Cyber incident response plan for a terminal (template)

A plan to fill in for a container terminal or a port facility: who calls whom, the controlled stop of the gate and the yard, the evidence to keep, the reporting deadlines and the return to normal operations. The first six hours are Port Cyber Alliance's planning window, not a legal deadline.

How to use it. Fill in every blank with your own names, numbers and systems, then have the plan approved by the person accountable for cyber and by the head of operations. Print it: in a cyber incident the network, the e-mail and the shared drive may be the first things you lose. Keep one paper copy in the gate office, one in the control room and one with the duty manager. Test it in a tabletop exercise at least once before you need it, and update it after every exercise and every incident.

Site: _____ **Plan owner:** _____ **Approved on:** _____

1. Scope and approval

Item	Our answer
Terminal / site	
Systems covered (TOS, gate, yard, cranes, access control, cameras, office IT)	
Plan owner (role and name)	
Approved by (accountable for cyber / head of operations)	
Version and date of approval	
Where the paper copies are kept	

2. Who calls whom (call list)

Role	Name	Phone	Backup name and phone	Calls next
Duty manager (receives the first call, declares the incident)				Incident lead
Incident lead (decides during the incident)				Crisis team
IT on call				
OT / automation on call (gate, cranes, yard equipment)				
Head of operations				
Person accountable for cyber				
Port facility security officer				
Legal / data protection				

Role	Name	Phone	Backup name and phone	Calls next
Communication				
Management (decides on reporting and on stopping operations)				
Incident response provider / insurer				
Software vendors (TOS, gate, other), one row each				
Authority for incident reports (CSIRT, competent authority, NRC)				
Port authority, main shipping lines, trucking companies				

3. When this plan starts

Item	Our answer
What counts as a cyber incident here (examples on our site)	
Who may declare the incident	
Our criteria for a significant (NIS2) or reportable (USCG) incident	
Out-of-band channel used during the incident	

4. The first six hours (tick, time, initials)

Minute 0 to 30 · Detect and declare

Goal: Turn a strange screen or an alert into a declared incident, with one person in charge. **Owner:** Duty manager (_____)

Done	Step	Time	Initials
[ ]	Whoever sees the problem (a frozen gate lane, a ransom note, an unknown account, an alert) calls the duty manager, not only IT.		
[ ]	The duty manager opens the incident log on paper: time, who reported, what was seen, which systems.		
[ ]	The duty manager declares the incident and names the incident lead. From now on one person decides.		
[ ]	Do not switch off, wipe or reinstall anything yet. Do not pay, answer or contact the attacker.		
[ ]	Our site-specific step: _____		

Minute 30 to hour 1 · Call the people on the list

Goal: The crisis team is reached by phone, not by the e-mail that may be compromised. **Owner:** Incident lead (_____)

Done	Step	Time	Initials
[ ]	Call the crisis team in the order of the call list: IT or OT on call, head of operations, the person accountable for cyber, the security officer.		
[ ]	Call the software vendors whose systems are affected, on the numbers written in the plan.		
[ ]	Open an out-of-band channel (phones, a separate messaging group) and say that the normal e-mail is not used for the incident.		
[ ]	Note every call in the log, with the time.		
[ ]	Our site-specific step: _____		

Hour 1 to 2 · Controlled stop of the gate and the yard

Goal: Stop what must stop, in order and safely, and switch to the written manual procedure. **Owner:** Head of operations, with IT or OT (_____)

Done	Step	Time	Initials
[ ]	Bring the cranes and yard equipment to a safe position before any network is cut. Safety comes before IT.		
[ ]	Close the automated gate lanes or switch them to the manual procedure; tell the trucks on site and those on their way.		
[ ]	Freeze moves that cannot be checked: no release of a container on a status the system can no longer prove.		
[ ]	Isolate the affected systems from the network as the plan says. Power a device down only if it cannot be disconnected.		
[ ]	Keep a paper record of every move made in manual mode, to re-enter it later.		
[ ]	Our site-specific step: _____		

Hour 2 to 4 · Contain and preserve evidence

Goal: Stop the spread without destroying what the investigators will need. **Owner:** IT or OT lead, with the incident response provider (_____)

Done	Step	Time	Initials
[ ]	Disconnect the affected systems and the links to partners (EDI, port community system, vendor remote access) that may carry the attack.		
[ ]	Before any clean-up, take a system image and a memory capture of a sample of affected machines, and keep the logs.		
[ ]	Keep the evidence untouched: dated copies, who handled them and when, stored offline.		
[ ]	Disable the accounts that are suspected, and reset the passwords of the administrator accounts from a clean machine.		
[ ]	Check that the backups are intact and offline before relying on them.		
[ ]	Our site-specific step: _____		

Hour 4 to 6 · Decide what to report and tell people

Goal: Know which authority must be told, by whom and before which time, and brief the people who depend on the terminal. **Owner:** Person accountable for cyber, with legal and the security officer (_____)

Done	Step	Time	Initials
[ ]	Assess whether the incident is significant (NIS2) or reportable (US Coast Guard rule) with the criteria written in the plan; note the time you became aware of it.		
[ ]	Prepare the early warning or the report with the facts known so far; send it within the deadline even if the facts are incomplete.		
[ ]	Tell the shipping lines, the truckers and the port authority what is affected and what to do, with one approved message.		
[ ]	Set the next crisis meeting and the hour of the next update. Write the decisions in the log.		
[ ]	Our site-specific step: _____		

5. Controlled stop of operations

System	Who decides to stop it	How to stop or isolate it safely	Manual fallback procedure	Where the paper forms are
Gate lanes				
Terminal operating system (TOS)				
Yard equipment				
Quay cranes				
Access control and cameras				
Links to partners (EDI, port community system, vendor remote access)				

