Securing a truck appointment portal: a checklist for terminals and trucking companies

One line per point. Sections A to F are for the terminal that runs the portal; section G is for each trucking company that books slots on it; section H joins the booking to the gate. Walk the list with whoever runs the portal, whoever runs the gate and, for section G, the dispatch manager of a trucking company. For each point, write down who owns it and where the evidence is kept, and mark it as in place, partial, missing or not applicable. Start with the shared accounts (A1, G1) and multi-factor authentication (B1): most of the rest depends on knowing who is behind each booking.

Scope. Covers a web portal or mobile app, and its API, on which trucking companies book, change and cancel time slots to deliver or collect containers or cargo at a terminal: the accounts of the trucking companies and their dispatchers, the terminal's own administrators, the booking and cancellation flows, the API used by transport management systems (TMS), the logs, and the check of the booking at the gate. It does not replace the port facility security plan, the terminal's terms of use or legal advice on your own jurisdiction.

Status

• in place · the evidence exists, is dated and someone owns it

• partial · the practice exists but the evidence is missing, out of date or covers only some users

• missing · nothing yet

• not applicable · write down why

Summary sheet · terminal or trucking company: _____ · date: _____

Point	Area	Status	Owner
A1 · No shared accounts	Accounts and roles		
A2 · Each trucking company administers its own users	Accounts and roles		
A3 · Accounts are reviewed and dormant ones closed	Accounts and roles		
A4 · Roles limit what each account can do	Accounts and roles		
A5 · Machines use keys, not people's logins	Accounts and roles		
B1 · Multi-factor authentication for every portal user	Login and multi-factor authentication		
B2 · Phishing-resistant MFA for administrators	Login and multi-factor authentication		
B3 · Failed logins are limited	Login and multi-factor authentication		
B4 · Known-compromised passwords are refused	Login and multi-factor authentication		
B5 · Account recovery cannot be talked around	Login and multi-factor authentication		
C1 · The rules on slot transfers are written	Slot integrity: resale and brokering		
C2 · A booking names the company, the truck and the cargo	Slot integrity: resale and brokering		
C3 · Every change to a booking is recorded	Slot integrity: resale and brokering		
C4 · Cancel-and-rebook patterns are watched	Slot integrity: resale and brokering		
C5 · Booking more than you use has a written consequence	Slot integrity: resale and brokering		
D1 · The sensitive flows are listed	Bots and rate limiting		
D2 · Rate limits per account, per key and per address	Bots and rate limiting		
D3 · Non-human patterns are detected	Bots and rate limiting		
D4 · Slot release is the same for everyone	Bots and rate limiting		
E1 · An official API for transport management systems	API access for transport management systems		
E2 · One key per integration, scoped and revocable	API access for transport management systems		
E3 · The API checks who may act on which booking	API access for transport management systems		
F1 · What is logged	Access logs and detection		
F2 · Logs are protected and kept for a written period	Access logs and detection		
F3 · Alerts that someone reads	Access logs and detection		
F4 · Each trucking company sees its own activity	Access logs and detection		
G1 · One login per dispatcher, with MFA	The trucking company's side		
G2 · Leavers removed the same day	The trucking company's side		
G3 · API keys kept in a vault	The trucking company's side		
G4 · No slots bought from third parties, no logins given to brokers	The trucking company's side		
G5 · Phishing that imitates the portal	The trucking company's side		
G6 · A strange booking is reported	The trucking company's side		

Point	Area	Status	Owner
H1 · The gate checks the booking against the truck	From the booking to the gate		
H2 · Drivers' data limited to what is needed	From the booking to the gate		

A · Accounts and roles

One person, one account; each trucking company manages its own users; machines use keys, not people's logins.

A1 · No shared accounts

Check: Every person who books, changes or cancels slots has a personal account: no login shared by a dispatch office, a shift or a group of drivers, and no account lent to a third party. The terms of use say so.

