SOUTHGATE TERMINAL

## Port Operations Security Documentation

Technical / Ops Procedures – Technical Containment Guide

Purpose:
To guide technical responders in identifying, isolating, and containing threats or anomalies within a live operational environment. This guide ensures containment actions align with system integrity, legal boundaries, and escalation procedures.

When to Use

- Anomalous behaviour is detected (e.g. signal spoofing, log inconsistencies, unexpected cron jobs)
- Security indicators suggest unauthorised access or persistence
- Service degradation appears linked to internal systems or VM-based infrastructure

General Containment Principles

- Containment does not equal resolution — aim to stop spread or limit damage
- Avoid making permanent changes unless directed by Ops or Legal
- Record all actions taken in a structured log (timestamp + action + system)
- Do not delete files, restart hosts, or isolate systems from the network unless explicitly authorised

Immediate Actions by VM Type

☐ Core Infrastructure VMs (e.g. AIS Aggregator, Scheduler, Container Planner)

- SSH into the machine: ssh admin@[vm-name] (credentials provided separately)
- Check system status:
- top
- journalctl -xe
- df -h
- du -sh /opt/*
- Review key logs:
- tail -n 100 /var/log/syslog
- grep -i error /opt/app/logs/planner.log

  - journalctl -u scheduler.service --since ”1 hour ago”
  - Stop only affected services:
  - systemctl stop planner.service
  - kill -9 [pid] # if service is unresponsive
  - Collect logs for evidence:
  - cp /opt/app/logs/planner.log /var/log/evidence/planner-incident.log
  - sha256sum /opt/app/logs/planner.log > /var/log/evidence/planner.log.hash
  - Store notes: /var/log/incident/containment-[YYYYMMDD-HHMM].txt

☐ Vendor Gateway VM

  - View-only access permitted. Do not restart or stop services.
  - Logs located at: /var/vendor/logs/gateway.log
  - Sample inspection:
  - tail -n 50 /var/vendor/logs/gateway.log
  - grep -i connect /var/vendor/logs/gateway.log
  - stat /usr/bin/gatewayd
  - Report any anomalies immediately via Coordinator — do not modify files or settings.

☐ Communications / GPS VM

  - Monitor traffic:
  - ss -tunap
  - tcpdump -i eth0 port not 22 -c 100
  - netstat -tnp
  - Check DNS, routing, and external connections:
  - cat /etc/resolv.conf
  - dig example.com
  - route -n
  - Isolate network (with authorisation only):
  - ifconfig eth0 down

☐ Physical Ops / Sensor Feed VM

  - Identify and stop containers:
  - docker ps

- docker stop [container_id]
- docker inspect [container_id] > /var/log/dumps/container-[id].json
- Review container logs:
- docker logs [container_id] | tail -n 100
- Review disk usage and file changes:
- find /opt/sensors/ -type f -mtime -1
- ls -lt /tmp/

Red Flags Requiring Immediate Escalation

- Unexpected cron entries:
- crontab -l
- cat /etc/cron.*/*
- Suspicious binaries or file changes:
- find / -type f -name ”*sh” -exec stat {} \;
- md5sum /usr/bin/ssh
- Cross-VM traffic or log evidence of lateral movement
- Services running from non-standard paths (e.g. /tmp/, /dev/shm/)

Communication & Coordination

- Log all containment actions in the team channel and incident log
- Tag actions with urgency (#containment, #forensics, #approval-needed)
- Validate vendor boundaries: do not breach service terms even under pressure
- Escalate prior to deleting or isolating persistent threats

CCTV Blackout Response SOP

Purpose

This procedure provides immediate and extended response protocols for CCTV system failures, ensuring continued safe operations during surveillance loss. Use when camera feeds go black, show static, or display frozen images.

