SOUTHGATE TERMINAL

Port Operations Security Documentation

Media / Communications – Crisis Communications SOP

Purpose:
To provide a clear and structured protocol for managing internal and external communications during a crisis or incident. This SOP ensures consistency, coordination, and alignment across executive, media, and legal teams.

When to Use

- Any event that affects operations, safety, data, or stakeholder trust
- Situations where media attention, public queries, or online visibility is expected or confirmed
- Regulatory, insurer, or legal triggers that require disclosure

RAPID CRISIS RESPONSE (When Under Immediate Pressure)

IMMEDIATE MEDIA PRESSURE (15-30 minutes to respond)

QUICK DECISION MATRIX: - **Media calling for immediate comment?** - Use 5-minute holding statement template below - **Social media posts about incident?** - Monitor and prepare rapid response - **TV crew on-site?** - Activate Final Media Deadline Management procedures - **Regulatory deadline approaching?** - Coordinate with legal team immediately

5-MINUTE HOLDING STATEMENT TEMPLATE:

```
"[Organization] is aware of [brief incident description]. The safety and security of our ope
```

15-MINUTE CRISIS COMMUNICATION SETUP:

1. **Minutes 1-3:** Assess severity and media visibility
2. **Minutes 4-8:** Draft initial holding statement using template
3. **Minutes 9-12:** Coordinate with legal team on approval
4. **Minutes 13-15:** Distribute statement and activate monitoring

SOCIAL MEDIA RAPID RESPONSE:

- **Anonymous posts about incident:** Monitor but don't engage directly
- **Factual inaccuracies spreading:** Prepare corrective statement
- **Trending hashtags:** Document and assess need for response

- **Employee posts:** Coordinate with HR for internal messaging

Primary Roles & Responsibilities

Media Lead

- Drafts and manages all public-facing messages
- Coordinates with CEO and Legal on tone, timing, and content
- Tracks media and social sentiment where applicable

CEO / Executive Lead

- Acts as official spokesperson unless delegated
- Approves all formal statements, including interviews
- Coordinates with stakeholders and board-level contacts

Legal Team

- Reviews content for liability, compliance, and contractual risks
- Advises on timing of statements relative to breach, insurer, or regulatory triggers

Core Messaging Workflow

1. **Trigger Identified**

- Media inquiry, social media mention, regulator request, or public visibility spike

2. **Initial Drafting (Media Lead)**

- Use Public Messaging Templates (Holding / Denial / Acknowledgement)
- Prepare both reactive (response) and proactive (pre-emptive) drafts

3. **Review & Input**

- Legal reviews for exposure, insurer language, compliance
- CEO reviews for tone, strategic alignment, and final authority

4. **Approval**

- Statements are not released until signed off by CEO or Crisis Lead

5. **Delivery Method**

- Choose appropriate channel (e.g. email, press release, website, social post)
- Coordinate timing with incident updates or external triggers

6. **Monitoring & Adjustments**

- Track feedback, media coverage, or public response
- Update talking points or FAQ as needed

Response Timing Guidance

Scenario Type **Recommende	d Timing**
Public tweet or media inquiry Wit	hin 30 minutes
Confirmed breach with external Wi	thin 1 hour of internal confirmation
risk	
Operational disruption only As n	eeded; not mandatory
Regulator or insurer contact Coo	rdinated with Legal response window

Content Do's and Don'ts

Do:

- Acknowledge awareness of issue (if public)
- Use factual language and confirmed details only
- Align statements with policy documents
- Provide timeline for follow-up where possible

Don't:

- Speculate on root cause or attribution
- Use technical jargon without explanation
- Over-promise (e.g. resolution timelines)
- Respond emotionally or defensively

Pre-Approved Templates Available

- Holding Statement Template
- Denial / Refute Template
- Acknowledgement + Timeline Template
- Post-Resolution Summary

Rapid Response Media Protocol (15-30 Minute Deadlines)

Purpose

This procedure provides streamlined decision-making and response protocols for urgent media requests with extremely tight deadlines. Use when reporters demand immediate responses, live broadcasts are imminent, or breaking news requires rapid organizational response.

When to Use

- Live TV interview requests with 15-30 minute deadlines
- Breaking news stories requiring immediate comment
- Social media crises demanding rapid response
- Reporter deadlines that cannot be extended
- News segments proceeding with or without organization input

Rapid Decision Framework

5-Minute Assessment Phase

1. **Threat Level Evaluation**

- **GREEN:** Routine story, low risk, standard response adequate
- **YELLOW:** Moderate risk, potential negative angle, careful response needed
- **RED:** High risk, crisis angle, strategic response critical

2. **Story Context Analysis**

☐ What information does reporter already have?
☐ What angle are they pursuing?
☐ Who else are they interviewing?
☐ What's the potential reach/impact?

