

MARITIME, PORTS & SHIPPING CYBERSECURITY

Secure port. Moving cargo.

Port IT/OT security, cargo platform testing, remote access controls, SOC and recovery for maritime, ports and shipping.

Three questions every port and shipping leader should be able to answer

If the TOS went dark, could we run the yard?

DP World Australia and Nagoya show that terminals stop when cargo systems stop; manual playbooks and tested restores decide the outcome.

Who can reach our cranes and PLCs from outside?

OEM remote links and flat terminal networks are the most common paths to control systems.

Could a stolen portal login release our cargo?

Delivery-order and truck-nomination fraud exploits weak portal authentication and missing anomaly checks.

915 MT

Major port cargo, 2025-26

30,000

Containers stranded, DP World Australia 2023

US\$300 m

Maersk NotPetya losses (upper estimate)

6 hours

Incident reporting to CERT-In

Built for every port and shipping company

Major port authorities · non-major ports and state maritime boards · PPP terminal operators · shipping lines, ship owners and managers · shipyards and repair yards · inland waterway, coastal and dredging operators.

The rules that drive your security calendar

Instrument	Key cybersecurity expectations
CERT-In Directions · audit guidelines (2022, 2025)	6-hour reporting, 180-day logs; independent audits incl. OT
IMO MSC.428(98) · IACS E26/E27 · ISPS	Cyber risk in the SMS; newbuild cyber resilience; port facility security
NCIIPC · DPDP · SEBI LODR	Critical sector duties; customer and crew data; quarterly disclosure (listed)

Port OT, cargo platforms, remote access, SOC, recovery and ships

Port IT/OT Security

Crane, gate, conveyor, SCADA and marine OT assessments with safe methods.

Cargo Platform Testing

TOS, PCS 1x, portals and customs APIs tested for flaws and fraud.

Remote Access Controls

OEM, integrator, contractor and ship-to-shore access brokered and recorded.

24/7 IT/OT SOC

Terminals, ports and fleets monitored; 6-hour reporting.

Recovery & Resilience

Backups, manual yard playbooks, tested TOS restores, crisis exercises.

Ship Cyber Risk

MSC.428(98) assessments, UR E26/E27 readiness, bridge and engine-room reviews.

Choose your starting point

Foundation

IT and terminal OT assessment, OEM access review, backup and recovery review, policy and crisis plan. For non-major ports, single terminals and ship managers.

Assurance

IEC 62443 assessment and segmentation, TOS, PCS 1x and portal testing, annual audit, IT/OT SOC. For major ports and multi-terminal operators.

Continuous Resilience

Continuous OT testing and red teaming, fleet-wide ship cyber programmes, SOC with hunting, Board and regulator reporting. For listed port groups, large fleets and CII owners.

Why Codec Networks

CERT-In empanelled

for information security auditing services, and empanelled with NISCI for application audit services.

Certified

ISO 9001:2015, ISO/IEC 27001:2022 and ISO/IEC 20000-1:2018.

Regulation-mapped

Every finding mapped to CERT-In, NCIIPC, IMO MSC.428(98), IACS UR E26/E27, ISPS and DPDP expectations and IEC 62443.

One connected partner

Testing, audits, SOC, forensics and privacy linked from finding to closure.

Book a scoping session

Share your terminals, control systems, cargo platforms, vendors and fleet. We will propose a practical, safety-aware assessment and assurance plan.

New Delhi: 507, 5th Floor, New Delhi House, Barakhamba Road, Connaught Place – 110001

Gurugram: 707, 7th Floor, Silverton Tower, Golf Course Extension Road, Sector 50 – 122018

Call: 011 430 496 96 · +91 99716 76124 · +91 88007 88220

Email: mktg@codecnetworks.com · www.codecnetworks.com

Regulatory references reflect public instruments as of October 2026; applicability depends on each entity's licence, category and activities. Services support risk reduction and assurance and do not guarantee prevention of all incidents or regulatory compliance. Sources: MoPSW, public reporting on DP World Australia and Maersk, CERT-In. Confirm obligations against the official instruments.