

# SOUTHGATE TERMINAL

## ## Port Operations Security Documentation

### Executive Briefing Template and Schedule

#### Document Information

**Document Type:** Executive Communication Framework

**Intended Users:** Executive Team, Incident Coordinators, Team Leads

**Usage Context:** During crisis situations requiring executive oversight and decision-making

**Related Scenarios:** Multi-system failures, cyber incidents, regulatory compliance, media attention

---

#### Purpose

This template provides structured executive briefing format and scheduling protocols during crisis situations, ensuring executives receive critical information efficiently and can make informed strategic decisions rapidly.

#### When to Use This Template

- Incidents requiring executive awareness or decision-making
  - Regulatory or legal implications requiring executive oversight
  - Media attention or public relations concerns
  - Resource allocation decisions exceeding operational authority
  - Safety incidents with potential liability or regulatory impact
- 

#### Executive Briefing Schedule Framework

##### Briefing Frequency by Crisis Level

**Level 1: Routine Incident (Green)** **Characteristics:** Single system issue, no safety impact, contained within operational response - **Briefing Frequency:** Daily summary email - **Format:** Written summary only - **Duration:** N/A (written communication) - **Attendees:** CEO or designated deputy

**Level 2: Significant Incident (Yellow)** **Characteristics:** Multiple systems affected, some operational impact, potential regulatory implications - **Briefing Frequency:** Every 4 hours - **Format:** Written summary + verbal brief if requested - **Duration:** 10 minutes maximum - **Attendees:** CEO, COO, CTO as appropriate

**Level 3: Major Incident (Orange)** **Characteristics:** Major operational impact, safety concerns, definite regulatory/legal implications - **Briefing Frequency:** Every 2 hours - **Format:** Structured verbal briefing + written summary - **Duration:** 15 minutes maximum - **Attendees:** CEO, COO, CTO, Legal Counsel, Head of Communications

**Level 4: Crisis (Red)** **Characteristics:** Terminal-wide impact, safety emergencies, potential organizational threat - **Briefing Frequency:** Every 30 minutes or as developments occur - **Format:** Immediate verbal brief + formal written summary - **Duration:** 20 minutes maximum - **Attendees:** Full executive team, board notification, external advisors as needed

---

## Executive Briefing Template

### Executive Summary (30 seconds)

**CURRENT STATUS:** [One sentence describing overall situation]  
**SAFETY STATUS:** [Personnel safety and any ongoing risks]  
**OPERATIONAL STATUS:** [Current operational capacity and limitations]  
**RESOLUTION TIMELINE:** [Expected timeline for resolution or next major milestone]

### Situation Overview (2 minutes)

**INCIDENT DESCRIPTION:** - What happened: [Brief factual description] - When: [Timeline of key events] - Systems affected: [Specific systems and impact] - Current scope: [Contained/expanding/stable]

**ROOT CAUSE ANALYSIS:** - Known causes: [Confirmed causes] - Suspected causes: [Under investigation] - External factors: [Weather, vendor issues, etc.] - Deliberate action: [Evidence for/against]

### Impact Assessment (2 minutes)

**OPERATIONAL IMPACT:** - Current capacity: [Percentage of normal operations] - Revenue impact: [Estimated financial impact] - Customer impact: [Service delays, disruptions] - Recovery timeline: [Estimated return to normal]

**SAFETY IMPACT:** - Personnel safety: [Any injuries or ongoing risks] - Public safety: [Community or environmental risks] - Safety measures: [Additional precautions in place] - Emergency services: [Involvement if any]

**REGULATORY/LEGAL IMPACT:** - Notification requirements: [What must be reported and when] - Compliance status: [Current standing with regulations] - Potential liability: [Legal exposure assessment] - Insurance implications: [Coverage and claims status]

### **Response Actions (2 minutes)**

**IMMEDIATE ACTIONS TAKEN:** - Technical response: [System restoration efforts] - Operational response: [Manual procedures, resource allocation] - Safety response: [Personnel protection measures] - Communication response: [Internal and external communications]

**ONGOING RESPONSE:** - Technical teams: [Current activities and focus] - Operations teams: [Current activities and capacity] - External support: [Vendors, contractors, emergency services] - Resource allocation: [Personnel and equipment deployment]

### **Decisions Required (1 minute)**

**IMMEDIATE DECISIONS NEEDED:** 1. [Decision 1]: [Brief description and urgency] 2. [Decision 2]: [Brief description and urgency] 3. [Decision 3]: [Brief description and urgency]

**STRATEGIC DECISIONS PENDING:** - [Medium-term decisions requiring executive input] - [Resource allocation decisions beyond operational authority] - [Policy or procedural changes under consideration]

### **External Factors (1 minute)**

**STAKEHOLDER CONCERNS:** - Customers: [Specific concerns and communication needs] - Vendors: [Impact on vendor relationships] - Regulatory bodies: [Agency interest or involvement] - Community: [Public interest or concerns]

**MEDIA AND PUBLIC RELATIONS:** - Media interest: [Current level and type of coverage] - Social media: [Public discussion and sentiment] - Communication needs: [Planned communications and messaging] - Reputation impact: [Assessment and mitigation strategies]

### **Next Steps and Timeline (1 minute)**

**NEXT 2 HOURS:** - [Key milestones and expected developments] - [Critical decisions or actions required] - [Resource needs or challenges anticipated]

**NEXT 24 HOURS:** - [Major restoration milestones] - [Key decision points] - [External commitments or deadlines]

**LONGER TERM:** - [Full recovery timeline] - [Lessons learned process] - [Prevention measures under consideration]

## Specialized Briefing Formats

### Cyber Security Incident Brief

**THREAT ASSESSMENT:** - Attack type: [Confirmed or suspected] - Threat actor: [Known or suspected source] - Attack vector: [How system was compromised] - Scope of compromise: [What systems/data affected]