When to Use

- Individual camera blackouts affecting critical zones
- Multiple camera failures across sectors
- Complete CCTV system failure
- Intermittent camera feed disruptions
- CCTV failures coinciding with other system issues

Immediate Response (First 5 minutes)

Step 1: Scope Assessment

1. Identify Affected Areas

☐ Document specific cameras/zones affected
☐ Map coverage gaps for operational areas
☐ Identify critical safety zones without coverage

2. System Status Check

☐ Verify CCTV control room system status
☐ Check network connectivity to camera feeds
☐ Review recent system configuration changes

3. Safety Evaluation

☐ Assess crane operations in blind zones
☐ Evaluate container movement safety
☐ Check personnel working in affected areas

Step 2: Immediate Safety Measures (Next 5 minutes)

1. Personnel Deployment

☐ Station manual spotters at affected critical zones
☐ Deploy safety personnel to blind spots
☐ Establish radio contact with all spotters

2. Operations Adjustment

☐ Slow down operations in affected areas
☐ Implement buddy system for crane operations
☐ Increase communication frequency

3. Communication Alert

☐ Alert all crane operators to CCTV loss
☐ Notify operations team of coverage gaps
☐ Establish direct radio protocols

Short-Term Response (5-30 minutes)

Enhanced Manual Procedures

1. Spotter Network Establishment

☐ Assign dedicated spotters to each blind zone
☐ Establish clear radio communication protocols
☐ Create backup spotter rotation schedule

2. Modified Operating Procedures

☐ Reduce crane movement speed in blind zones
☐ Require verbal confirmation for all container moves
☐ Implement double-check system for safety clearances

3. Alternative Monitoring

☐ Use handheld radios for constant communication
☐ Deploy temporary mobile cameras if available
☐ Increase frequency of safety walks

Cross-System Impact Assessment

1. Network Correlation Check

☐ Verify if CCTV loss correlates with network issues
☐ Check if other systems affected simultaneously
☐ Document timing relationships

2. AIS Correlation Check

☐ Compare CCTV blackout timing with AIS anomalies
☐ Assess if vessels are visible but not tracking
☐ Note any cross-system pattern implications

Extended Response (30+ minutes)

Sustained Operations Protocol

1. Workforce Adjustments

☐ Rotate spotter personnel to prevent fatigue
☐ Brief all personnel on modified safety procedures
☐ Monitor crew stress and confidence levels

2. Operational Capacity Assessment

☐ Calculate safe operational capacity without CCTV
☐ Determine if operations should be reduced or halted
☐ Document capacity limitations for planning

3. Alternative Solutions

□ Deploy temporary surveillance equipment
□ Consider external security personnel
□ Evaluate mobile camera options

Decision Points for Operations Continuation

CONTINUE FULL OPERATIONS IF:

- Adequate manual spotters available
- Clear radio communication maintained
- Crew comfortable with manual procedures
- No correlation with other system failures

REDUCE OPERATIONS IF:

- Limited spotter coverage available
- Communication challenges identified
- Crew expressing safety concerns
- Multiple systems affected simultaneously

HALT OPERATIONS IF:

- Cannot ensure safe container movements
- Inadequate personnel for manual spotting
- Crew refusing to work without visual confirmation
- Safety risk assessment indicates high danger

Communication Protocols

To Crane Operators

- "CCTV blackout in [zones]. Manual spotters deployed at [locations]. Reduce speed, require verbal clearance for all moves."

To Operations Team

- "CCTV system [partially/fully] compromised. Manual procedures implemented. Current capacity: [X]%. Safety [maintained/at risk]."

To Technical Team

- "CCTV blackout affects [zones]. Correlates with [network/AIS] issues at [time]. Technical investigation and restoration required urgently."

To Incident Coordinator

- “CCTV Status: [description]. Manual procedures: [implemented]. Operations: [continuing/reduced/halted]. Restoration priority: HIGH.”

