Contents

SOUTHGATE TERMINAL

Port Operations Security Documentation

Legal / Compliance – Breach Disclosure Checklist

Purpose:
To guide Legal teams in identifying whether a data or system security incident meets the threshold for disclosure under organisational policy, legal obligations, or insurer requirements. This checklist ensures timely, accurate, and compliant handling of potential breaches.

Breach Classification Decision Tree

Purpose

This decision tree provides systematic classification of security incidents to determine appropriate legal responses, notification requirements, and regulatory obligations. Use this before proceeding with any breach disclosure process.

Classification Categories

CATEGORY 1: Technical Anomaly (No breach classification)

- System glitches or configuration errors
- No evidence of unauthorized access
- No data exposure or system compromise
- Standard operational procedures sufficient

CATEGORY 2: Security Incident (Internal review required)

- Suspicious activity detected but contained
- Potential unauthorized access attempts
- System integrity questions but no confirmed compromise
- Enhanced monitoring and investigation needed

CATEGORY 3: Confirmed Breach (Regulatory review required)

- Confirmed unauthorized access to systems
- Evidence of data exposure or system manipulation
- Operational impact from security compromise
- Formal breach protocols and notifications required

CATEGORY 4: Persistent Unauthorized Access (Immediate escalation)

- Evidence of ongoing unauthorized system access
- Installation of unauthorized scripts or programs
- Lateral movement between systems
- Advanced persistent threat characteristics

Decision Tree Process

Step 1: Initial Evidence Assessment (5 minutes) **Question 1:** Is there evidence of unauthorized access to systems? - **NO** - Proceed to Technical Anomaly Assessment - **YES** - Proceed to Step 2

Question 2: Is there evidence of data exposure or system modification? - **NO** - Classify as Security Incident (Category 2) - **YES** - Proceed to Step 3

Question 3: Is there evidence of persistent or ongoing unauthorized access? - **NO** - Classify as Confirmed Breach (Category 3) - **YES** - Classify as Persistent Access (Category 4)

Step 2: Technical Anomaly Assessment **Indicators suggesting Category 1:** - [ ] System logs show configuration errors - [ ] Network issues correlate with maintenance activities - [ ] No authentication failures or unauthorized commands - [ ] Vendor systems involved with known issues

If ANY of these are present, escalate to Category 2: - [ ] Unusual timing of technical issues - [ ] Multiple systems affected simultaneously - [ ] External connections or traffic patterns - [ ] Administrative access during non-business hours

Step 3: Persistent Access Evaluation Indicators of Category 4 (Persistent Access): - [ ] Unauthorized cron jobs or scheduled tasks detected - [ ] Evidence of lateral movement between systems - [ ] Creation of unauthorized user accounts or privileges - [ ] Installation of unauthorized software or scripts - [ ] Log deletion or tampering evidence - [ ] Command execution outside normal parameters

Legal Classification Criteria

Category 1: Technical Anomaly Legal Obligations: - Internal documentation only - No external notifications required - Standard incident response procedures

Regulatory Requirements: - None (unless pattern develops)

Category 2: Security Incident Legal Obligations: - Internal legal review required - Consider preliminary insurance notification - Enhanced documentation requirements

Regulatory Requirements: - Monitor for escalation to reportable event - Prepare for potential future notifications

Category 3: Confirmed Breach Legal Obligations: - Formal legal assessment required - Insurance notification mandatory - Board/executive notification required - Consider external legal counsel

Regulatory Requirements: - Assess notification obligations under Cybersecurity Act - Consider Maritime Security Authority notification - Evaluate customer/partner notification requirements

Category 4: Persistent Unauthorized Access Legal Obligations: - Immediate executive escalation - External legal counsel engagement - Law enforcement consideration - Full insurance claim preparation

Regulatory Requirements: - Mandatory Cybersecurity Act notification (24-72 hours) - Maritime Security Authority immediate notification - Consider national security implications

Notification Timeline Requirements

Category 1: Technical Anomaly

- **Internal:** Document in incident log
- **Legal:** No specific timeline
- **Regulatory:** None required

Category 2: Security Incident

- **Internal:** Notify legal team within 4 hours
- **Legal:** Preliminary insurance contact within 24 hours
- **Regulatory:** Monitor for 72 hours for escalation

Category 3: Confirmed Breach

- **Internal:** Executive notification within 2 hours
- **Legal:** Full legal assessment within 8 hours
- **Insurance:** Formal notification within 24 hours
- **Regulatory:** Assessment complete within 24 hours, notifications within 72 hours

Category 4: Persistent Unauthorized Access

- **Internal:** Immediate executive notification
- **Legal:** External counsel within 4 hours
- **Insurance:** Immediate notification
- **Regulatory:** Notification within 24 hours (Cybersecurity Act)
- **Law Enforcement:** Consider immediate contact

Evidence Preservation Requirements

For All Categories 2-4:

