# Portfall Scenario Summary – All Teams Brief

## Scenario Title: Portfall – Coordinated Maritime Cyber Crisis Simulation

**Duration:** 2 Hours  
**Setting:** Southgate Maritime Terminal, a critical intermodal logistics hub  
**Format:** Real-time team-based simulation with injects, dashboards, decisions, and live media pressure

## Objective

This immersive exercise tests your ability to respond to a rapidly evolving cyber-physical crisis impacting maritime operations. Your team must analyse unfolding events, coordinate responses, communicate under pressure, and make strategic decisions in real time.

You will not be told what to do — you must work it out together, as you would in a real crisis.

## Team Roles (You Will Support One)

* **Executive** – Leadership, strategic decisions, stakeholder response
* **Legal / Compliance** – Liability, breach disclosure, risk framing
* **Media / Comms** – Internal & public messaging, media pressure
* **Technical / Cyber** – Forensic analysis, threat mitigation, system recovery
* **Operations / Logistics** – Container flow, crane management, workforce safety
* **Incident Coordinator** – Scenario-wide logging, coordination, team tracking

Each facilitator supports one team. You will nudge, observe, record decisions, and help pace the experience.

## Scenario Structure: 4 Phases

**Phase 1 – Early Indicators (T+0 to T+30)**  
Initial anomalies emerge. Teams begin detecting signs of trouble but lack full context. This phase tests alertness and initial coordination.

**Phase 2 – Escalation and Uncertainty (T+30 to T+60)**  
More systems fail. Pressure mounts. Stakeholders and media begin demanding answers. Decisions under stress are key.

**Phase 3 – Full Crisis Realised (T+60 to T+90)**  
Operational disruptions peak. Crane failure, morale collapse, system overrides. Teams must coordinate under real-world pressure.

**Phase 4 – Resolution and Accountability (T+90 to T+120)**  
Debrief, public response, final decisions. Teams are judged by how they close the loop: communications, reports, breach disclosure.

## Scenario Mechanics

* **Injects**: Timed events delivered by email, dashboard, or facilitator prompt
* **Dashboards**: AIS, CCTV, Email, and Media interfaces provide live updates
* **Logs & VMs**: Some technical injects require accessing server logs or simulated services
* **Policies**: Teams will be given real policies to interpret and act upon
* **Scoring**: Teams are not told their scores, but each decision affects outcome

## Facilitator Guidance

You will:

* Stay with your assigned team
* Use your Facilitator Scoring Sheet and Decision Log Template
* Prompt teams only when needed (“Have you checked the logs?”)
* Encourage collaboration, but don’t lead them

You are the mirror, not the driver.

## Final Notes

* The exercise begins with a short in-character kickoff
* You will help drive momentum, realism, and reflection
* After the scenario, teams will be debriefed and scored

Let the scenario lead them. Let pressure shape behaviour. Observe closely.

**End of Scenario Summary**