SOUTHGATE TERMINAL

Port Operations Security Documentation

ADDITION TO: Crisis Communications SOP.docx

INSERT LOCATION: Add as new section after existing crisis communication procedures

SECTION TITLE: Internal Information Leak Response Procedures

Internal Information Leak Response Procedures

Purpose

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

When to Use

- Internal emails or memos discovered on public forums
- HR documents or communications leaked to media
- Vendor correspondence appearing in unauthorised 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 organisational content
☐ Check for potential alterations or fabrications
☐ Verify source documents exist in organisational 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 minimising 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**

- Emphasise normal business operations continuing
- Highlight organisational 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 organisational 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 organisational reputation minimised
- 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)