Gate camera and OCR security: a terminal's checklist

One line per point. Walk the gate with whoever runs IT, whoever runs the lanes and the camera or OCR vendor's contact. For each point, check what the line asks, 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 points of section H: they decide what happens at the barrier on the day the OCR stops reading.

Scope. Covers the truck gate of a container, ro-ro or bulk terminal: the cameras that read plates, container and chassis numbers and seals, the OCR or licence plate recognition (LPR) units and their servers, the lane controllers and kiosks, the barriers and the link to the terminal operating system (TOS). It does not replace the port facility security plan, a data protection impact assessment 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• partial · the practice exists but the evidence is missing, out of date or covers only some lanes

• missing · nothing yet

• not applicable · write down why

Summary sheet · terminal: _____ · date: _____

Point	Area	Status	Owner
A1 · Every gate device is in the inventory	Inventory and ownership		
A2 · The data flows of the gate are drawn	Inventory and ownership		
A3 · One owner for the gate system	Inventory and ownership		
B1 · Gate devices on their own network segment	Network segmentation		
B2 · Only the chosen flows cross to the TOS, and they are logged	Network segmentation		
B3 · No gate device reachable from the Internet	Network segmentation		
B4 · Unused services turned off	Network segmentation		
B5 · Lane cabinets and network ports physically protected	Network segmentation		
C1 · No default password left on any device	Accounts and passwords		
C2 · Named accounts, separate admin accounts, leavers removed	Accounts and passwords		
C3 · Multi-factor authentication for admin and remote access	Accounts and passwords		
D1 · Versions known, update channel and support end known	Firmware and vulnerabilities		
D2 · Updates tested on one lane first, with a way back	Firmware and vulnerabilities		
D3 · The vendor tells you about vulnerabilities	Firmware and vulnerabilities		
E1 · Remote access through a path the terminal controls	Remote vendor access		
E2 · Every vendor session logged	Remote vendor access		
E3 · Images and reads stay where the contract says	Remote vendor access		
F1 · Logs leave the devices and are protected	Logging and monitoring		
F2 · Someone is told when a camera goes dark or a configuration changes	Logging and monitoring		
F3 · Clocks synchronised	Logging and monitoring		
G1 · What is captured, and why, is listed	Drivers' personal data		
G2 · A retention period per purpose, and automatic deletion	Drivers' personal data		
G3 · Access to images and reads is limited and logged	Drivers' personal data		
G4 · Drivers are told	Drivers' personal data		
G5 · The assessment or policy the law asks for is written	Drivers' personal data		
G6 · Sharing is written down	Drivers' personal data		
H1 · Low-confidence reads go to a person	When the OCR fails		
H2 · A written degraded mode and a manual lane	When the OCR fails		
H3 · No barrier opens silently	When the OCR fails		
H4 · The manual mode is practised	When the OCR fails		
H5 · Back to normal quickly	When the OCR fails		

A · Inventory and ownership

Know every camera, OCR unit, recorder, kiosk and lane controller, and who answers for it.

A1 · Every gate device is in the inventory

Check: Each camera, OCR or LPR unit, video recorder, kiosk, lane controller and barrier controller is listed with its location (lane, pole, cabinet), IP and MAC address, model, firmware version, owner and vendor support contact.

Why: A device that is not in the inventory is not patched, not segmented and not monitored. Gate devices are often installed by a contractor and never enter the IT asset list.

Evidence to hold: [ ] The inventory, dated, with one line per device · [ ] A network scan of the gate segments that matches the inventory

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); NIST, NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline (2020-05)

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

A2 · The data flows of the gate are drawn

Check: A diagram shows what each device sends, to where, and how: camera to OCR server, OCR server to gate system, gate system to TOS, images to storage, and any flow to the vendor's cloud or to an authority.

Why: Segmentation rules, firewall rules and the privacy notice all depend on knowing the flows. A flow to a vendor cloud is both a network exposure and a transfer of personal data.

Evidence to hold: [ ] A dated data-flow diagram of the gate · [ ] The list of external destinations (vendor, cloud, authorities), with the reason for each

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); NIST, SP 800-82 Rev. 3, Guide to Operational Technology (2023-09)

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

A3 · One owner for the gate system

Check: One person answers for the gate as a whole (IT network, OT devices, physical security, data), and knows how to reach the vendor and the port facility security officer at any hour.

