

SOUTHGATE TERMINAL

Port Operations Security Documentation

Quick Reference Action Cards

Document Information

Purpose: Rapid reference cards for time-critical scenarios **Usage:** Keep accessible during incidents for quick decision-making **Format:** Print and cut into individual cards for team reference

TECHNICAL TEAM QUICK REFERENCE CARDS

CARD T1: SYSTEM ANOMALY INVESTIGATION

WHEN: Unusual system behaviour, authentication failures, network issues

IMMEDIATE (0-5 min): - [] Preserve evidence FIRST (hash all logs) - [] Assign team members to different systems - [] Start with highest risk systems first

INVESTIGATION (5-25 min): - [] Check vm-gateway for trap scripts (DO NOT EXECUTE) - [] Look for unauthorised cron jobs in /etc/cron.d/ - [] Document but don't run scripts in /opt/security/, /home/

HANDOFF (25-30 min): - [] Package evidence with hashes for vm-audit - [] Brief incident coordinator on findings - [] Report trap scripts found to all teams

DANGER SIGNS: restore_feed.sh, remove_malware.sh, temp_session=true
KEY PRINCIPLE: When in doubt, preserve evidence and avoid execution

CARD T2: MULTI-SYSTEM FAILURE

WHEN: Multiple systems failing, coordinated issues, evidence of attack

DIVIDE & CONQUER (0-5 min): - [] Assign one VM per team member - [] Start evidence preservation immediately - [] Coordinate with ops on system isolation decisions

INVESTIGATION PRIORITY: 1. vm-gateway (evidence destruction risk)
2. vm-coretech (GPS/AIS systems) 3. vm-opsnode (CCTV/safety systems)

CRITICAL COORDINATION: - ☐ Check with ops before isolating Node-04
- ☐ Report service account failures immediately - ☐ Document timeline for legal team

OUTPUTS NEEDED: Evidence package, trap script warnings, system correlation analysis

OPERATIONS TEAM QUICK REFERENCE CARDS

CARD 01: CCTV BLACKOUT RESPONSE

WHEN: Camera feeds black, frozen, or showing static

IMMEDIATE SAFETY (0-5 min): - ☐ Deploy manual spotters to blind zones - ☐ Slow all crane operations to 50% speed - ☐ Establish radio contact with all operators - ☐ Clear personnel from automated operation zones

MANUAL PROCEDURES (5-20 min): - ☐ Implement spotter network per CCTV procedures - ☐ Brief crew on manual safety protocols - ☐ Calculate reduced operational capacity - ☐ Coordinate with technical team on restoration

DECISION POINTS: - Can safety be maintained with manual procedures?
- Are adequate personnel available for spotting? - Is crew comfortable with manual operations?

ESCALATION TRIGGER: If safety cannot be ensured with available procedures

CARD 02: AUTHENTICATION SYSTEM FAILURE

WHEN: Service accounts failing, automated systems not responding

SAFETY FIRST (0-2 min): - ☐ Complete any active container movements safely - ☐ Switch affected systems to manual control - ☐ Alert all operators to authentication issues

MANUAL OVERRIDE (2-15 min): - ☐ Implement manual authorisation procedures - ☐ Use alternative verification methods - ☐ Enhanced spotting for crane operations - ☐ Document all manual overrides

COORDINATION: - ☐ Work with technical team on service account recovery - ☐ Brief executive team if operations halt needed - ☐ Monitor crew stress and confidence levels

KEY PRINCIPLE: Safety over efficiency - don't rush manual procedures

LEGAL TEAM QUICK REFERENCE CARDS

CARD L1: CYBER INCIDENT ESCALATION

WHEN: Evidence of unauthorised access, system compromise, data breach

IMMEDIATE ASSESSMENT (0-10 min): - ☐ Criminal activity suspected?
- Escalate to executive immediately - ☐ Safety systems compromised? - Priority regulatory review - ☐ Data breach indicators? - Start breach classification - ☐ Multiple systems affected? - Consider major incident protocols

NOTIFICATION DECISION TREE: - Personal data affected? - GDPR/privacy law notifications - Safety systems down? - Maritime authority notifications - Criminal activity? - Law enforcement coordination - Insurance claims likely? - Insurer notifications

EVIDENCE COORDINATION: - ☐ Implement legal hold for investigation evidence - ☐ Coordinate with technical team on evidence preservation - ☐ Protect attorney-client privilege in documentation

TIME-CRITICAL DECISIONS: Breach notifications, law enforcement contact, regulatory reporting

CARD L2: REGULATORY COMPLIANCE CRISIS

WHEN: Multiple notification deadlines, regulatory violations, compliance gaps

PRIORITY MATRIX (0-5 min): 1. Safety-related notifications (immediate)
2. Criminal activity reports (2 hours) 3. Data breach notifications (24-72 hours)
4. Insurance notifications (24 hours)

RAPID RESPONSE: - ☐ Use breach classification decision tree - ☐ Draft notifications using templates - ☐ Coordinate language with technical/ops teams - ☐ Get executive approval for formal notifications

COORDINATION POINTS: - Technical team: Evidence and technical details - Executive team: Strategic decisions and approvals - Media team: Public communication coordination

PRINCIPLE: Regulatory compliance deadlines take priority over perfect language

MEDIA TEAM QUICK REFERENCE CARDS

CARD M1: IMMEDIATE MEDIA PRESSURE

WHEN: Media calls, social media posts, external visibility of incident

5-MINUTE RESPONSE: - ☐ Use holding statement template: “Aware of [issue], investigating, safety priority” - ☐ Coordinate with legal team on language approval - ☐ Monitor social media for spread and sentiment - ☐ Alert executive team to media interest

