**Technical / Ops Procedures – Downtime Impact Estimator**

**Purpose:**  
To provide a structured framework for estimating the operational and business impact of system or service outages during an incident. This helps inform crisis decisions, stakeholder communication, and post-event cost review.

**When to Use**

• During an incident with disruption to planning, scheduling, or physical ops systems  
• Following a failed service restart or manual override  
• Before stakeholder or executive updates involving impact scale

**Step 1: Identify Impacted Systems**

• Tick all that apply and add estimated disruption:

* AIS Feed → ☐ Disruption: \_\_\_ mins
* GPS Service → ☐ Disruption: \_\_\_ mins
* Container Scheduler → ☐ Disruption: \_\_\_ mins
* Crane Feedback Link → ☐ Disruption: \_\_\_ mins
* Berth Planner Tool → ☐ Disruption: \_\_\_ mins
* CCTV/Perimeter Feed → ☐ Disruption: \_\_\_ mins

**Step 2: Estimate Operational Effects**

• Delayed ship arrivals or departures? \_\_\_ ships delayed (ETA impact: \_\_\_ mins)  
• Containers not moved or misrouted? \_\_\_ total affected  
• Manual crane lifts required? \_\_\_ (estimate)  
• Missed manifest window / customs errors? ☐ Yes ☐ No  
• Unplanned overtime or shift disruption? ☐ Yes ☐ No

**Step 3: Estimate Financial & Business Risk**

• Daily operational throughput loss (if applicable): AU$ \_\_\_\_\_\_\_\_  
• Downtime period cost multiplier (labour, fuel, port fees): ☐ Mild ☐ Moderate ☐ High  
• Reputational flags:

* Delayed customer shipment
* Missed KPI with shipping partner
* News/media escalation risk

**Step 4: Confidence & Communication Flag**

• Confidence in estimates:

* ☐ Low (very limited visibility)
* ☐ Medium (based on partial logs or Ops feedback)
* ☐ High (corroborated across systems and teams)

• Communication ready for:

* ☐ Executive Brief
* ☐ Legal Hold / Review
* ☐ Public Messaging Draft

**Notes / Additional Context:**  
(Add any specific causes, patterns, or technical constraints that shaped the estimate.)

**Owner:** Ops Lead  
**Reference:** TECH-09  
**Version:** 1.0  
**Approved by:** Cyber-Ops Coordination Cell