**CONTAINMENT STATUS:** - Systems isolated: [What has been disconnected] - Ongoing threats: [Active threats remaining] - Evidence preservation: [Forensic actions taken] - Law enforcement: [Involvement status]

### Safety Emergency Brief

**INCIDENT DETAILS:** - Personnel involved: [Number and condition] - Emergency response: [Services involved] - Cause analysis: [Known or suspected causes] - Ongoing risks: [Continuing safety concerns]

**RESPONSE STATUS:** - Medical response: [Treatment and transport] - Area security: [Evacuation or isolation] - Investigation: [Safety investigation status] - Regulatory notification: [Required reporting status]

### Media Crisis Brief

**MEDIA LANDSCAPE:** - Coverage scope: [Local/national/international] - Key narratives: [What stories are being told] - Source accuracy: [Factual vs. speculative reporting] - Trend analysis: [Growing/stable/declining coverage]

**COMMUNICATION STRATEGY:** - Current messaging: [Key messages being used] - Spokesperson status: [Who is speaking for organization] - Planned communications: [Upcoming statements or interviews] - Stakeholder outreach: [Direct communication with key parties]

---

## Executive Decision Framework

### Decision Categories and Authority

**Category A: Immediate Safety Decisions** **Authority:** CEO or any executive present **Timeline:** Immediate implementation **Examples:** Personnel evacuation, emergency services contact, operations shutdown **Documentation:** Decision and rationale recorded immediately

**Category B: Operational Continuity Decisions** **Authority:** CEO with COO consultation **Timeline:** Within 30 minutes **Examples:** Extended manual operations, significant resource allocation, vendor engagement **Documentation:** Formal decision record with impact assessment

**Category C: Strategic Communication Decisions**    **Authority:** CEO with Communications/Legal consultation    **Timeline:** Within 1 hour    **Examples:** Public statements, media interviews, stakeholder communications    **Documentation:** Message approval and legal review record

**Category D: Legal and Regulatory Decisions**    **Authority:** CEO with Legal Counsel required    **Timeline:** As required by regulation    **Examples:** Regulatory notifications, legal proceedings, insurance claims    **Documentation:** Legal compliance documentation

### Decision Documentation Template

**DECISION ID:** [Unique identifier]  
**DATE/TIME:** [When decision was made]  
**DECISION MAKER:** [Executive making decision]  
**CATEGORY:** [A/B/C/D as above]  
**DECISION:** [Specific action authorized]  
**RATIONALE:** [Key factors influencing decision]  
**CONSULTATION:** [Who was consulted]  
**IMPLEMENTATION:** [Who will implement and timeline]  
**REVIEW:** [When decision will be reviewed]

---

## Communication Protocols

### Pre-Briefing Preparation (15 minutes before briefing)

**Information Gathering:** - [ ] Collect latest status updates from all teams - [ ]  
Verify all facts and timelines - [ ] Prepare decision options with recommendations  
- [ ] Review previous briefing for updates

**Document Preparation:** - [ ] Complete briefing template - [ ] Prepare visual aids if helpful (charts, timelines) - [ ] Have supporting documents available - [ ]  
Prepare alternative scenarios or options

### During Briefing

**Presenter Guidelines:** - [ ] Stick to template structure and timeline - [ ]  
Present facts clearly and concisely - [ ] Acknowledge uncertainties honestly - [ ]  
Provide clear recommendations for decisions - [ ] Be prepared to answer follow-up questions

**Executive Guidelines:** - [ ] Ask clarifying questions immediately - [ ] Focus on strategic decisions needed - [ ] Consider organizational and stakeholder impacts - [ ]  
Make decisions promptly when possible - [ ] Request additional information if needed for decisions

### **Post-Briefing Actions (5 minutes after briefing)**

**Documentation:** - ☐ Record all decisions made - ☐ Document any new information requirements - ☐ Update briefing schedule if needed - ☐ Communicate decisions to implementation teams

**Follow-up:** - ☐ Ensure decisions are being implemented - ☐ Schedule next briefing - ☐ Alert stakeholders to executive decisions as appropriate - ☐ Update crisis status level if warranted

---

## **Escalation and External Coordination**

### **Board Notification Triggers**

**Immediate Notification Required:** - Safety incidents with serious injury or fatality - Criminal activity or major security breaches - Regulatory investigations or legal proceedings initiated - Media crisis with national attention - Financial impact exceeding \$[X] threshold

**24-Hour Notification Required:** - Extended operational shutdowns - Major customer or vendor relationship impacts - Regulatory compliance violations - Reputation risks requiring strategic response

### **External Advisor Engagement**

**Legal Counsel:** - Criminal activity suspected - Regulatory investigations - Potential liability issues - Contract or employment law implications

**Crisis Communications Specialist:** - National media attention - Social media campaigns against organization - Stakeholder relationship management needs - Reputation recovery planning

**Technical Specialists:** - Cyber security incidents requiring forensic expertise - System failures beyond internal expertise - Vendor coordination for critical systems - Emergency procurement needs

---

## **Success Criteria**

- Executives receive timely, accurate, and actionable information
  - Strategic decisions made promptly with appropriate consultation
  - Clear documentation of all executive decisions and rationale
  - Effective coordination between operational response and executive oversight
  - Appropriate stakeholder communication and relationship management
-

## **Related Documents**

- Crisis Decision Authority Matrix
- Crisis Communications SOP
- Legal Risk Escalation Flowchart
- Safety Risk Assessment Template
- Multi-System Failure Coordination Guide