ASIAN SCHOOL OF CYBER LAWS

Cyber Security Checklist for Ports and Shipping: 20 Questions to Ask

Tick each question you can answer with a confident yes. Every unticked box is a place to start.

VISIBILITY

- 01 ☐ Do we have a current inventory of the systems on every ship and in every terminal?
- 02 ☐ Do we know every connection to our ships and terminals, including satellite links and vendor access?
- 03 ☐ Do we know which shared platforms our operations depend on?

ACCESS

- 04 ☐ Is multi-factor authentication enforced on all remote access to ships and terminals?
- 05 ☐ Is vendor access switched on only when needed, and monitored?
- 06 ☐ Are accounts removed promptly when staff and crew move on?

NETWORK

- 07 ☐ Are navigation and machinery systems separated from business IT and crew internet on every ship?
- 08 ☐ Is the terminal operating system separated from corporate IT and partner connections?
- 09 ☐ Is removable media scanned before it touches shipboard or terminal systems?

DETECTION

- 10 ☐ Do we monitor terminal networks and ship traffic for signs of intrusion?
- 11 ☐ Would our bridge teams recognise GPS jamming or spoofing quickly?
- 12 ☐ Do GNSS interference warnings reach both ships and shore operations?

RESILIENCE

- 13 ☐ Are backups of the terminal operating system and key ship systems stored offline and tested?
- 14 ☐ Could our terminals keep moving cargo manually for several days?
- 15 ☐ Can our ships navigate safely without GPS in high-risk areas?

RESPONSE

- 16 ☐ Do we have incident response plans covering both ships and terminals?
- 17 ☐ Have we decided in advance who can order a switch to manual operations?
- 18 ☐ Have we run an exercise with partners such as shipping lines, hauliers and customs in the last 12 months?

PEOPLE AND GOVERNANCE

- 19 ☐ Have crews, port staff and finance teams been trained on phishing, removable media and payment fraud?
- 20 ☐ Does the board receive regular reporting on cyber risk across the fleet and terminals?