Why: At the gate, IT, operations and security meet. Without one owner, a fault falls between three teams while trucks queue.

Evidence to hold: [ ] A named owner and a deputy, in writing · [ ] The escalation list (vendor, IT on call, security officer)

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: _____

B · Network segmentation

Keep gate devices away from the corporate network, the TOS and the Internet, except for the flows you chose.

B1 · Gate devices on their own network segment

Check: Cameras, OCR units and lane controllers sit on a dedicated segment (VLAN or physical network), not on the office network and not flat with the TOS servers.

Why: IMO Rev.4 asks to segment OT device networks from IT networks; CISA and its partners ask to segment IT and OT and to pass data through a demilitarised zone. A compromised camera should not see the TOS.

Evidence to hold: [ ] The segment plan (VLANs, subnets, firewalls) · [ ] A test from a gate device showing that the office network and the TOS servers are not reachable directly

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); NIST, SP 800-82 Rev. 3, Guide to Operational Technology (2023-09); 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: _____

B2 · Only the chosen flows cross to the TOS, and they are logged

Check: Between the gate segment and the TOS, only the flows of the A2 diagram are allowed (named hosts, named ports), ideally through one broker or interface server; every connection is logged.

Why: The gate system has to talk to the TOS; the rest of the gate does not. One controlled crossing is easier to watch than many.

Evidence to hold: [ ] The firewall rules between the gate segment and the TOS, reviewed and dated · [ ] Logs of the connections across that boundary

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); NIST, SP 800-82 Rev. 3, Guide to Operational Technology (2023-09)

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

B3 · No gate device reachable from the Internet

Check: No camera, recorder, OCR server or lane controller answers from the Internet: no port forwarding, no exposed web interface, no vendor « cloud access » or peer-to-peer feature left on by default.

Why: CISA and its partners list the removal of OT connections to the public Internet first, because exposed devices are found by simple searches of public address ranges.

Evidence to hold: [ ] An external scan of the terminal's public addresses, dated, with no gate device answering · [ ] The list of cloud or peer-to-peer features checked and turned off

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); 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: _____

B4 · Unused services turned off

Check: On each device model, services that are not used (telnet, FTP, UPnP, unencrypted web interface, default SNMP communities) are turned off, and the hardened configuration is saved.

Why: Every open service is a way in. The baseline of device security capabilities includes control of the device's configuration and of access to its interfaces.

Evidence to hold: [ ] A hardening sheet per device model · [ ] The saved configuration of each device

Sources: NIST, NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline (2020-05); ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures (2017-11-20)

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

B5 · Lane cabinets and network ports physically protected

Check: Cabinets at the lanes and on poles are locked, network ports in kiosks and cabinets are disabled when not in use or bound to the expected device, and access to them is recorded.

Why: The gate is the part of the terminal that outsiders reach every day. A free network socket in a lane cabinet is a way onto the gate segment.

Evidence to hold: [ ] The key or badge list for gate cabinets · [ ] The switch configuration showing port security or disabled ports

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); EDPB, Guidelines 3/2019 on processing of personal data through video devices, version 2.0 (2020-01-29)

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

C · Accounts and passwords

No default password, named accounts, multi-factor authentication for admin and remote access.

C1 · No default password left on any device

Check: Every camera, recorder, OCR unit, kiosk and controller has had its default password changed before going live, and no two devices share one password unless a vault manages it.

Why: IMO Rev.4 asks to change all default passwords on all devices; CISA and its partners found default or easily guessed passwords on the OT systems targeted; the US Coast Guard rule asks for default passwords to be changed before use.

Evidence to hold: [ ] The commissioning record of each device showing the password change · [ ] Where the passwords are kept (a vault), and who can read them

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); CISA, Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords (2023-12-15); 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: _____

C2 · Named accounts, separate admin accounts, leavers removed

Check: Clerks, supervisors, IT and vendor staff each log into the gate system and the device consoles with their own account; administrator accounts are separate; accounts of people who leave are disabled the same day.

Why: A shared « gate » login means no one can say who opened a barrier or changed a camera. IMO Rev.4 asks for unique credentials and separate privileged accounts.