Why: A shared login cannot be traced to a person, cannot be removed when one person leaves, and cannot carry multi-factor authentication properly. The US Coast Guard rule asks for separate credentials and the removal of a user's credentials when the user leaves; NIS2 lists access control policies among the minimum measures.

Evidence to hold: [ ] The terms of use of the portal with the one-person-one-account rule · [ ] A list of accounts showing one named person per account (no generic names such as « dispatch » or « office »)

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); Directive (2022-12-14); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A2 · Each trucking company administers its own users

Check: Each trucking company has one or two named administrators who create and remove the accounts of their dispatchers; the terminal knows who they are and can see the user list of each company.

Why: The terminal cannot know when a dispatcher leaves a trucking company. The company can, if it is given the tool and the responsibility. Without it, the accounts of people who left stay open.

Evidence to hold: [ ] The named administrators of each trucking company, with the date of the last check · [ ] The user list per company, readable by the terminal

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); Directive (2022-12-14)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A3 · Accounts are reviewed and dormant ones closed

Check: At a written interval, each trucking company confirms its list of users; accounts not used for a period the terminal sets are disabled, and accounts of people who left are removed.

Why: Dormant accounts are a favourite target of credential stuffing because no one notices when they are used again. Removing the credentials of people who leave is a requirement of the US Coast Guard rule.

Evidence to hold: [ ] The review procedure and the date of the last review · [ ] The list of accounts disabled at the last review

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); OWASP Automated Threats to Web Applications, handbook v1.30 (2026-03-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A4 · Roles limit what each account can do

Check: Roles separate at least: booking for one's own company, administering one's own company's users, and terminal administration. Terminal administrator accounts are few, named and separate from the person's everyday account.

Why: The principle of least privilege for administrator accounts and separate credentials for critical systems are both in 33 CFR 101.650(a). An administrator account can change every booking on the terminal.

Evidence to hold: [ ] The role matrix of the portal · [ ] The list of terminal administrator accounts, with their owners

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

A5 · Machines use keys, not people's logins

Check: A transport management system or a script that books slots uses an API key issued for that integration, never the username and password of a dispatcher.

Why: A person's password stored in a script is a shared account by another name: it does not leave with the person and cannot do multi-factor authentication. It also pushes integrators to automate the web pages instead of the API.

Evidence to hold: [ ] The list of API keys, one line per integration and per trucking company · [ ] The rule, in the terms of use, that automation goes through the API

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05); US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B · Login and multi-factor authentication

MFA for every user, stronger MFA for administrators, failed logins limited, account recovery that cannot be talked around.

B1 · Multi-factor authentication for every portal user

Check: Every account that can book, change or cancel a slot logs in with a second factor (an authenticator app, a security key or a passkey); SMS is a temporary fallback only, written as such.

Why: A password alone is reused, phished or guessed. NIS2 lists multi-factor authentication among the minimum measures (Article 21(2)(j)); 33 CFR 101.650(a)(4) requires it on password-protected IT systems. CISA describes SMS and voice codes as weaker than the alternatives.

Evidence to hold: [ ] The portal setting that enforces MFA, with the share of active accounts enrolled · [ ] The list of accounts still without MFA, each with a reason and a date

Sources: Directive (2022-12-14); US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); CISA, Implementing Phishing-Resistant MFA (2022-10-31)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B2 · Phishing-resistant MFA for administrators

Check: Terminal administrators, and if possible trucking-company administrators, use phishing-resistant authentication (security keys or passkeys based on FIDO2/WebAuthn, or certificates).

Why: An administrator account controls every slot. CISA's fact sheet of October 2022 says FIDO/WebAuthn and PKI-based authentication are the phishing-resistant options and asks organisations to start with their most exposed accounts.

Evidence to hold: [ ] The authentication method of each administrator account

Sources: CISA, Implementing Phishing-Resistant MFA (2022-10-31); NIST, SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management (2025-07-31)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B3 · Failed logins are limited

Check: Repeated failed logins on one account lead to a delay or a lockout; many failed logins across accounts from the same addresses are blocked and raise an alert.