Safety Risk Assessment Matrix

LOW RISK (Continue normal operations)

- Single non-critical camera failure
- Adequate alternative visual coverage
- Clear weather and good visibility
- Minimal personnel in affected area

MEDIUM RISK (Enhanced procedures required)

- Multiple camera failures
- Critical zone coverage lost
- Reduced but adequate spotter coverage
- Normal weather conditions

HIGH RISK (Consider operations reduction)

- Major system failure affecting multiple critical zones
- Limited spotter availability
- Poor weather affecting visibility
- Heavy operational activity in blind areas

CRITICAL RISK (Halt operations)

- Complete CCTV failure with inadequate manual coverage
- Safety concerns raised by operational personnel
- Weather conditions limiting visibility
- Evidence of deliberate system interference

Technical Coordination Requirements

With Network Team

- Coordinate if CCTV loss correlates with network issues
- Share timing information for cross-system analysis
- Prioritize network restoration if CCTV depends on it

With Cyber Security (if applicable)

- Escalate if CCTV failure appears deliberate
- Preserve logs if cyber incident suspected
- Coordinate with other system anomaly investigations

Restoration Verification Process

Pre-Restoration Testing

1. Camera Functionality

☐ Test each camera feed individually
☐ Verify image quality and positioning
☐ Confirm recording functionality restored

2. Network Connectivity

☐ Test network stability to camera systems
☐ Verify no packet loss or delay issues
☐ Confirm backup systems operational

Gradual Return to Automated Monitoring

1. Phased Restoration

☐ Restore most critical cameras first
☐ Gradually reduce manual spotter coverage
☐ Maintain enhanced communication during transition

2. Extended Monitoring

☐ Monitor system stability for first hour after restoration
☐ Keep backup spotters available
☐ Document any recurring issues

Success Criteria

- Safe operations maintained despite CCTV loss
- Adequate manual monitoring coverage established
- Clear communication protocols functioning
- Crew confidence and safety maintained
- Smooth transition back to CCTV monitoring

Related Procedures

- Use with: Manual Override Authorization (for modified operations)
- Coordinate with: Safety Risk Assessment Template
- Reference: Network Diagnostics SOP (if network correlation identified)
- Escalate to: Crisis Decision Authority Matrix (for operations halt decisions)

Log Deletion Investigation SOP

Purpose

This procedure provides systematic investigation steps for suspected or confirmed log deletion events, preserving evidence and determining scope of potential security compromise. Use when system logs appear missing, modified, or deliberately deleted.

When to Use

- System alerts indicating log file deletion
- Missing logs during routine security reviews
- Gaps in log timelines correlating with incidents
- Evidence of unauthorized access to log files
- System administrators reporting log anomalies

Immediate Response (First 10 minutes)

Step 1: Incident Confirmation

1. Alert Verification

☐ Confirm log deletion alert is genuine
☐ Identify specific log files or systems affected
☐ Note exact time of deletion detection

2. System Status Check

☐ Verify affected systems are still operational
☐ Check if logging services are currently functioning
☐ Assess immediate security posture

3. Initial Scope Assessment

☐ Determine which log types were deleted (auth, system, application)
☐ Identify time range of missing logs
☐ Check for patterns or systematic deletion

Step 2: Evidence Preservation

1. System Isolation Assessment

☐ Determine if affected system should be isolated
☐ Consider operational impact of isolation
☐ Document decision rationale

2. Immediate Evidence Capture

☐ Take system snapshots before any changes
☐ Preserve current log status and configurations

☐ Document system state with timestamps

3. Chain of Custody Initiation

☐ Begin forensic evidence log
☐ Assign evidence custodian
☐ Restrict system access to authorized investigators

Investigation Phase (10-45 minutes)

System Analysis

1. Log System Configuration Review

☐ Check log rotation settings and schedules
☐ Verify log retention policies and implementation
☐ Review recent configuration changes

2. Access Log Analysis

☐ Review authentication logs for unusual access
☐ Check for administrative access during deletion timeframe
☐ Identify users with log file access permissions

3. Command History Review

☐ Check bash/shell history for deletion commands
☐ Review sudo logs for privileged operations
☐ Analyze cron jobs or scheduled tasks

Deletion Pattern Analysis

1. Systematic vs. Targeted Deletion

- Systematic: All logs deleted = likely cover-up of extensive activity
- Targeted: Specific logs deleted = attempt to hide particular actions
- Time-based: Logs from specific period = incident-related deletion

2. Deletion Method Analysis

☐ Standard deletion commands (rm, del)
☐ Secure deletion tools (shred, wipe)
☐ Log rotation manipulation
☐ Service configuration changes

