SOUTHGATE TERMINAL

Port Operations Security Documentation

ADDITION TO: Legal Risk Escalation Flowchart.docx

INSERT LOCATION: Add as new section after existing escalation procedures

SECTION TITLE: Regulatory Timeline Compliance Tracker

Regulatory Timeline Compliance Tracker

Purpose

This tracker provides systematic management of overlapping regulatory notification requirements and deadlines during cyber incidents, ensuring compliance with all applicable laws and regulations. Use when multiple regulatory bodies may have notification or reporting requirements.

Key Regulatory Frameworks

Cybersecurity Act (Federal) **Scope:** Incidents affecting critical infrastructure or cybersecurity **Notification Requirements:** - **Initial Notification:** 24 hours for confirmed breaches - **Detailed Report:** 72 hours for comprehensive incident analysis - **Follow-up Reports:** As required during investigation

Triggers: - Unauthorised access to critical systems - Evidence of persistent unauthorised access - Data exposure affecting operations - Cyber attacks affecting multiple systems

Maritime Security Authority (MSA) **Scope:** Incidents affecting port operations or maritime safety **Notification Requirements:** - **Immediate:** Safety-critical incidents affecting operations - **24 Hours:** Operational disruptions affecting shipping - **48 Hours:** Security incidents with potential maritime implications

Triggers: - AIS system failures affecting vessel tracking - CCTV blackouts affecting safety monitoring - Container movement disruptions - Port operational capacity reductions

Privacy and Information Commissioner (PIC) **Scope:** Personal data breaches or privacy violations **Notification Requirements:** - **72 Hours:** Personal data breaches - **30 Days:** Privacy impact assessments

Triggers: - Access to employee personal information - Customer or vendor data exposure - HR system compromises

WorkSafe Authority **Scope:** Workplace safety incidents **Notification Requirements:** - **Immediate:** Serious injury or safety incidents - **24 Hours:** Workplace hazard notifications - **7 Days:** Safety management system failures

Triggers: - Manual operations creating safety risks - Equipment malfunctions affecting worker safety - CCTV failures affecting safety monitoring

Multi-Jurisdiction Compliance Matrix

Incident Type: Confirmed Cyber Breach

Regulatory Body	Timeline	Requirements	Priority
Cybersecurity Act	24 hours	Initial notification	HIGH
MSA	24 hours	If operational impact	MEDIUM
PIC	72 hours	If personal data affected	HIGH
WorkSafe	24 hours	If safety implications	MEDIUM

Incident Type: AIS System Failure

Regulatory Body	Timeline	Requirements	Priority
MSA	Immediate	Safety-critical notification	CRITICAL
Cybersecurity Act	24 hours	If cyber cause confirmed	HIGH
WorkSafe	24 hours	If manual operations risk	MEDIUM

Incident Type: Multi-System Compromise

Regulatory Body	Timeline	Requirements	Priority
Cybersecurity Act	24 hours	Critical infrastructure impact	CRITICAL
MSA	Immediate	Port operations affected	CRITICAL
PIC	72 hours	If data systems compromised	HIGH
WorkSafe	24 hours	Safety system impacts	HIGH

Timeline Management Process

Hour 0-4: Initial Assessment and Immediate Notifications

1. **Immediate Safety Notifications**

☐ MSA if vessel safety affected

☐ WorkSafe if worker safety at risk
☐ Coast Guard if maritime emergency

2. **Initial Legal Assessment**

☐ Determine applicable regulatory frameworks
☐ Identify potential notification triggers
☐ Assess preliminary timeline requirements

3. **Evidence Preservation**

☐ Preserve all relevant documentation
☐ Begin regulatory compliance log
☐ Assign regulatory compliance coordinator

Hour 4-12: Detailed Analysis and Preparation

1. **Comprehensive Regulatory Review**

☐ Complete regulatory applicability analysis
☐ Prepare preliminary notification drafts
☐ Coordinate with technical teams for evidence

2. **Timeline Coordination**

☐ Map all applicable deadlines
☐ Identify deadline conflicts or overlaps
☐ Prioritise notifications by criticality

3. **Internal Coordination**

☐ Brief executive team on compliance requirements
☐ Coordinate with technical teams for technical details
☐ Align with legal strategy and messaging

Hour 12-24: Primary Notifications

1. **Critical 24-Hour Notifications**

☐ Cybersecurity Act (if applicable)
☐ MSA operational impact notifications
☐ WorkSafe safety incident reports

2. **Notification Coordination**

☐ Ensure consistent messaging across agencies
☐ Coordinate timing to avoid conflicts
☐ Document all submissions and responses