Why: Credential stuffing tries passwords leaked elsewhere on many accounts at once. 33 CFR 101.650(a)(1) requires automatic lockout after repeated failures; NIST SP 800-63B-4 asks verifiers to limit failed attempts; OWASP lists credential stuffing and the lack of such limits as a broken-authentication risk (API2:2023).

Evidence to hold: [ ] The lockout and throttling settings of the portal and of the API · [ ] An example alert from a test

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); NIST, SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management (2025-07-31); OWASP API Security Top 10, 2023 edition (2023-06-05); OWASP Automated Threats to Web Applications, handbook v1.30 (2026-03-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B4 · Known-compromised passwords are refused

Check: When a user sets a password, it is checked against a list of passwords known to be compromised or too common, and refused if it matches.

Why: NIST SP 800-63B-4 asks verifiers to compare new passwords against such a blocklist. It stops the passwords that credential stuffing tries first.

Evidence to hold: [ ] The password policy of the portal, with the blocklist check

Sources: NIST, SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management (2025-07-31)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

B5 · Account recovery cannot be talked around

Check: A forgotten password or a lost second factor is reset through a written process that checks the person (for example through the trucking company's own administrator), never on a phone call to the help desk alone. The user is told by e-mail when the password, the second factor or the e-mail address changes.

Why: The help desk that resets accounts on request is the shortest way around multi-factor authentication. This point is plain practice; the US Coast Guard rule asks personnel to be trained on the techniques used to circumvent security measures.

Evidence to hold: [ ] The written reset procedure for the help desk · [ ] The notification e-mail sent on a change of password, factor or address

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C · Slot integrity: resale and brokering

A slot belongs to the company that booked it; every change of company, truck or driver is recorded; hoarding and resale are visible.

C1 · The rules on slot transfers are written

Check: The terms of use say whether a slot can be passed from one trucking company to another, and if so only through the portal, with both companies named; selling slots, or booking slots to sell them on, is forbidden.

Why: When slots are scarce, some accounts book them to resell them, by hand or with bots: OWASP names this threat scalping (OAT-005) and lists the slot-booking bot among its forms. A rule that is not written cannot be enforced.

Evidence to hold: [ ] The clause of the terms of use on transfers and resale · [ ] The date the trucking companies accepted the current version

Sources: OWASP Automated Threats to Web Applications, handbook v1.30 (2026-03-17); OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C2 · A booking names the company, the truck and the cargo

Check: Each booking holds the trucking company, the container or cargo reference and, before the arrival, the truck registration; a booking without a company is refused.

Why: A slot that does not say who will use it can be sold to anyone. Naming the company and the truck lets the gate check the booking (section H) and makes resale visible in the records.

Evidence to hold: [ ] The mandatory fields of a booking, read in the portal

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C3 · Every change to a booking is recorded

Check: A change of company, truck, driver, container or time on a booking is recorded with who made it, from which account or API key, and when; the history is kept with the booking.

Why: Brokered slots show up as bookings that change hands or trucks shortly before the slot. Without the history, the terminal cannot tell a normal change from a sale.

Evidence to hold: [ ] The change history of a sample booking

Sources: ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21); US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C4 · Cancel-and-rebook patterns are watched

Check: The terminal looks for slots cancelled by one account and taken by another account within moments, for accounts that book far more slots than they use, and for accounts that always book the instant slots are released.

Why: These are the traces of slot brokering and of hoarding. OWASP describes hoarding without using as denial of inventory (OAT-021) and fast automated buying as scalping (OAT-005). This point is detection, not a verdict: the terminal checks before it acts.

Evidence to hold: [ ] The report or query used, with its date and owner · [ ] The last review of its results

Sources: OWASP Automated Threats to Web Applications, handbook v1.30 (2026-03-17); OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

C5 · Booking more than you use has a written consequence

Check: The terms of use say what happens to repeated no-shows and late cancellations, and the rule is applied the same way to every trucking company.

