Contents

SOUTHGATE TERMINAL

## Port Operations Security Documentation

Legal / Compliance – Insurance Communications Template

Purpose:
To guide the Legal team in preparing and sending communications to insurers in the event of a potential incident or claim. This template ensures clarity, compliance with policy terms, and protects the organisation's position in the event of a formal claim or investigation.

Insurance Clause Interpretation Guide

Purpose

This guide provides framework for interpreting key insurance policy clauses during cyber incidents, helping determine coverage applicability and required notifications. Use when incident characteristics may trigger specific policy provisions.

Key Policy Clauses and Interpretations

Clause 4.7: Data Inaccuracy and Operational Disruption **Policy Language:** "Coverage applies to losses resulting from data inaccuracy affecting operational systems, provided such inaccuracy results from covered cyber events."

Interpretation Framework: 1. **Data Inaccuracy Defined:** - AIS vessel position errors or missing data - Navigation system discrepancies - Operational system displaying incorrect information

2. **Operational Disruption Defined:**

- Container movement delays or errors
- Manual override requirements
- Reduced operational capacity

3. **Covered Cyber Events:**

- Unauthorized system access
- External interference with systems
- System manipulation by unauthorized parties

Application to Current Scenarios: - **AIS Anomalies (INJ002A, INJ005A):** Likely covered if external interference suspected - **Container Misrouting (INJ010B):** Covered if system manipulation confirmed - **System Configuration Changes (INJ006A):** Covered if unauthorized access proven

Clause 7.4: Cyber Attack with Systemic Risk **Policy Language:** "Enhanced coverage provisions apply when cyber attacks create systemic operational risk affecting multiple operational systems."

Interpretation Framework: 1. **Cyber Attack Defined:** - Deliberate unauthorized access - System manipulation with malicious intent - Coordinated interference with multiple systems

2. **Systemic Risk Defined:**

- Multiple operational systems affected
- Cross-system dependencies compromised
- Overall operational capability threatened

3. **Enhanced Coverage Provisions:**

- Higher coverage limits
- Reduced deductibles
- Extended business interruption coverage

Application to Current Scenarios: - **Multi-System Failures:** If network, AIS, and CCTV all affected by same incident - **Coordinated Attacks:** Evidence of deliberate multi-system targeting - **Persistent Access:** Ongoing unauthorized access affecting multiple systems

Clause 12.3: Vendor System Integration **Policy Language:** "Coverage extends to losses arising from cyber events affecting integrated vendor systems, subject to vendor cooperation requirements."

Interpretation Framework: 1. **Integrated Vendor Systems:** - Network infrastructure provided by vendors - AIS systems with vendor components - Any operational system with vendor access

2. **Vendor Cooperation Requirements:**

- Vendor must provide system logs and analysis
- Vendor must cooperate with incident investigation
- Vendor liability limitations must be documented

Application to Current Scenarios: - **Network Issues (INJ001A, INJ001B):** If vendor-provided network infrastructure involved - **Vendor Email Leaks (INJ004E):** Coverage for vendor-related information exposure - **Vendor Payment Delays (INJ004C):** Coverage implications for vendor relationship impacts

Coverage Determination Process

Step 1: Incident Characterization (10 minutes)

1. **Technical Assessment**

☐ Document specific systems affected
☐ Identify evidence of unauthorized access
☐ Assess cross-system impact patterns

2. **Operational Impact Assessment**

☐ Quantify operational disruption
☐ Document data inaccuracy instances
☐ Calculate business interruption costs

3. **Vendor Involvement Analysis**

☐ Identify vendor systems involved
☐ Assess vendor cooperation availability
☐ Document vendor liability positions

Step 2: Clause Applicability Analysis (15 minutes)

1. **Clause 4.7 Assessment**

- **Triggered if:** Data inaccuracy + operational disruption + cyber event evidence
- **Evidence needed:** System logs, operational records, technical analysis
- **Coverage level:** Standard operational disruption coverage

2. **Clause 7.4 Assessment**

- **Triggered if:** Cyber attack + systemic risk + multiple systems
- **Evidence needed:** Attack attribution, cross-system analysis, risk assessment
- **Coverage level:** Enhanced coverage with reduced deductibles

3. **Clause 12.3 Assessment**
   - **Triggered if:** Vendor system involvement + integration confirmed
   - **Evidence needed:** Vendor system logs, cooperation confirmation
   - **Coverage level:** Extended to vendor-related losses

Step 3: Coverage Decision Matrix **SCENARIO 1: Single System, Clear Technical Cause** - **Primary Clause:** Clause 4.7 (if data inaccuracy present) - **Coverage Level:** Standard - **Notification Priority:** Standard (24-48 hours)

SCENARIO 2: Multiple Systems, Suspected Cyber Attack - **Primary Clause:** Clause 7.4 (systemic risk) - **Coverage Level:** Enhanced - **Notification Priority:** Urgent (immediate to 24 hours)

SCENARIO 3: Vendor Systems Involved - **Primary Clause:** Clause 12.3 + applicable operational clause - **Coverage Level:** Extended vendor coverage - **Notification Priority:** Standard (coordinate with vendor)

Insurance Notification Templates

Standard Notification (Clause 4.7) **TO:** [Insurance Representative] **SUBJECT:** Incident Notification - Clause 4.7 Potential Coverage **PRIORITY:** Standard

