict resolution - `Multi_System_Failure_Coordination_Guide.md` - Multi-team coordination

PROCESS PRIORITY - Use Within 10 Minutes

For incident management: - `Crisis Escalation Tree.md` - Escalation procedures - `Incident Reporting Guide (Technical).md` - Incident documentation - `Executive_Briefing_Template_and_Schedule.md` - Executive coordination

CLOSURE - Use for Incident Wrap-up

For incident closure: - `Incident Log Closure Protocol.md` - Incident closure procedures - `Crisis_De_escalation_Criteria_and_Process.md` - De-escalation procedures - `Workforce_Safety_Communication_Protocol.md` - Team debriefing

---

DOCUMENT PRIORITY LEGEND

CRITICAL (Use Immediately - 0-5 minutes)

- Purpose: Life safety, regulatory deadlines, active threats
- Characteristics: Short, actionable, decision-focused
- Usage: Print and keep readily accessible

HIGH PRIORITY (Use Within 15 minutes)

- Purpose: Investigation, containment, immediate response
- Characteristics: Procedural, step-by-step, time-sensitive
- Usage: Reference when implementing quick reference card actions

REFERENCE (Use When Time Permits)

- Purpose: Comprehensive procedures, detailed guidance
- Characteristics: Complete procedures, background information
- Usage: Follow for thorough implementation after immediate response

TEMPLATES & REPORTING (Use for Documentation)

- Purpose: Documentation, reporting, evidence preservation
- Characteristics: Forms, templates, checklists
- Usage: Ensure proper documentation and evidence handling

QUICK SELECTION GUIDE

"I Need To…" Quick Finder

"I need to preserve evidence"

- `Evidence_Transfer_Chain_of_Custody.md`

"I need to check for malware/traps"

- `VM_Specific_Investigation_Procedures.md`

"I need to shut down operations safely"

- `Container_Operations_Emergency_Procedures.md`

"I need to notify regulators"

- `Breach_Classification_Decision_Tree.md` - `Regulatory_Timeline_Compliance.md`

"I need to respond to media"

- `Rapid_Response_Media_Protocol.md`

"I need to coordinate multiple teams"

- `Multi_System_Failure_Coordination_Guide.md`

"I need to brief executives"

- `Executive_Briefing_Template_and_Schedule.md`

I need to handle CCTV blackout"

- `CCTV_Blackout_Response.md` (both technical and operational sections)

"I need to investigate authentication failures"

- `Service_Account_Authentication_Response.md`

"I need to calculate incident impact"

- `Downtime Impact Estimator.md`

INTEGRATION WITH QUICK REFERENCE CARDS

How This Guide Works With Quick Reference Cards

1. Start with Quick Reference Cards (`QUICK_REFERENCE_CARDS.md`)

- Use cards for immediate 0-30 minute response
- Cards tell you WHAT to do quickly

2. Then Use This Navigation Guide

- Find detailed procedures for HOW to do it thoroughly
- Get comprehensive guidance for complex situations

3. Document References

- Quick Reference Cards - Immediate action
- This Guide - Detailed procedures
- Individual Documents - Complete instructions

Example Usage Flow

Scenario: CCTV Blackout Detected

1. Use Card O1: CCTV Blackout Response (Quick Reference)

- Deploy manual spotters (0-5 min)
- Slow crane operations (immediate)
- Establish radio contact (immediate)

2. Then Use This Guide (Operations Team Navigator)

- Find `CCTV_Blackout_Response.md` under "OPERATIONAL PRIORITY"
- Follow detailed manual procedures
- Coordinate with technical team using full procedures

3. Cross-Team Coordination

- Technical team uses `CCTV_Blackout_Response.md` (technical sections)
- Incident Coordinator uses `Multi_System_Failure_Coordination_Guide.md`
- Executive team briefs using `Executive_Briefing_Template_and_Schedule.md`

Owner: All Teams Reference: DNG-01 Version: 1.0 Approved by: Cyber-Ops Coordination Cell Companion Document: QUICK_REFERENCE_CARDS.md