Evidence to hold: [ ] The account list of the gate system and of each device console · [ ] The leaver procedure, and the last review of the list

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

C3 · Multi-factor authentication for admin and remote access

Check: Administrator access to the gate system and every remote access to the gate segment use multi-factor authentication, phishing-resistant where possible.

Why: CISA and its partners ask for phishing-resistant multi-factor authentication on remote access to OT; the US Coast Guard rule asks for it on remotely accessible OT.

Evidence to hold: [ ] The configuration of the remote access gateway and of the gate system's admin login

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); 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: _____

D · Firmware and vulnerabilities

Know the versions, update them in a controlled way, hear about vulnerabilities from the vendor.

D1 · Versions known, update channel and support end known

Check: For each device model, the inventory records the firmware or software version, how updates are delivered and verified, and until when the vendor supports the model.

Why: A device that can no longer be updated has to be isolated or replaced. Software update is part of the baseline of device security capabilities.

Evidence to hold: [ ] Versions and support end dates in the inventory · [ ] The vendor's update and support policy

Sources: NIST, NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline (2020-05); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (2025-01-13)

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

D2 · Updates tested on one lane first, with a way back

Check: An update is installed on one lane, read rates and the TOS link are checked, then it is rolled out; the previous version and configuration are kept to roll back.

Why: An update that breaks the reads at every lane at once is an outage. Testing on one lane keeps the gate open. Plain practice, consistent with the regular updates IMO Rev.4 asks for.

Evidence to hold: [ ] The update procedure and the record of the last update · [ ] The stored previous firmware and configuration

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: _____

D3 · The vendor tells you about vulnerabilities

Check: The contract or support agreement says the vendor informs the terminal of vulnerabilities and incidents affecting its devices or software, without delay, and how fixes are delivered.

Why: The US Coast Guard rule asks facilities to have IT and OT vendors notify them of vulnerabilities and incidents; CISA's guidance for OT buyers lists vulnerability management among the things to ask for.

Evidence to hold: [ ] The clause in the contract or support agreement · [ ] The vendor's security contact

Sources: US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (2025-01-17); CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (2025-01-13)

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

E · Remote vendor access

The vendor connects through a path the terminal controls, when the terminal opens it, and every session is logged.

E1 · Remote access through a path the terminal controls

Check: The vendor reaches the gate devices only through the terminal's VPN or jump host, with multi-factor authentication, limited to the devices it supports; access is off by default and opened for a time window on request.

Why: CISA and its partners ask to re-evaluate remote access to OT, to keep it off the public Internet, to apply least privilege by asset and role, and to disable dormant accounts. A permanent vendor tunnel is a door left open.

Evidence to hold: [ ] The remote access procedure (request, approval, opening, closing) · [ ] The configuration showing that vendor access is limited to the gate devices

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); 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: _____

E2 · Every vendor session logged

Check: Each remote session records who connected, when, to which device and what was changed; the terminal can review it.

Why: The US Coast Guard rule asks facilities to monitor and document third-party remote connections. After an incident, the session log is the first thing asked for.

Evidence to hold: [ ] The session logs of the last vendor interventions

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: _____

E3 · Images and reads stay where the contract says

Check: The contract says whether the vendor may copy images or reads off site (for support or to train its models), where they are stored, for how long, and that it acts only on the terminal's instructions.

Why: In the EU, a vendor that processes personal data for the terminal is a processor and needs a written contract (GDPR Article 28). Elsewhere, the same clause tells you where your drivers' images are.

Evidence to hold: [ ] The data processing clause or agreement with the vendor · [ ] The list of places where images and reads are stored

Sources: Regulation (2016-04-27); California Civil Code §§ 1798.90.5-1798.90.55, Collection of License Plate Information (2016-01-01)

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

F · Logging and monitoring

Logs leave the devices, are protected, and someone sees a camera that goes dark or a configuration that changes.

F1 · Logs leave the devices and are protected

Check: The gate system, OCR servers and, where they can, the devices send their logs (logins, configuration changes, errors, barrier events) to a central place that the gate team cannot edit.

Why: IMO Rev.4 asks to collect and securely store logs for intrusion detection and incident response; the US Coast Guard rule asks for logs that only privileged users can reach.