6. Evidence to keep

Item	Our answer
Who takes the system images and memory captures	
Where the logs are and how long they are kept	
Where the evidence is stored offline, and who signs for it	
Contact of the incident response provider	

7. Reporting

NIS2 (EU) · for: Ports and terminals that are essential or important entities under NIS2 (Annex I, water transport) · to: The national CSIRT or competent authority · clock starts at: Becoming aware of the significant incident

- **24 hours**: Early warning: whether the incident is suspected to be malicious or could have a cross-border impact
- **72 hours**: Incident notification: an update, a first assessment of severity and impact, the indicators of compromise where available
- **On request**: Intermediate report on relevant status updates

• **1 month**: Final report, one month after the incident notification: description, severity and impact, root cause, mitigation, cross-border impact

U.S. Coast Guard rule (33 CFR part 101 subpart F) · for: Facilities with a Facility Security Plan under 33 CFR part 105, U.S.-flagged vessels and Outer Continental Shelf facilities · to: The National Response Center (NRC) · clock starts at: The reportable cyber incident

• **Without delay**: Report every reportable cyber incident to the NRC, unless already reported to the Coast Guard under 33 CFR 6.16-1 (in force since 16 July 2025)

IMO guidelines, Rev.4 · for: Ships and the ship/port interface, as guidance · to: As national rules and the plan require · clock starts at: The incident

• **Respond (3.5.5)**: Plans that are developed, implemented and practised; incidents reported within the required time frames; records kept

• **Recover (3.5.6)**: Measures to restore the systems impaired by the incident: recovery strategies for critical systems, training, root cause analysis

NIS2, Article 23(4): « without undue delay and in any event within 24 hours of becoming aware of the significant incident, an early warning, which, where applicable, shall indicate whether the significant incident is suspected of being caused by unlawful or malicious acts or could have a cross-border impact; (b) without undue delay and in any event within 72 hours of becoming aware of the significant incident, an incident notification, which, where applicable, shall update the information referred to in point (a) and indicate an initial assessment of the significant incident, including its severity and impact, as well as, where available, the indicators of compromise; […] (d) a final report not later than one month after the submission of the incident notification under point (b) »

Does NIS2 apply to us? _____ Does the U.S. Coast Guard rule apply to us? _____

Reports sent

Report	Authority and how to reach it	Deadline	Who prepares	Who signs and sends	Sent at (date, time)
Early warning					
Incident notification					
Intermediate report (on request)					
Final report					
Other reports (police, data protection authority, insurer, contracts)					

8. Messages to people who depend on the terminal

Item	Our answer
Who approves outgoing messages	
Shipping lines: who tells them, how	
Truckers and the gate queue: who tells them, how	
Staff on site: who tells them, how	
Press: who answers	

9. Return to normal operations

Done	Step	Done on	By
[ ]	Restore in the order of operations. Rebuild first the systems without which the terminal cannot work (identity and accounts, then the TOS, then the gate and the yard), from backups checked as clean, on machines rebuilt or verified.		
[ ]	Check before you reconnect. Reconnect one system at a time and watch it. Change the passwords and keys the attacker may have seen. Reconnect partners and vendor remote access last, once both sides agree.		
[ ]	Re-enter the manual period. Re-enter in the TOS the moves recorded on paper during the manual period, and check the yard against the system before releasing containers again.		
[ ]	Restart in steps. Open the gate in manual mode first, then the automated lanes, with a named person able to stop again. The incident lead declares the end of the incident, with the time.		
[ ]	Learn and close. Hold an after-action review within the following weeks: what happened, the root cause, what worked, what to change. Update this plan, send the final report where one is due, and plan the next exercise.		

10. After the incident, and testing this plan

Item	Our answer
Date of the after-action review	
Changes made to this plan	
Date of the last tabletop exercise	
Date of the next exercise	
Date of the next review of this plan	

Sources (public, dated)

Directive (EU) 2022/2555 (NIS2), Article 23 (reporting obligations) and Annex I (water transport: managing bodies of ports, their port facilities and entities operating works and equipment within ports), 2022-12-14. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

U.S. Coast Guard, Cybersecurity in the Marine Transportation System, final rule, 90 FR 6298 (33 CFR part 101 subpart F; reporting in §§ 101.615 and 101.620(b)(7); in force 16 July 2025), 2025-01-17. https://www.federalregister.gov/documents/2025/01/17/2025-00708/cybersecurity-in-the-marine-transportation-system

IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (functional elements Respond, paragraph 3.5.5, and Recover, paragraph 3.5.6), 2026-05-28. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

NIST SP 800-61 Rev. 3, Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile (supersedes Rev. 2 of 2012), 2025-04-03. https://csrc.nist.gov/pubs/sp/800/61/r3/final

CISA, MS-ISAC, NSA and FBI, #StopRansomware Guide (update of the 2020 Ransomware Guide), 2023-09. https://www.cisa.gov/stopransomware/ransomware-guide

ENISA, Guidelines - Cyber Risk Management for Ports (a four-phase approach mapped to the risk assessment steps of the ISPS Code), 2020-12-17. https://www.enisa.europa.eu/publications/guidelines-cyber-risk-management-for-ports

Licence

Creative Commons Attribution 4.0 International (CC BY 4.0), https://creativecommons.org/licenses/by/4.0/ . You may copy, adapt and share this template, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/resources/incident-response-playbook/ .

Generic and anonymised: no terminal, port, client or vendor is named, no statistic. This template is a planning aid, not legal advice: check which rules apply to your site with your competent authority.