

Contents

SOUTHGATE TERMINAL	3
Quick Reference Action Cards	3
Print on cardstock, cut along page breaks for individual cards	3
□ SYSTEM ANOMALY INVESTIGATION	4
TECHNICAL TEAM CARD T1	4
□ WHEN TO USE	4
□ IMMEDIATE ACTIONS (0-5 minutes)	4
□ INVESTIGATION PHASE (5-25 minutes)	4
□ HANDOFF PHASE (25-30 minutes)	4
□ KEY PRINCIPLE	4
□ MULTI-SYSTEM FAILURE	5
TECHNICAL TEAM CARD T2	5
□ WHEN TO USE	5
□ DIVIDE & CONQUER (0-5 minutes)	5
□ INVESTIGATION PRIORITY ORDER	5
□ CRITICAL COORDINATION	5
□ OUTPUTS REQUIRED	5
□ CCTV BLACKOUT RESPONSE	6
OPERATIONS TEAM CARD O1	6
□ WHEN TO USE	6
□ IMMEDIATE SAFETY (0-5 minutes)	6
□ MANUAL PROCEDURES (5-20 minutes)	6
□ DECISION CHECKLIST	6
□ ESCALATION TRIGGER	6
□ AUTHENTICATION SYSTEM FAILURE	7
OPERATIONS TEAM CARD O2	7
□ WHEN TO USE	7
□ SAFETY FIRST (0-2 minutes)	7
□ MANUAL OVERRIDE (2-15 minutes)	7
□ COORDINATION ACTIONS	7
□ KEY PRINCIPLE	7
□ CYBER INCIDENT ESCALATION	8
LEGAL TEAM CARD L1	8
□ WHEN TO USE	8
□ IMMEDIATE ASSESSMENT (0-10 minutes)	8
□ NOTIFICATION DECISION TREE	8
□ EVIDENCE COORDINATION	8
□ TIME-CRITICAL DECISIONS	8
□ REGULATORY COMPLIANCE CRISIS	9
LEGAL TEAM CARD L2	9
□ WHEN TO USE	9
□ PRIORITY MATRIX (0-5 minutes)	9
□ RAPID RESPONSE ACTIONS	9
□ COORDINATION POINTS	9
□ KEY PRINCIPLE	9

IMMEDIATE MEDIA PRESSURE	10
MEDIA TEAM CARD M1	10
WHEN TO USE	10
5-MINUTE RESPONSE	10
15-MINUTE SETUP	10
DECISION MATRIX	10
KEY PRINCIPLE	10
SOCIAL MEDIA CRISIS	11
MEDIA TEAM CARD M2	11
WHEN TO USE	11
IMMEDIATE MONITORING (0-5 minutes)	11
RESPONSE STRATEGY	11
ESCALATION TRIGGERS	11
REQUIRED OUTPUTS	11
OPERATIONS HALT DECISION	12
EXECUTIVE TEAM CARD E1	12
WHEN TO USE	12
30-SECOND DECISION FRAMEWORK	12
INFORMATION NEEDED	12
COMMUNICATION ACTIONS	12
KEY PRINCIPLE	12
CRISIS ESCALATION DECISIONS	13
EXECUTIVE TEAM CARD E2	13
WHEN TO USE	13
STRATEGIC DECISIONS NEEDED	13
COORDINATION REQUIREMENTS	13
ESCALATION TRIGGERS	13
REQUIRED OUTPUTS	13
MULTI-TEAM COORDINATION	14
INCIDENT COORDINATOR CARD IC1	14
WHEN TO USE	14
COORDINATION SETUP (0-5 minutes)	14
PRIORITY MATRIX	14
TEAM COORDINATION	14
CONFLICT RESOLUTION	14
EXTERNAL PRESSURE MANAGEMENT	15
INCIDENT COORDINATOR CARD IC2	15
WHEN TO USE	15
PRESSURE POINT MANAGEMENT	15
RESOURCE ALLOCATION BALANCE	15
ESCALATION CRITERIA	15
KEY PRINCIPLE	15
USAGE INSTRUCTIONS FOR CARDS	16
CARD DISTRIBUTION	16
WHEN TO USE CARDS	16
CARD MAINTENANCE	16
INTEGRATION WITH FULL PROCEDURES	16