INCIDENT SUMMARY: [Brief description] **SYSTEMS AFFECTED:** [List with operational impact] **DATA INACCURACY IDENTIFIED:** [Specific examples] **CYBER EVENT EVIDENCE:** [Security assessment summary] **PRELIMINARY LOSS ASSESSMENT:** [Initial estimates] **ADDITIONAL INFORMATION:** Available upon request

Enhanced Notification (Clause 7.4) **TO:** [Insurance Representative] **SUBJECT:** URGENT - Systemic Cyber Event Notification **PRIORITY:** Urgent

INCIDENT SUMMARY: [Brief description] **SYSTEMIC RISK FACTORS:** [Multi-system impacts] **CYBER ATTACK INDICATORS:** [Evidence of deliberate action] **OPERATIONAL DISRUPTION SCOPE:** [Full impact assessment] **ENHANCED COVERAGE REQUEST:** Under Clause 7.4 provisions **IMMEDIATE ASSISTANCE NEEDED:** [Specific support requirements]

Vendor Integration Notification (Clause 12.3) **TO:** [Insurance Representative] **SUBJECT:** Vendor System Integration Incident - Clause 12.3 **PRIORITY:** Standard

INCIDENT SUMMARY: [Brief description] **VENDOR SYSTEMS INVOLVED:** [List with integration details] **VENDOR COOPERATION STATUS:** [Confirmed/pending/declined] **INTEGRATION IMPACT:** [How vendor systems affected operations] **EXTENDED COVERAGE REQUEST:** Under vendor integration provisions **VENDOR COORDINATION:** [Current status and needs]

Decision Factors for Coverage Classification

Factors Supporting Clause 7.4 (Enhanced Coverage):

☐ Three or more operational systems affected
☐ Evidence of coordinated or deliberate attack
☐ Significant business interruption (>4 hours)
☐ Cross-system dependencies exploited
☐ Public safety or security implications

Factors Supporting Standard Coverage:

☐ Single system or limited scope impact
☐ Technical malfunction with cyber elements
☐ Limited operational disruption
☐ Clear resolution timeline available

Factors Requiring Vendor Clause Application:

☐ Vendor-provided systems central to incident
☐ Vendor access rights potentially exploited
☐ Vendor cooperation essential for investigation
☐ Vendor liability questions affecting coverage

Documentation Requirements for Insurance Claims

Immediate Documentation (Within 4 hours):

☐ Incident timeline with specific timestamps
☐ System logs and security event records
☐ Operational impact documentation
☐ Initial technical assessment

Detailed Documentation (Within 24 hours):

☐ Comprehensive technical analysis
☐ Business interruption calculation
☐ Vendor involvement assessment
☐ Legal and regulatory implications analysis

Ongoing Documentation:

☐ Daily incident updates
☐ Recovery cost tracking
☐ External expert reports

☐ Regulatory correspondence

Success Criteria

- Accurate determination of applicable insurance clauses
- Timely notification to insurance providers
- Proper documentation for claim substantiation
- Maximum coverage obtained under policy terms

Related Procedures

- Use with: Breach Classification Decision Tree (for incident categorization)
- Coordinate with: Legal Risk Escalation Flowchart
- Reference: Legal Precedent Summary Sheet (for coverage disputes)
- Escalate to: Crisis Decision Authority Matrix (for coverage strategy decisions)

When to Use

- There is a confirmed or suspected security, operational, or compliance incident
- The organisation's insurance policy requires notification of potential claims or risks
- Insurer inquiry or policy-related questions have been received

Before Sending

Ensure the following have been reviewed:

- Active insurance policy (e.g. cyber, business continuity, professional indemnity)
- Policy notification requirements and timeframes
- Any prior communications with the insurer regarding the incident
- Legal review of drafted content

Template Structure

Subject: Notification of Potential Incident – [Organisation Name]

To: [Insurer Contact Name / Claims Department Email]
From: [Legal Contact Name, Title]
Date: [Insert Date]

Body:

Dear [Insurer Contact],

We are writing to notify you of a potential incident that may fall within the coverage of our policy #[Policy Number] held with your organisation.

Summary of Incident:

- Description of the event (brief and factual)
- Date/time of occurrence or detection
- Systems, services, or stakeholders potentially impacted

Initial Actions Taken:

- Description of internal response measures (containment, investigation, notifications)
- Involvement of any external legal, technical, or forensic advisers

Current Status:

- Whether the issue is ongoing, contained, or under investigation
- Any known financial, reputational, or operational consequences

Request:
We are providing this notice in accordance with our policy obligations and welcome any direction from your office regarding next steps, documentation, or support required.

Please confirm receipt and advise if further details are required at this stage. We will continue to keep you informed as the situation evolves.

Kind regards,

[Full Name]
[Role / Title]
[Organisation Name]
[Contact Details]

Optional Attachments

- Incident summary memo (internal)
- Technical timeline or logs (if available)
- Draft or issued media statements (if applicable)
- Risk register reference or legal opinion (if escalated internally)

Reminders

- Avoid speculative language. Clearly mark estimates or assumptions.
- Avoid admitting liability or fault.

- All communications should be logged in the legal incident register.

Owner: Legal / Compliance Lead
Reference: LEG-03
Version: 1.0
Approved by: Risk & Legal Steering Group