Evidence to hold: [ ] Where the logs go, and how long they are kept · [ ] Who can read and who can delete them

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

F2 · Someone is told when a camera goes dark or a configuration changes

Check: Alerts exist for a camera or OCR unit that stops sending, a configuration change outside a planned window, and a new device appearing on the gate segment; each alert has someone who acts on it.

Why: A camera that has been dark for a week is a blind lane. IMO Rev.4 asks to monitor systems and detect unintended activity in a timely manner.

Evidence to hold: [ ] The list of alerts and who receives them · [ ] The last alerts and what was done

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); NIST, NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline (2020-05)

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

F3 · Clocks synchronised

Check: Cameras, OCR servers, the gate system and the TOS take their time from the same source, so a photo, a read, a log line and a gate transaction can be matched.

Why: Images and logs are evidence in a damage claim, a customs query or an incident. Evidence with clocks that disagree is weak. Plain practice.

Evidence to hold: [ ] The time source configured on each device type

Sources: NIST, SP 800-82 Rev. 3, Guide to Operational Technology (2023-09)

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

G · Drivers' personal data

Plates, faces and IDs are personal data: purpose, retention, access, notice and sharing are written down.

G1 · What is captured, and why, is listed

Check: A table lists each kind of data the gate captures (plate, container and chassis numbers, seal, cab images that may show a face, driver ID or licence, biometric template if any) and the purpose of each.

Why: A licence plate or an image that can identify a person is personal data under the GDPR. Data minimisation asks to collect only what the purpose needs (Article 5(1)(c)).

Evidence to hold: [ ] The data inventory of the gate, with a purpose per data type

Sources: Regulation (2016-04-27); EDPB, Guidelines 3/2019 on processing of personal data through video devices, version 2.0 (2020-01-29)

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

G2 · A retention period per purpose, and automatic deletion

Check: Each data type has a written retention period tied to its purpose (gate transaction record, damage claims, security footage), and deletion happens automatically at the end of it.

Why: Storage limitation (GDPR Article 5(1)(e)). The EDPB guidelines on video devices say footage should in most cases be erased after a few days, and that the longer the period (especially beyond 72 hours), the more the controller must justify it. In California, an ALPR operator's policy must state how long ALPR information is kept. Contracts and customs rules may require longer periods for transaction records: write each one down with its basis.

Evidence to hold: [ ] The retention schedule, with the basis of each period · [ ] Proof that deletion runs (a log of the last purge)

Sources: Regulation (2016-04-27); EDPB, Guidelines 3/2019 on processing of personal data through video devices, version 2.0 (2020-01-29); California Civil Code §§ 1798.90.5-1798.90.55, Collection of License Plate Information (2016-01-01)

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

G3 · Access to images and reads is limited and logged

Check: Only named roles can view, search or export images and reads; every search and export records who, when, what was searched and why.

Why: Security of processing (GDPR Article 32). In California, an ALPR operator must keep a record of each access with the date and time, the data used to query, the user and the purpose (Civil Code 1798.90.52).

Evidence to hold: [ ] The roles allowed to search or export · [ ] The access log, and the last review of it

Sources: Regulation (2016-04-27); California Civil Code §§ 1798.90.5-1798.90.55, Collection of License Plate Information (2016-01-01)

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

G4 · Drivers are told

Check: Signs before the gate say that cameras and automatic reading are in use, by whom and where to find more; a fuller notice is available (website, kiosk, haulier portal).

Why: Transparency (GDPR Article 13). The EDPB guidelines describe a layered approach: a warning sign with the key facts, then a full notice.

Evidence to hold: [ ] A photo of the sign at each gate entrance · [ ] The full privacy notice and where drivers find it

Sources: Regulation (2016-04-27); EDPB, Guidelines 3/2019 on processing of personal data through video devices, version 2.0 (2020-01-29)

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

G5 · The assessment or policy the law asks for is written

Check: In the EU, check whether a data protection impact assessment is needed and keep it. In California, an ALPR operator publishes a usage and privacy policy. Elsewhere, check the state or national rules, including any law on biometric identifiers if the gate matches faces or fingerprints.