3. **Response Option Assessment**

- **PARTICIPATE:** Provide spokesperson and statement
- **STATEMENT ONLY:** Written response, no interview
- **DECLINE:** No participation, organization statement if needed

10-Minute Decision Process

For GREEN Level (Routine)

- **Decision Maker:** Media Team Lead
- **Response Time:** 10 minutes
- **Approval Required:** None (use pre-approved messaging)

For YELLOW Level (Moderate Risk)

- **Decision Maker:** Media Team + Incident Coordinator
- **Response Time:** 15 minutes
- **Approval Required:** Incident Coordinator sign-off

For RED Level (High Risk)

- **Decision Maker:** Media Team + Executive
- **Response Time:** 20 minutes maximum
- **Approval Required:** CEO or designated executive

Rapid Response Toolkit

Pre-Approved Holding Statements (Use Immediately)

1. **Technical Issue Response:** "We are currently addressing a technical issue affecting some of our systems. Safety remains our top priority, and we are working to resolve this matter promptly. We will provide updates as appropriate."
2. **Operational Disruption Response:** "We are managing an operational situation while maintaining our commitment to safety and service. Our teams are working to minimize any impacts and restore normal operations."
3. **Investigation Response:** "We are investigating the current situation and working with relevant authorities as appropriate. We take these matters seriously and will provide updates when we have confirmed information."

15-Minute Response Templates

PARTICIPATION DECISION TEMPLATE **TO:** Executive/Incident Coordinator **SUBJECT:** URGENT - Media Response Decision Required **DEADLINE:** [Time] (15 minutes)

MEDIA REQUEST: [Outlet] requests [interview/comment] for [story angle] **DEADLINE:** [Reporter's deadline] **RISK LEVEL:** [Green/Yellow/Red] **RECOMMENDATION:** [Participate/Statement Only/Decline] **RATIONALE:** [Brief explanation] **PROPOSED RESPONSE:** [Key messages if participating]

RAPID APPROVAL REQUEST **IF YOU APPROVE:** Reply "APPROVED - [any modifications]" **IF YOU DECLINE:** Reply "DECLINED - [use statement only/no response]" **NO RESPONSE BY [TIME] = AUTOMATIC DECLINE**

Spokesperson Rapid Deployment

15-Minute Spokesperson Preparation

1. **Key Messages (3 points maximum)**

☐ Primary message (what we want them to remember)
☐ Safety/responsibility message
☐ Next steps/resolution message

2. **Anticipated Questions & Responses**

☐ What happened? - [Factual, brief response]
☐ Who's responsible? - [Investigation underway, focus on resolution]
☐ What's the impact? - [Specific impacts, mitigation measures]

3. **Interview Guidelines**

☐ Stay calm and confident
☐ Stick to facts, avoid speculation
☐ Bridge back to key messages
☐ Acknowledge concerns, emphasize safety priority

Emergency Spokesperson Options

1. **PRIMARY:** CEO or designated executive spokesperson
2. **BACKUP:** Communications Director
3. **TECHNICAL:** Operations Manager (for technical questions only)
4. **FALLBACK:** Written statement only if no spokesperson available

Social Media Rapid Response

15-Minute Social Media Assessment

1. **Platform Monitoring**

☐ Check Twitter, Facebook, LinkedIn for mentions
☐ Identify trending hashtags or viral content
☐ Assess volume and tone of social media activity

2. **Response Strategy**

- **ENGAGE:** Respond directly to concerns with facts
- **REDIRECT:** Point to official statement or information
- **MONITOR:** Watch but don't engage if risk of escalation

Social Media Response Templates

- **Acknowledgment:** "We're aware of [situation] and are working to address it. Safety is our priority. Updates: [link]"
- **Correction:** "We want to clarify [misinformation]. The facts are: [brief correction]. More info: [link]"
- **Appreciation:** "Thank you for your patience as we work to resolve [situation]. We appreciate your understanding."