15-MINUTE SETUP: - ☐ Assess severity and likely media interest - ☐ Prepare expanded statement if needed - ☐ Set up social media monitoring - ☐ Coordinate with incident coordinator on messaging

DECISION MATRIX: - Anonymous posts? - Monitor, don’t engage directly - Media requests? - Prepared statement or brief interview - TV crew on-site? - Activate Final Media Deadline procedures - Factual errors spreading? - Prepare corrective statement

KEY PRINCIPLE: Better to provide accurate information than let speculation spread

CARD M2: SOCIAL MEDIA CRISIS

WHEN: Anonymous posts, trending hashtags, viral misinformation about incident

IMMEDIATE MONITORING (0-5 min): - ☐ Screenshot and document all posts - ☐ Track hashtags and sentiment - ☐ Identify if posts contain internal information - ☐ Alert legal team if internal leaks suspected

RESPONSE STRATEGY: - ☐ Don’t engage directly with anonymous posts - ☐ Prepare factual counter-narrative if misinformation spreading - ☐ Coordinate with HR if employee posts identified - ☐ Use official channels for authoritative information

ESCALATION TRIGGERS: - Posts going viral with significant inaccuracies - Internal information being leaked - Safety concerns being raised publicly - Media picking up social media narrative

OUTPUTS: Social media monitoring report, recommended response actions, stakeholder alerts

EXECUTIVE TEAM QUICK REFERENCE CARDS

CARD E1: OPERATIONS HALT DECISION

WHEN: Safety concerns, multiple system failures, crew refusing to work

30-SECOND DECISION FRAMEWORK: - **HALT if:** Cannot ensure safety, crew unsafe, regulatory requirement - **CONTINUE if:** Manual procedures adequate, crew confident, safety verified - **REDUCE if:** Partial capability, enhanced procedures needed

INFORMATION NEEDED: - ☐ Operations team safety assessment - ☐ Technical team system status - ☐ Legal team compliance requirements - ☐ Media team external visibility

COMMUNICATION: - ☐ Brief board if operations halted - ☐ Coordinate stakeholder messaging - ☐ Support team decisions publicly - ☐ Prepare for media questions

KEY PRINCIPLE: Support operational team decisions while ensuring proper oversight

CARD E2: CRISIS ESCALATION DECISIONS

WHEN: Major incident, regulatory investigations, board involvement needed

STRATEGIC DECISIONS NEEDED: - ☐ External assistance (cyber forensics, crisis consultants) - ☐ Stakeholder communication level (customers, partners, board) - ☐ Legal strategy (defensive vs. transparent) - ☐ Business continuity priorities

COORDINATION REQUIREMENTS: - ☐ Legal team: Approve major legal positions - ☐ Media team: Approve public statements - ☐ Technical team: Resource prioritisation decisions - ☐ Operations team: Business continuity support

ESCALATION TRIGGERS: - Multiple system compromise confirmed - Regulatory investigation likely - Major customer/partner impact - Significant media attention

OUTPUTS: Strategic direction, resource authorisation, stakeholder communication approval

INCIDENT COORDINATOR QUICK REFERENCE CARDS

CARD IC1: MULTI-TEAM COORDINATION

WHEN: Multiple teams active, resource conflicts, complex incident

COORDINATION SETUP (0-5 min): - ☐ Assign communication lead for each team - ☐ Establish 15-minute update cycle - ☐ Set up central documentation location - ☐ Identify resource conflict potential

PRIORITY MATRIX: 1. Safety and regulatory compliance 2. Evidence preservation and investigation 3. Operational continuity 4. Stakeholder communication

TEAM COORDINATION: - ☐ Technical + Operations: System isolation decisions - ☐ Legal + Media: Communication approval - ☐ Executive + All: Resource authorisation - ☐ All teams: Information sharing

CONFLICT RESOLUTION: When teams have competing priorities, apply priority matrix and escalate to executive if needed

CARD IC2: EXTERNAL PRESSURE MANAGEMENT

WHEN: Regulatory deadlines, media pressure, insurer demands, executive escalation

PRESSURE POINT MANAGEMENT: - ☐ Map all external deadlines and requirements - ☐ Coordinate team priorities against deadlines - ☐ Escalate conflicts to executive team - ☐ Maintain communication with external parties

RESOURCE ALLOCATION: - Technical team: Investigation vs. restoration balance - Legal team: Compliance vs. strategic advice - Media team: External vs. internal communication - Operations team: Safety vs. capacity

ESCALATION CRITERIA: - Competing regulatory deadlines - Resource shortfalls for critical tasks - Team disagreement on priorities - External pressure exceeding team capability

KEY PRINCIPLE: Coordinate rather than control - teams are experts in their domains

USAGE INSTRUCTIONS FOR CARDS

Card Distribution:

- Each team gets their relevant cards

- Incident Coordinator gets all cards for reference
- Print on cardstock for durability
- Laminate for repeated use

When to Use Cards:

- **Time pressure situations** (less than 30 minutes to respond)
- **Multiple simultaneous issues** requiring quick prioritisation
- **New team members** who need quick reference
- **High-stress situations** where detailed procedures might be overwhelming

Card Maintenance:

- Update cards when procedures change
- Test card effectiveness during drills
- Gather feedback from teams on card usefulness
- Add new cards for scenarios not covered

Integration with Full Procedures:

- Cards supplement, don't replace, full procedures
- Use cards for immediate response, full procedures for comprehensive action
- Reference full procedures when time permits for complete guidance
- Use cards to identify which full procedures to follow

Owner: All Teams **Reference:** QRC-01 **Version:** 1.0 **Approved by:** Cyber-Ops Coordination Cell