3. Timeline Correlation

☐ Compare deletion time with other security events
☐ Check correlation with system anomalies
☐ Analyze relationship to operational incidents

Technical Investigation

File System Analysis

1. Deleted File Recovery Attempts

☐ Check for recoverable deleted files
☐ Review system trash/recycle bins
☐ Attempt forensic file recovery if appropriate

2. File System Metadata Analysis

☐ Check file creation/modification timestamps
☐ Review file permission changes
☐ Analyze disk space usage patterns

3. Backup and Archive Review

☐ Check if deleted logs exist in backups
☐ Review archive systems for log copies
☐ Verify backup integrity and availability

Network and Remote Access Analysis

1. Remote Access Review

☐ Check VPN connections during deletion timeframe
☐ Review remote desktop or SSH sessions
☐ Analyze network connections to log systems

2. External Communication

☐ Check for data exfiltration attempts
☐ Review outbound network traffic
☐ Analyze communication to external systems

Evidence Recovery and Reconstruction

Alternative Log Sources

1. Centralized Logging Systems

☐ Check SIEM or centralized log servers
☐ Review log forwarding configurations
☐ Verify remote log copies

2. Application and Service Logs

☐ Review application-specific logs
☐ Check database audit logs
☐ Analyze service-specific logging

3. Network Device Logs

☐ Review firewall and router logs
☐ Check network switch logs
☐ Analyze intrusion detection system logs

Timeline Reconstruction

1. Event Correlation

☐ Correlate available logs with incident timeline
☐ Map user activities before deletion
☐ Identify gaps requiring investigation

2. Activity Pattern Analysis

☐ Analyze normal vs. anomalous activity patterns
☐ Identify unusual system or user behavior
☐ Document potential indicators of compromise

Classification and Escalation

Incident Classification

1. Accidental Deletion

- Indicators: Admin error, legitimate maintenance, single user
- Response: Standard incident procedures, improved controls

2. Insider Threat

- Indicators: Deliberate deletion by authorized user, selective targeting
- Response: HR coordination, enhanced monitoring, possible termination

3. External Compromise

- Indicators: Unauthorized access, systematic deletion, correlation with other attacks
- Response: Cyber team escalation, potential law enforcement, full investigation

Escalation Criteria IMMEDIATE ESCALATION TO CYBER TEAM IF: - [ ] Evidence of unauthorized access to log systems - [ ] Systematic deletion suggesting cover-up of extensive activity - [ ] Correlation with other confirmed security incidents - [ ] Critical security logs deleted (authentication, privileged access)

EXECUTIVE ESCALATION IF: - [ ] Evidence suggests insider threat or malicious intent - [ ] Regulatory compliance implications identified - [ ] Potential law enforcement involvement required

Recovery and Remediation

Immediate Recovery Actions

1. Log Service Restoration

☐ Restore logging services to full operation
☐ Implement enhanced logging if available
☐ Verify log integrity mechanisms

2. Access Control Review

☐ Review and restrict log file access permissions
☐ Implement enhanced monitoring for log files
☐ Consider log file immutability solutions

Long-term Improvements

1. Enhanced Logging Strategy

☐ Implement centralized logging with remote storage
☐ Add log integrity checking mechanisms
☐ Enhance log retention and backup procedures

2. Monitoring and Alerting

☐ Implement real-time log deletion monitoring
☐ Add file integrity monitoring for critical logs
☐ Enhance alerting for suspicious log access

Communication Protocols

To Technical Team "Log deletion incident confirmed on [system]. Scope: [description]. Investigation status: [in progress/completed]. Technical coordination needed for: [specific requirements]."

To Incident Coordinator "SECURITY ALERT: Log deletion detected. Classification: [accidental/insider/external]. Investigation timeline: [estimate]. Escalation requirements: [none/cyber team/executive]."

To Executive (if required) "Critical security incident: Deliberate log deletion detected. Potential implications: [regulatory/legal/operational]. Investigation underway. External assistance: [required/not required]."