- ☐ Preserve all system logs immediately
- ☐ Document timeline of events
- ☐ Secure affected systems from further access
- ☐ Photograph or screenshot evidence
- ☐ Maintain chain of custody for digital evidence

Additional for Categories 3-4:

- ☐ Engage forensic specialists if available
- ☐ Create bit-for-bit copies of affected systems
- ☐ Document all investigative actions
- ☐ Prepare for potential law enforcement involvement

Cross-Reference with Specific Incidents

Unauthorized Cron Jobs (INJ016A, INJ017A)

- **Initial Classification:** Category 2 (Security Incident)
- **Escalate to Category 4 if:** Evidence of system manipulation or ongoing access
- **Key Evidence:** Purpose of script, authorization for installation, system impact

Log Deletion (INJ016B)

- **Initial Classification:** Category 3 (Confirmed Breach)
- **Escalate to Category 4 if:** Systematic deletion or ongoing tampering
- **Key Evidence:** What logs deleted, timing, method of deletion

Authentication Failures (INJ008A)

- **Initial Classification:** Category 2 (Security Incident)
- **Escalate to Category 3 if:** Successful unauthorized access confirmed
- **Key Evidence:** Number of attempts, source, success rate

System Configuration Changes (INJ006A)

- **Initial Classification:** Category 2 (Security Incident)
- **Escalate to Category 3 if:** Unauthorized modifications confirmed
- **Key Evidence:** Nature of changes, authorization, operational impact

Decision Documentation Template

INCIDENT ID: [Unique identifier] **DATE/TIME:** [Classification decision time] **DECISION MAKER:** [Name and role] **CLASSIFICATION:** [Category 1-4]

EVIDENCE SUMMARY: - Primary indicators: [List key evidence] - Supporting factors: [Additional considerations] - Exclusionary factors: [Evidence against higher classification]

RATIONALE: [Brief explanation of classification decision]

REQUIRED ACTIONS: - [ ] Legal notifications: [Timeline and recipients] - [ ] Regulatory requirements: [Specific obligations] - [ ] Evidence preservation: [Specific requirements] - [ ] Escalation triggers: [Conditions for reclassification]

REVIEW TIMELINE: [When to reassess classification]

Success Criteria

- Accurate classification based on available evidence
- Appropriate legal and regulatory responses initiated
- Proper evidence preservation protocols followed
- Clear documentation for future reference and audit

Related Procedures

- Use with: Insurance Communications Template (for Categories 3-4)
- Coordinate with: Legal Risk Escalation Flowchart
- Reference: Post-Breach Reform Guidance (for Category 4)

- Escalate to: Crisis Decision Authority Matrix (for executive decisions)

When to Use This Checklist

- A security incident has affected operations, data, systems, or third-party assets
- Legal has been alerted to anomalies or external attention (e.g. media inquiry, insurer request)
- Unauthorised access, loss of control, or data/system integrity compromise is suspected

Step 1: Confirm Potential Breach Indicators

Tick all that apply:

- Unauthorised access attempt or credential misuse detected
- Suspicious cron job, file modification, or system persistence mechanism found
- Customer, shipment, or system data was manipulated or misrouted
- Communications or dashboards displayed false or manipulated information
- External party alerted or notified the organisation first
- Insurance contact or regulator has formally inquired about status

If **two or more indicators are present**, initiate **Step 2**.

Step 2: Assess Disclosure Requirements

- **Internal Policy** – Does this meet internal breach notification thresholds?
- **Regulatory Duty** – Are we legally obligated to notify any regulatory body?
- **Contractual Obligation** – Do any active agreements require disclosure (e.g. vendors, insurers)?
- **Reputational Risk** – Would failure to disclose damage stakeholder trust?

Document basis for each answer using:

- Legal Risk Escalation Flowchart
- Insurance Communications Template
- Breach Policy Register (if applicable)

If **any requirement is met**, proceed to **Step 3**.

Step 3: Prepare Disclosure Packet

- Draft breach summary (use: Breach Notification Template)
- Attach validated timeline/log artefacts from Technical and Coordinator
- Confirm insurer contact procedure (see Insurance Comms Template)
- Cross-check any draft statement with Media/Executive
- Classify incident per Risk Register (e.g. Class B, Class A)
- Identify named spokesperson and legal point of contact

Step 4: Submit and Record

- Send formal notification via approved channels (email or form submission)
- Archive all communication threads related to the breach
- Ensure incident is tagged for legal review during post-incident debrief
- If regulator or insurer response is pending, assign owner to track response timeframe

Additional Notes

- Do not delay disclosure solely for reputational reasons if legal/contractual thresholds are met
- Always label preliminary findings as “subject to verification”
- If unsure, escalate using Legal Risk Escalation Flowchart for joint Executive review

Owner: Legal / Compliance Lead
Reference: LEG-01
Version: 1.0
Approved by: Risk & Legal Steering Group