Hour 24-72: Secondary Notifications and Follow-ups

1. **72-Hour Notifications**

☐ PIC privacy breach notifications
☐ Cybersecurity Act detailed reports
☐ MSA comprehensive incident reports

2. **Follow-up Requirements**

☐ Response to regulatory inquiries
☐ Additional information requests
☐ Ongoing compliance monitoring

Regulatory Notification Templates

Cybersecurity Act Initial Notification **TO:** National Cybersecurity Centre **SUBJECT:** Critical Infrastructure Cyber Incident - Initial Notification **TIMELINE:** Within 24 hours of confirmation

INCIDENT SUMMARY: [Brief technical description] **SYSTEMS AFFECTED:** [Critical infrastructure systems impacted] **PRELIMINARY ASSESSMENT:** [Initial scope and impact] **ONGOING ACTIONS:** [Response measures implemented] **CONTACT INFORMATION:** [Designated incident coordinator] **FOLLOW-UP TIMELINE:** [Expected detailed report timing]

Maritime Security Authority Notification **TO:** MSA Incident Response Team **SUBJECT:** Port Operational Incident - Safety Notification **TIMELINE:** Immediate for safety issues, 24 hours for operational

INCIDENT TYPE: [Safety/Security/Operational] **LOCATION:** [Specific port areas affected] **OPERATIONAL IMPACT:** [Specific impacts on maritime operations] **SAFETY MEASURES:** [Immediate safety actions taken] **VESSEL IMPACTS:** [Effects on vessel operations or safety] **RESTORATION TIMELINE:** [Expected resolution timeframe]

Privacy Commissioner Notification **TO:** Privacy and Information Commissioner **SUBJECT:** Personal Data Breach Notification **TIMELINE:** Within 72 hours

BREACH DESCRIPTION: [Nature of personal data involved] **INDIVIDUALS AFFECTED:** [Number and categories of individuals] **DATA CATEGORIES:** [Types of personal information exposed] **RISK ASSESSMENT:** [Likelihood and severity of harm] **MITIGATION MEASURES:** [Steps taken to address breach] **PREVENTION MEASURES:** [Actions to prevent recurrence]

Compliance Monitoring Dashboard

Current Notification Status

Regulatory Body	Deadline	Status	Responsible	Notes
Cybersecurity Act	[Date/Time]	[Pending/Submitted/Complete]	[Name]	[Comments]
MSA	[Date/Time]	[Pending/Submitted/Complete]	[Name]	[Comments]
PIC	[Date/Time]	[Pending/Submitted/Complete]	[Name]	[Comments]
WorkSafe	[Date/Time]	[Pending/Submitted/Complete]	[Name]	[Comments]

Escalation Triggers

- **RED:** Deadline within 4 hours and notification not submitted
- **YELLOW:** Deadline within 12 hours and preparation not complete
- **GREEN:** On track for compliance with adequate preparation time

Cross-Reference with Specific Incidents

Network Issues (INJ001A, INJ001B)

- **Primary:** Cybersecurity Act if cyber cause confirmed
- **Secondary:** MSA if operational impact significant
- **Timeline:** 24 hours for both

AIS Anomalies (INJ002A, INJ005A, INJ007B)

- **Primary:** MSA immediate notification for vessel safety
- **Secondary:** Cybersecurity Act if external interference confirmed
- **Timeline:** Immediate for MSA, 24 hours for Cybersecurity Act

CCTV Failures (INJ003A, INJ003B, INJ003F)

- **Primary:** WorkSafe for safety monitoring failure
- **Secondary:** MSA if vessel safety affected
- **Timeline:** 24 hours for WorkSafe, immediate if vessel safety

Log Deletion (INJ016B)

- **Primary:** Cybersecurity Act for evidence tampering
- **Secondary:** PIC if personal data logs affected
- **Timeline:** 24 hours for Cybersecurity Act, 72 hours for PIC

Unauthorised Access (INJ016A, INJ017A)

- **Primary:** Cybersecurity Act for persistent access
- **Secondary:** All others depending on system impact
- **Timeline:** 24 hours initial, varying for detailed reports

Success Criteria

- All applicable regulatory notifications submitted within required timeframes
- Consistent messaging across regulatory submissions
- Proper documentation of all compliance activities
- Effective coordination between technical, legal, and regulatory requirements
- No regulatory penalties or compliance violations

Related Procedures

- Use with: Breach Classification Decision Tree (for notification triggers)
- Coordinate with: Insurance Clause Interpretation Guide (for coverage coordination)
- Reference: Legal Precedent Summary Sheet (for regulatory strategy)
- Escalate to: Crisis Decision Authority Matrix (for approval decisions)