Why: If holding a slot costs nothing, booking slots in case, or to resell, is rational. A written, equal rule removes the incentive. This point is plain practice; the rule itself is the terminal's business decision.

Evidence to hold: [ ] The clause on no-shows and late cancellations · [ ] The record of its application

Sources: OWASP Automated Threats to Web Applications, handbook v1.30 (2026-03-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D · Bots and rate limiting

The booking flows are identified, limited per account, key and address, and watched for non-human patterns.

D1 · The sensitive flows are listed

Check: The terminal has listed the flows that would hurt if used too fast or too often: login, slot search, booking, change, cancellation, and account creation.

Why: OWASP's API6:2023 (unrestricted access to sensitive business flows) gives the example of an attacker who reserves all the available time slots and prevents other users from using the system, and asks to identify these flows first, then to choose protections.

Evidence to hold: [ ] The list of sensitive flows, with the protection chosen for each

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D2 · Rate limits per account, per key and per address

Check: Each sensitive flow has a limit per account, per API key and per network address, set from the real use of the portal, with a clear error when a limit is reached.

Why: OWASP API4:2023 (unrestricted resource consumption) and API6:2023 both ask for limits. Without them, one script can search and book faster than every dispatcher together.

Evidence to hold: [ ] The rate-limit settings, flow by flow · [ ] A test showing the limit and the error

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D3 · Non-human patterns are detected

Check: The portal or its protection layer looks at how the booking flow is used (headless browsers, request timing, the same sequence repeated without pause) and can challenge or block it.

Why: OWASP lists device fingerprinting, human detection and the analysis of non-human patterns among the ways to slow automated abuse of a business flow (API6:2023).

Evidence to hold: [ ] The detection in place and where its alerts go

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05); OWASP Automated Threats to Web Applications, handbook v1.30 (2026-03-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

D4 · Slot release is the same for everyone

Check: The way and the time new slots are released are documented, and every trucking company sees them the same way, through the portal or the API.

Why: When release is predictable to some and not to others, bots and brokers gain the advantage that a slot-booking bot is built for. This point is plain practice.

Evidence to hold: [ ] The published release rule

Sources: OWASP Automated Threats to Web Applications, handbook v1.30 (2026-03-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

E · API access for transport management systems

An official, documented API with one key per integration, so that no one needs to script the web portal.

E1 · An official API for transport management systems

Check: Trucking companies that want to automate get a documented API for slot search and booking, with the same rules as the portal; scraping the web pages is not needed and is forbidden by the terms of use.

Why: If no API exists, integrators automate the web pages with stored logins, which looks exactly like a bot. OWASP asks to secure and limit access to APIs consumed directly by machines (API6:2023).

Evidence to hold: [ ] The API documentation and its access conditions

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

E2 · One key per integration, scoped and revocable

Check: Each API key belongs to one trucking company and one integration, can only act for that company, can be revoked at once, and is replaced when a person who handled it leaves or when it may have been exposed.

Why: A key shared between companies or integrations cannot be traced or revoked without breaking everyone. NIS2 lists the security of the relationships with suppliers and service providers among the minimum measures.

Evidence to hold: [ ] The key register (company, integration, scope, creation date, last use) · [ ] The revocation procedure

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05); Directive (2022-12-14)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

E3 · The API checks who may act on which booking

Check: Every API call that reads or changes a booking checks that the key belongs to the company that owns the booking; a key cannot read or cancel another company's bookings by changing an identifier.

Why: Broken object-level authorisation is the first risk of the OWASP API Security Top 10 (API1:2023). On a booking API it means one trucking company can see or cancel another's slots.

Evidence to hold: [ ] A test where a key tries to read and cancel another company's booking and is refused

Sources: OWASP API Security Top 10, 2023 edition (2023-06-05)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

F · Access logs and detection

Logins, bookings, cancellations and admin actions are logged, kept out of reach of those they record, and someone reads the alerts.

F1 · What is logged

Check: The portal and the API log: logins (successful and failed), MFA and password changes, account creation and removal, bookings, changes, cancellations, transfers, administrator actions, and API calls with the key that made them.