Documentation Requirements

Investigation Log

☐ Timeline of all investigation activities

☐ Evidence collected and chain of custody
☐ Analysis results and conclusions
☐ Recommendations for prevention

Technical Report

☐ Detailed technical findings
☐ Recovery actions taken
☐ System configuration changes
☐ Lessons learned and improvements

Success Criteria

- Complete investigation of log deletion incident
- Maximum evidence recovery and preservation
- Accurate classification of incident type and intent
- Appropriate escalation and response actions taken
- Preventive measures implemented to reduce future risk

Related Procedures

- Use with: Breach Classification Decision Tree (for incident categorization)
- Coordinate with: Network Diagnostics SOP (if network compromise suspected)
- Reference: Forensics Summary Template (for evidence documentation)
- Escalate to: Crisis Decision Authority Matrix (for executive decisions)

Enhanced Crane Safety Procedures During CCTV Blackout

Purpose

This subsection provides specific crane safety procedures to implement during CCTV blackouts, ensuring safe crane operations when visual monitoring systems are compromised.

Immediate Crane Safety Actions (0-5 minutes)

Crane Operation Assessment   For Each Active Crane: - [ ] Current Load Status: Identify any containers currently being lifted - [ ] Load Position: Determine exact position of suspended loads - [ ] Operator Status: Verify crane operator awareness of CCTV loss - [ ] Spotter Availability: Confirm qualified spotters available for each crane

Emergency Load Management For Suspended Containers: 1. Immediate Safety: - [ ] Complete current lift if nearly finished and safe to do so - [ ] Lower container to nearest safe position if lift cannot be completed - [ ] Ensure area beneath suspended load is completely clear - [ ] Maintain constant radio contact with crane operator

2. Area Clearance:

- ☐ Evacuate all personnel from beneath suspended loads
- ☐ Establish expanded safety zones around crane operations
- ☐ Post additional personnel to maintain clear zones
- ☐ Use air horns or whistles to alert personnel

Enhanced Spotter Deployment for Cranes

Spotter Assignment Matrix Single Crane Operations: - Primary Spotter: Positioned at optimal viewing angle for crane operator’s blind spots - Secondary Spotter: Ground-level container guidance and area monitoring - Roving Spotter: Personnel and vehicle traffic monitoring

Multiple Crane Operations: - Dedicated Spotter per Crane: One primary spotter assigned to each active crane - Central Coordinator: Overall coordination between multiple crane operations - Safety Officer: Continuous safety monitoring across all crane operations

Spotter Positioning Guidelines Primary Spotter Position: - Clear visual line to crane operator cab - Unobstructed view of entire crane movement area - Safe distance from crane operation (minimum 20 feet from load path) - Radio communication capability with crane operator

Communication Protocol: - Continuous radio contact on dedicated crane channel - Hand signals as backup communication method - Emergency stop signals clearly understood by all personnel - Regular check-ins every 2 minutes during operations

Modified Crane Operation Procedures

Reduced Speed Operations Speed Restrictions During CCTV Blackout: - Hoist Speed: Reduce to 50% of normal operating speed - Trolley Travel: Reduce to 40% of normal speed - Bridge Travel: Reduce to 30% of normal speed - Slewing (if applicable): Reduce to 25% of normal speed

Enhanced Verification Procedures Pre-Move Verification (Every container move): 1. Spotter Confirmation: - [ ] Primary spotter confirms area clear - [ ] Ground spotter confirms load path clear - [ ] Safety officer confirms overall area safety

2. Operator Verification:

☐ Crane operator confirms readiness
☐ Load weight and rigging verified
☐ Destination confirmed and cleared
☐ Emergency stop procedures reviewed

3. Communication Check:

☐ Radio communication tested
☐ Hand signal understanding confirmed
☐ Emergency signal protocols verified

Step-by-Step Move Protocol For Each Container Movement: 1. Pre-Lift Phase (2-3 minutes): - [ ] Spotters positioned and confirmed - [ ] Area cleared and secured - [ ] Communication established - [ ] Load rigging verified

2. Lift Phase (Extended time):

☐ Slow, controlled lift with constant spotter communication
☐ Regular position updates from spotters
☐ Continuous area monitoring
☐ Ready for immediate stop if needed