Crisis Interview Do's and Don'ts

DO:

- Stay calm and speak clearly
- Acknowledge the seriousness of the situation
- Emphasize safety as top priority
- Provide specific timelines when possible
- Show empathy for any impacts
- Redirect to positive actions being taken

DON'T:

- Speculate about causes or blame
- Make promises you can't keep
- Get defensive or argumentative
- Provide detailed technical information
- Comment on ongoing investigations
- Make statements beyond your authority

Escalation Triggers for Executive Involvement

IMMEDIATE EXECUTIVE ESCALATION IF:

- National media requesting immediate interview
- Story angle suggests significant reputational damage
- Legal implications of response statements
- Safety incidents with potential liability
- Regulatory or government interest indicated

EXECUTIVE NOTIFICATION (not necessarily involvement):

- Local media coverage with moderate impact
- Social media activity requiring organizational response
- Industry publication coverage
- Stakeholder inquiries about media coverage

Documentation Requirements

Rapid Response Log

- ☐ Time of media request received
- ☐ Reporter name, outlet, deadline given
- ☐ Decision made and decision maker
- ☐ Response provided and time delivered
- ☐ Follow-up requirements identified

Post-Response Assessment

☐ Media coverage analysis
☐ Message effectiveness evaluation
☐ Process improvement recommendations
☐ Stakeholder reaction monitoring

Success Criteria

- Response delivered within reporter's deadline
- Key organizational messages communicated effectively
- No contradictory statements made
- Follow-up plan established if needed
- Crisis escalation prevented or managed

Related Procedures

- Use with: Crisis Communications SOP (for overall strategy)
- Coordinate with: Internal Information Leak Response (if internal source)
- Reference: Public Messaging Templates (for consistent messaging)
- Escalate to: Crisis Decision Authority Matrix (for high-risk decisions)

Internal Information Leak Response Procedures

Purpose

This procedure provides immediate response protocols when internal documents, communications, or information appear in public forums, media, or unauthorized channels. Use when confidential organizational information is discovered outside authorized channels.

When to Use

- Internal emails or memos discovered on public forums
- HR documents or communications leaked to media
- Vendor correspondence appearing in unauthorized locations
- Confidential operational information shared externally
- Employee communications leaked to industry forums

Immediate Response (First 10 minutes)

Step 1: Leak Scope Assessment

1. **Information Identification**

☐ Document specific information that was leaked
☐ Identify classification level (confidential, internal, public)

☐ Assess potential damage or sensitivity

2. **Source Analysis**

☐ Identify where leak was discovered (social media, news, forum)
☐ Note time of discovery vs. estimated leak time
☐ Assess distribution scope and audience reach

3. **Authenticity Verification**

☐ Confirm information is genuine organizational content
☐ Check for potential alterations or fabrications
☐ Verify source documents exist in organizational systems

Step 2: Immediate Containment

1. **Internal Notifications**

☐ Alert Executive team immediately
☐ Notify Legal team for privilege review
☐ Inform IT Security of potential breach

2. **External Monitoring**

☐ Monitor for additional leaked information
☐ Track social media spread and commentary
☐ Identify media outlets picking up the story

3. **Documentation**

☐ Screenshot or preserve evidence of leak
☐ Document discovery timeline and circumstances
☐ Begin chain of custody for evidence

Investigation Phase (10-30 minutes)

Internal Investigation Coordination

1. **Access Review**

☐ Identify who had access to leaked information
☐ Review recent document sharing or email forwarding
☐ Check system access logs for unusual activity

2. **Communication Chain Analysis**

☐ Trace email distribution lists and recipients
☐ Review meeting attendees who received information
☐ Identify external parties with legitimate access

3. **System Security Check**

☐ Coordinate with IT to check for system compromise
☐ Review email security and external forwarding rules

☐ Assess if leak resulted from cyber incident vs. human error

Damage Assessment

1. **Content Analysis**

☐ Assess competitive sensitivity of leaked information
☐ Evaluate legal or regulatory implications
☐ Consider reputational damage potential

2. **Stakeholder Impact**

☐ Identify affected customers, partners, or vendors
☐ Assess impact on ongoing negotiations or relationships
☐ Consider employee morale and trust implications

Response Strategy Development (20-45 minutes)

Response Option Analysis

1. **NO RESPONSE STRATEGY**

- **When appropriate:** Low-sensitivity information, limited distribution
- **Risks:** May appear to confirm authenticity
- **Benefits:** Avoids drawing additional attention

2. **CLARIFICATION STRATEGY**

- **When appropriate:** Information is taken out of context
- **Response:** Provide context without confirming specific details
- **Example:** "Recent reports mischaracterize our normal operational discussions"