Why: Without these events, none of the checks of sections A to E can be proven or investigated. The joint guide on event logging (ASD's ACSC with CISA, the FBI, the NSA and partners, 21 August 2024) sets a baseline for what to log and how.

Evidence to hold: [ ] The list of logged events · [ ] A sample log entry for a booking change

Sources: ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

F2 · Logs are protected and kept for a written period

Check: Logs are sent to a place that portal administrators and the vendor cannot edit, and kept for a period written in the security plan.

Why: 33 CFR 101.650(c)(1) requires logs to be securely captured, stored and protected so that only privileged users can reach them. A log that the person it records can delete proves nothing.

Evidence to hold: [ ] Where the logs go and who can read or delete them · [ ] The written retention period

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

F3 · Alerts that someone reads

Check: Alerts exist at least for: many failed logins, a login from an unusual place for an administrator, MFA removed from an account, an account or API key booking far above its usual pattern, and administrator changes to bookings. Each alert has an owner.

Why: Logs nobody reads detect nothing. IMO Rev.4 asks to detect cyber events (3.5.4); the joint logging guide asks for detection based on the events collected.

Evidence to hold: [ ] The alert list with an owner for each · [ ] The last alert handled, with what was done

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

F4 · Each trucking company sees its own activity

Check: A trucking company's administrator can see the logins and booking actions of the company's own accounts and API keys.

Why: The trucking company is the first to notice a login or a booking that none of its dispatchers made, if it can see them. This point is plain practice.

Evidence to hold: [ ] The activity view offered to trucking-company administrators

Sources: ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G · The trucking company's side

What each trucking company protects on its own side: its logins, its keys, its leavers, and the slots it is offered.

G1 · One login per dispatcher, with MFA

Check: Each dispatcher has a personal account with multi-factor authentication turned on; no login is written on a board, in a shared document or in a group chat.

Why: Bookings made from a shared login are bookings no one can account for. If the terminal offers MFA, the trucking company turning it on is the cheapest protection of its slots.

Evidence to hold: [ ] The list of the company's portal users, one per person, MFA on

Sources: CISA, Implementing Phishing-Resistant MFA (2022-10-31); Directive (2022-12-14)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G2 · Leavers removed the same day

Check: When a dispatcher, driver with an account or subcontractor stops working for the company, the company's portal administrator removes the account and any API key the person handled is replaced.

Why: A former employee's account can still book and cancel the company's slots. The US Coast Guard rule asks for the removal of credentials when a user leaves; the same logic applies on the trucking company's side.

Evidence to hold: [ ] The leaver checklist with the portal on it

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G3 · API keys kept in a vault

Check: The API key of the transport management system is stored in the TMS's secret store or a password manager, never in an e-mail, a spreadsheet or the source code, and only the people who need it can read it.

Why: An API key sent by e-mail or kept in a file is a password anyone who finds it can use. This point is plain practice; NIS2 lists access control and cryptography policies among the minimum measures.

Evidence to hold: [ ] Where the key is stored and who can read it

Sources: Directive (2022-12-14)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G4 · No slots bought from third parties, no logins given to brokers

Check: The company books only through its own accounts and does not buy slots from, or give its login to, an intermediary offering « guaranteed » slots.

Why: A broker who holds your login can book, cancel and read in your name; slots bought from a third party may break the terminal's terms of use and may be cancelled. This point is plain practice.

Evidence to hold: [ ] The rule written in the company's dispatch instructions

Sources: OWASP Automated Threats to Web Applications, handbook v1.30 (2026-03-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G5 · Phishing that imitates the portal

Check: Dispatchers know the portal's real address, type it or use a bookmark, and know the terminal never asks for a password or an MFA code by e-mail, phone or message. A suspicious message is reported to the terminal.

Why: A copy of the login page collects the password and the one-time code together; only phishing-resistant methods stop it (CISA, October 2022). The US Coast Guard rule includes recognising threats in the training of personnel.