3. Travel Phase (Extended time):

☐ Spotters move with crane maintaining visual contact
☐ Continuous clear-path verification
☐ Ground personnel maintain safe distances
☐ Regular safety check-ins

4. Placement Phase (Extended time):

☐ Destination area verified clear
☐ Precise placement with spotter guidance
☐ Slow, controlled lowering
☐ Final placement confirmation

Environmental and Weather Considerations

Enhanced Weather Monitoring Additional Weather Restrictions During CCTV Blackout: - Wind Speed: Reduce maximum operating wind speed by 25% - Visibility: Stop operations if visibility drops below 500 meters - Precipitation: Consider stopping operations in moderate rain or snow - Temperature: Monitor for operator fatigue in extreme temperatures

Lighting Requirements Enhanced Lighting for Night/Low-Light Operations: - [ ] Additional portable lighting deployed in crane operation areas - [ ] Spotter positions illuminated for visibility - [ ] Container landing areas well-lit - [ ] Emergency lighting systems verified operational

Crew Fatigue and Stress Management

Operator Rotation Schedule Enhanced Rotation During CCTV Blackout: - Standard Rotation: Every 2 hours instead of 4 hours - Stress Assessment: Monitor for signs of stress or fatigue - Break Requirements: 15-minute break every hour - Backup Operators: Ensure qualified backup operators available

Stress Indicators Monitoring Watch for Operator Stress Signs: - Delayed responses to spotter communications - Jerky or unsteady crane movements - Increased mistakes or near-misses - Expressions of uncertainty or fear - Physical signs of fatigue or stress

Immediate Actions for Stress/Fatigue: 1. Assessment: Evaluate operator condition 2. Rest: Provide immediate break if needed 3. Replacement: Replace operator if stress/fatigue significant 4. Support: Provide additional spotter support if continuing

Emergency Procedures Specific to CCTV Blackout

Emergency Stop Procedures Enhanced Emergency Stop Protocol: - Multiple Trigger Points: Any spotter can initiate emergency stop - Clear Signals: Both radio and visual emergency signals - Immediate Response: All crane operations stop immediately - Area Evacuation: Enhanced evacuation procedures for limited visibility

Equipment Malfunction Response Crane Equipment Issues During CCTV Blackout: 1. Immediate Actions: - [ ] Emergency stop of affected crane - [ ] Secure any suspended loads safely - [ ] Clear area beneath crane - [ ] Assess nature of malfunction

2. Enhanced Safety Measures:

☐ Additional safety perimeter established
☐ Backup crane positioned if available
☐ Emergency response team alerted
☐ Alternative load handling planned

Container-Specific Safety Procedures

Container Type Considerations Enhanced Procedures by Container Type: - Standard Containers: Standard enhanced procedures apply - Oversize/Heavy Containers: Additional spotters and reduced speeds - Hazardous Materials:

Stop operations until CCTV restored or exceptional safety measures - Refrigerated Containers: Priority handling with enhanced monitoring

Container Securing and Verification Enhanced Container Handling: - [ ] Double-check container identification before lift - [ ] Verify container weight and center of gravity - [ ] Ensure proper spreader engagement - [ ] Confirm container condition before move

Communication Enhancement

Radio Protocol During CCTV Blackout Enhanced Radio Discipline: - Clear, concise communications only - Regular check-ins every 2 minutes - Immediate reporting of any concerns - Emergency channel kept clear for emergencies

Standard Communication Format:

```
"Crane [Number] to Spotter [Position]: [Action] - [Status] - [Next Action]"
"Spotter [Position] to Crane [Number]: [Confirmation] - [Area Status] - [Clear/Hold]"
```

Success Criteria for Crane Operations During CCTV Blackout

- Safe crane operations maintained without visual monitoring systems
- Zero safety incidents related to reduced visibility
- Effective spotter communication and coordination
- Appropriate operational speed adjustments implemented
- All personnel comfortable and confident with enhanced safety procedures

---

Owner: Technical Lead
Reference: TECH-01
Version: 1.1
Approved by: Cyber-Ops Coordination Cell