SOUTHGATE TERMINAL

Quick Reference Action Cards

Print on cardstock, cut along page breaks for individual cards

❑ SYSTEM ANOMALY INVESTIGATION

TECHNICAL TEAM | CARD T1

❑ WHEN TO USE

Unusual system behaviour • Authentication failures • Network issues

❑ IMMEDIATE ACTIONS (0-5 minutes)

1. PRESERVE EVIDENCE FIRST
 - Hash all logs before investigation
2. DIVIDE THE TEAM
 - Assign one person per affected system
3. PRIORITIZE HIGH-RISK SYSTEMS
 - Start with vm-gateway, vm-coretech first

❑ INVESTIGATION PHASE (5-25 minutes)

CHECK FOR TRAPS:

- ❑ vm-gateway for trap scripts (DO NOT EXECUTE!)
- ❑ Unauthorised cron jobs in /etc/cron.d/
- ❑ Scripts in /opt/security/ or /home/ (DOCUMENT ONLY)

DANGER SCRIPTS TO WATCH FOR:

- ❑ restore_feed.sh
- ❑ remove_malware.sh
- ❑ temp_session=true

❑ HANDOFF PHASE (25-30 minutes)

- ❑ Package evidence with hashes for vm-audit
- ❑ Brief incident coordinator on findings
- ❑ Report any trap scripts found to ALL teams

❑ KEY PRINCIPLE

When in doubt: PRESERVE EVIDENCE and AVOID EXECUTION

☐ **MULTI-SYSTEM FAILURE**

TECHNICAL TEAM | CARD T2

☐ **WHEN TO USE**

Multiple systems failing • Coordinated attacks • Evidence of systematic compromise

☐ **DIVIDE & CONQUER (0-5 minutes)**

- ☐ Assign ONE VM per team member
- ☐ Start evidence preservation IMMEDIATELY
- ☐ Coordinate with ops on isolation decisions

☐ **INVESTIGATION PRIORITY ORDER**

1st PRIORITY: vm-gateway
→ Highest evidence destruction risk

2nd PRIORITY: vm-coretech
→ GPS/AIS navigation systems

3rd PRIORITY: 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 REQUIRED**

Evidence package • Trap script warnings • System correlation analysis

☐ **CCTV BLACKOUT RESPONSE**

OPERATIONS TEAM | CARD 01

☐ **WHEN TO USE**

Camera feeds black • Frozen screens • Static display • Visual monitoring lost

☐ **IMMEDIATE SAFETY (0-5 minutes)**

- ☐ Deploy manual spotters to ALL blind zones
- ☐ Reduce crane operations to 50% speed
- ☐ Establish radio contact with ALL operators
- ☐ Clear personnel from automated zones

☐ **MANUAL PROCEDURES (5-20 minutes)**

- ☐ Implement full spotter network
- ☐ Brief ALL crew on manual safety protocols
- ☐ Calculate reduced operational capacity
- ☐ Coordinate with TECHNICAL team on restoration

☐ **DECISION CHECKLIST**

- ✓ 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 → HALT OPERATIONS

☐ **AUTHENTICATION SYSTEM FAILURE**

OPERATIONS TEAM | CARD 02

☐ **WHEN TO USE**

Service accounts failing • Automated systems not responding • Access denied errors

☐ **SAFETY FIRST (0-2 minutes)**

- ☐ Complete any active container movements SAFELY
- ☐ Switch affected systems to MANUAL control
- ☐ Alert ALL operators to authentication issues

☐ **MANUAL OVERRIDE (2-15 minutes)**

- ☐ Implement manual authorisation procedures
- ☐ Use alternative verification methods
- ☐ Enhanced spotting for crane operations
- ☐ Document ALL manual overrides

☐ **COORDINATION ACTIONS**

- ☐ Work with TECHNICAL team on recovery
- ☐ Brief EXECUTIVE team if halt needed
- ☐ Monitor crew stress and confidence levels