Evidence to hold: [ ] The short instruction given to dispatchers · [ ] The terminal's contact for reporting

Sources: CISA, Implementing Phishing-Resistant MFA (2022-10-31); US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

G6 · A strange booking is reported

Check: The company checks its upcoming bookings, and tells the terminal at once about a booking, cancellation or login it did not make.

Why: The terminal sees many companies; each company knows its own trucks. The two views together catch account takeover early. This point is plain practice.

Evidence to hold: [ ] Who checks the bookings, and how often · [ ] The terminal's contact for reporting

Sources: ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection (2024-08-21)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

H · From the booking to the gate

The gate checks that the truck in the lane is the one on the booking, and the drivers' data is kept to what is needed.

H1 · The gate checks the booking against the truck

Check: At the gate, the truck registration and the container are checked against the booking (by a clerk or by gate cameras and OCR); a mismatch goes to a person, and the decision is recorded.

Why: If the gate only checks that a slot exists, a resold or stolen slot works as well as a real one. The gate camera and OCR page of Port Cyber Alliance covers the devices that make this check.

Evidence to hold: [ ] The gate procedure for a booking that does not match the truck · [ ] The record of mismatches over a recent period

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

H2 · Drivers' data limited to what is needed

Check: The portal asks only for the driver and truck data the terminal needs, says why and for how long it is kept, and deletes it at the end of a written period.

Why: Driver names, licence numbers and plates are personal data in the EU: collect what the purpose needs, keep it no longer than needed, secure it, tell the people (GDPR Articles 5, 13 and 32). Outside the EU, check the law of each jurisdiction. This is not legal advice.

Evidence to hold: [ ] The list of driver data fields and the purpose of each · [ ] The retention period and the privacy notice

Sources: Regulation (2016-04-27)

Status: [ ] in place [ ] partial [ ] missing [ ] n/a Owner: _____ Evidence at: _____

Sources (public, dated)

OWASP API Security Top 10, 2023 edition (API1 broken object level authorization, API2 broken authentication, API4 unrestricted resource consumption, API6 unrestricted access to sensitive business flows), 2023-06-05.
https://api-security.owasp.org/editions/2023/en/0x11-t10/

OWASP Automated Threats to Web Applications, handbook v1.30 (OAT-005 Scalping incl. slot-booking bots, OAT-008 Credential Stuffing, OAT-021 Denial of Inventory), 2026-03-17.
https://owasp.org/www-project-automated-threats-to-web-applications/

Directive (EU) 2022/2555 (NIS2), Article 21(2): supply chain security (d), access control (i), multi-factor authentication (j), 2022-12-14. https://eur-lex.europa.eu/eli/dir/2022/2555/oj

US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (account security: lockout, MFA, least privilege, separate credentials, removal of leavers' credentials; protected logs; training), in force since 16 July 2025, 2025-01-17.
https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F

CISA, Implementing Phishing-Resistant MFA (fact sheet), 2022-10-31.
https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

NIST, SP 800-63B-4, Digital Identity Guidelines: Authentication and Authenticator Management, 2025-07-31.
https://csrc.nist.gov/pubs/sp/800/63/b/4/final

ASD's ACSC, CISA, FBI, NSA and partners, Best Practices for Event Logging and Threat Detection, 2024-08-21.
https://www.cisa.gov/resources-tools/resources/best-practices-event-logging-and-threat-detection

IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (3.5.3 protect: accounts and logs, 3.5.4 detect), 2026-05-28.
https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

Regulation (EU) 2016/679, General Data Protection Regulation (Articles 5, 13 and 32), 2016-04-27.
https://eur-lex.europa.eu/eli/reg/2016/679/oj

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 checklist, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/who-we-protect/trucking-companies/truck-appointment-portal-security/ . Generic: no terminal, port, client or vendor is named and no figure is invented. This checklist is not legal advice and does not replace your port facility security plan, the terms of use of the portal or advice on the law of your jurisdiction; Port Cyber Alliance does not certify or audit terminals or portals.