3. **CORRECTION STRATEGY**

- **When appropriate:** Information is inaccurate or misleading
- **Response:** Correct misinformation while minimizing leak confirmation
- **Example:** "Reports contain inaccuracies about our operational procedures"

4. **ACKNOWLEDGMENT STRATEGY**

- **When appropriate:** High-profile leak requiring direct response
- **Response:** Acknowledge situation while emphasizing investigation
- **Example:** "We are investigating unauthorized disclosure of internal communications"

Message Development Framework

1. **Core Messages (Maximum 3 points)**

- **Primary:** We take information security seriously
- **Secondary:** We are investigating the source and circumstances

- **Tertiary:** This does not affect our operational capabilities/commitments

2. **Supporting Messages**

- Emphasize normal business operations continuing
- Highlight organizational commitment to transparency where appropriate
- Reinforce stakeholder relationship commitments

Communication Protocols

Internal Communications

1. **To All Staff (within 2 hours if leak is public)** "We are aware of unauthorized disclosure of internal communications. We are investigating how this occurred and will take appropriate action. Please refer any media inquiries to [communications team contact]."
2. **To Executive Team** "Information leak confirmed: [brief description]. Response strategy: [selected approach]. Legal review: [in progress/complete]. Estimated timeline for resolution: [estimate]."
3. **To Legal Team** "Internal information leaked: [description]. Potential legal implications: [assessment]. Privilege review needed for: [specific items]. Investigation coordination required."

External Communications

1. **Standard Holding Statement** "We are investigating reports of unauthorized disclosure of internal communications. We take information security seriously and will take appropriate action based on our investigation findings."
2. **Clarification Statement (if misinformation present)** "Recent reports mischaracterize routine operational discussions. We remain committed to [relevant organizational commitments] and continue normal operations."
3. **Investigation Statement (for serious breaches)** "We are conducting a thorough investigation into unauthorized disclosure of internal communications. We have engaged appropriate specialists and will take all necessary steps to prevent future incidents."

Media Inquiry Response Protocols

Standard Media Response Process

1. **Acknowledge Receipt** (within 1 hour) "We have received your inquiry and are reviewing the matter. We will respond by [specific time]."
2. **Assessment Questions for Reporter**

- What specific information are you referring to?

- Where did you obtain this information?
- What is your publication timeline?
- What other sources are you consulting?

3. **Response Delivery**

- Use pre-approved response strategy
- Stick to key messages
- Avoid confirming specific details
- Offer background briefing if appropriate

Escalation Triggers for Executive Involvement

- National media interest
- Legal proceedings threatened or initiated
- Regulatory agency inquiries
- Significant stakeholder concerns raised
- Employee or union relations implications

Legal Coordination Requirements

Immediate Legal Review (within 30 minutes)

☐ Privilege implications of leaked communications
☐ Potential defamation or privacy law violations
☐ Employment law implications if employee involved
☐ Contract confidentiality clause violations

Investigation Coordination

☐ Coordinate with HR for employee-related investigations
☐ Consider law enforcement involvement for criminal activity
☐ Preserve evidence for potential legal proceedings
☐ Document investigation process for legal protection

Recovery and Prevention

Short-term Recovery Actions

1. **Stakeholder Communication**

☐ Contact affected partners or customers directly
☐ Provide reassurance about ongoing commitments
☐ Offer additional briefings if relationship-critical

2. **Employee Communication**

☐ Address concerns about information security
☐ Reinforce confidentiality policies and training
☐ Provide clear reporting channels for concerns

Long-term Prevention Measures

1. **Information Security Review**

☐ Review document classification and handling procedures
☐ Assess email security and external sharing controls
☐ Consider additional training or technology solutions

2. **Communication Protocol Updates**

☐ Review what information should be documented in writing
☐ Update confidentiality markings and warnings
☐ Revise distribution list management procedures

Success Criteria

- Rapid identification and assessment of leaked information
- Appropriate response strategy implemented effectively
- Damage to organizational reputation minimized
- Stakeholder relationships maintained or restored
- Prevention measures implemented to reduce future risk

Related Procedures

- Use with: Crisis Communications SOP (for overall strategy)
- Coordinate with: Rapid Response Media Protocol (for urgent deadlines)
- Reference: Legal Risk Escalation Flowchart (for legal implications)
- Escalate to: Crisis Decision Authority Matrix (for high-impact decisions)

Owner: Media & Communications Lead
Reference: MED-01
Version: 1.0
Approved by: Executive Communications and Legal Team