☐ **KEY PRINCIPLE**

SAFETY over EFFICIENCY - Don't rush manual procedures

☐ CYBER INCIDENT ESCALATION

LEGAL TEAM | CARD L1

☐ WHEN TO USE

Unauthorised access • System compromise • Data breach evidence

☐ IMMEDIATE ASSESSMENT (0-10 minutes)

- ☐ Criminal activity suspected?
→ YES: Escalate to EXECUTIVE immediately
- ☐ Safety systems compromised?
→ YES: Priority regulatory review
- ☐ Data breach indicators?
→ YES: Start breach classification
- ☐ Multiple systems affected?
→ YES: Major incident protocols

☐ NOTIFICATION DECISION TREE

- Personal data affected → GDPR/privacy 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 preservation
- ☐ Protect attorney-client privilege in documentation

☐ TIME-CRITICAL DECISIONS

Breach notifications • Law enforcement contact • Regulatory reporting

□ REGULATORY COMPLIANCE CRISIS

LEGAL TEAM | CARD L2

□ WHEN TO USE

Multiple notification deadlines • Regulatory violations • Compliance gaps

□ PRIORITY MATRIX (0-5 minutes)

- IMMEDIATE: Safety-related notifications
- 2 HOURS: Criminal activity reports
- 24-72 HOURS: Data breach notifications
- 24 HOURS: Insurance notifications

□ RAPID RESPONSE ACTIONS

- 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

□ KEY PRINCIPLE

Regulatory deadlines take PRIORITY over perfect language

☐ IMMEDIATE MEDIA PRESSURE

MEDIA TEAM | CARD M1

☐ WHEN TO USE

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 info than let speculation spread

☐ **SOCIAL MEDIA CRISIS**

MEDIA TEAM | CARD M2

☐ **WHEN TO USE**

Anonymous posts • Trending hashtags • Viral misinformation about incident

☐ **IMMEDIATE MONITORING (0-5 minutes)**

- ☐ 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

☐ **REQUIRED OUTPUTS**

Social media monitoring report • Response actions • Stakeholder alerts

☐ OPERATIONS HALT DECISION

EXECUTIVE TEAM | CARD E1

☐ WHEN TO USE

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 ACTIONS

- ☐ 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

☐ **CRISIS ESCALATION DECISIONS**

EXECUTIVE TEAM | CARD E2

☐ **WHEN TO USE**

Major incident • Regulatory investigations • Board involvement needed

☐ **STRATEGIC DECISIONS NEEDED**

- ☐ External assistance needed?
 - Cyber forensics, crisis consultants
- ☐ Stakeholder communication level?
 - Customers, partners, board
- ☐ Legal strategy approach?
 - Defensive vs. transparent
- ☐ Business continuity priorities?
 - Critical vs. non-essential operations

☐ **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**

☐ **REQUIRED OUTPUTS**

Strategic direction • Resource authorisation • Stakeholder approval

❑ **MULTI-TEAM COORDINATION**

INCIDENT COORDINATOR | CARD IC1

❑ **WHEN TO USE**

Multiple teams active • Resource conflicts • Complex incident

❑ **COORDINATION SETUP (0-5 minutes)**

- ❑ Assign communication LEAD for each team
- ❑ Establish 15-minute UPDATE cycle
- ❑ Set up central DOCUMENTATION location
- ❑ Identify resource CONFLICT potential

❑ **PRIORITY MATRIX**

- ❑ Safety and regulatory compliance
- ❑ Evidence preservation and investigation
- ❑ Operational continuity
- ❑ Stakeholder communication

❑ **TEAM COORDINATION**

TECHNICAL + OPERATIONS → System isolation decisions

LEGAL + MEDIA → Communication approval

EXECUTIVE + ALL → Resource authorisation

ALL TEAMS → Information sharing

❑ **CONFLICT RESOLUTION**

Apply priority matrix → Escalate to EXECUTIVE if needed

□ EXTERNAL PRESSURE MANAGEMENT

INCIDENT COORDINATOR | CARD IC2

□ WHEN TO USE

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 BALANCE

TECHNICAL TEAM → Investigation vs. restoration
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:** 2.0 | **Approved by:** Cyber-Ops Coordination Cell