Why: GDPR Article 35(3)(c) requires an impact assessment for systematic monitoring of a publicly accessible area on a large scale, and the EDPB guidelines point to it for video surveillance. California Civil Code 1798.90.51 lists what an ALPR usage and privacy policy must contain. Biometric data used to identify a person is a special category under GDPR Article 9.

Evidence to hold: [ ] The impact assessment or the written reason why none is needed · [ ] The published policy where one is required

Sources: Regulation (2016-04-27); EDPB, Guidelines 3/2019 on processing of personal data through video devices, version 2.0 (2020-01-29); California Civil Code §§ 1798.90.5-1798.90.55, Collection of License Plate Information (2016-01-01)

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

G6 · Sharing is written down

Check: The list of who receives images or reads (shipping lines, hauliers, customs, police, insurers, the vendor) says on what basis, through which channel, and who approves a request.

Why: Requests for gate images come from many sides. A written rule stops ad hoc exports by e-mail. California's ALPR policy must cover the purposes, process and restrictions for sharing.

Evidence to hold: [ ] The sharing list and the request procedure · [ ] The record of the last requests

Sources: Regulation (2016-04-27); California Civil Code §§ 1798.90.5-1798.90.55, Collection of License Plate Information (2016-01-01)

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

H · When the OCR fails

A degraded mode and a manual lane that keep the same checks, and no barrier that opens silently.

H1 · Low-confidence reads go to a person

Check: Below a confidence level set by the terminal, a read is not accepted automatically: the images go to a clerk who confirms or corrects, and the correction is recorded.

Why: A wrong read that is accepted silently sends the wrong box or lets the wrong truck in. Gate tenders commonly ask for an exception queue for unclear reads. Plain practice.

Evidence to hold: [ ] The confidence threshold and who set it · [ ] The exception queue and its correction log

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 · A written degraded mode and a manual lane

Check: A procedure says what happens when cameras, OCR or the link to the TOS are down: which lanes switch to manual, who keys in the numbers, how the booking or appointment and the driver are still checked, and how the records are caught up afterwards.

Why: CISA and its partners ask to practise and keep the ability to operate OT manually. IMO Rev.4 asks for plans to keep ship-port operations going and recover. The manual lane must apply the same checks as the automated one.

Evidence to hold: [ ] The degraded-mode procedure, dated · [ ] The forms or screens the clerks use in manual mode

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28); ISPS Code, Parts A and B, as reproduced in Regulation (2004-03-31)

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

H3 · No barrier opens silently

Check: Every barrier opening without a matched gate transaction (manual override, emergency opening, maintenance) records who, when, which lane and why, and the list is reviewed every day.

Why: When the OCR stops, the pressure is to « just open the barrier ». An override without a reason turns a technical fault into a security bypass that no one sees. Gate tenders commonly ask for overrides with a mandatory reason.

Evidence to hold: [ ] The override log with reasons · [ ] The daily review record

Sources: ISPS Code, Parts A and B, as reproduced in Regulation (2004-03-31); 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: _____

H4 · The manual mode is practised

Check: At least once a year, one shift runs a lane in degraded mode on purpose, and the drill is recorded with what went wrong.

Why: A procedure that has never been run fails on the day. CISA and its partners ask for manual operation to be routinely tested; the ISPS Code and the US Coast Guard rule already require drills and exercises in which a gate scenario fits.

Evidence to hold: [ ] The drill record and the actions that followed

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (2025-05-06); ISPS Code, Parts A and B, as reproduced in Regulation (2004-03-31); 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: _____

H5 · Back to normal quickly

Check: Device configurations and the gate system are backed up, spare units or parts are on site or on contract, and a known-good firmware image is kept, so a lane can be rebuilt without the vendor on site.

Why: IMO Rev.4 asks for regular backups and for recovery strategies for critical systems; the US Coast Guard rule asks to back up critical IT and OT systems and test the backups.

Evidence to hold: [ ] The backup list and the last restore test · [ ] The spares list or the replacement terms in the contract

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

Sources (public, dated)

IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (3.5.2.2 inventory, 3.5.3.1-3.5.3.3 accounts, default passwords, segmentation and logs, 3.5.3.7 backups and updates, 3.5.4 detect, 3.5.5-3.5.6 respond and recover), 2026-05-28. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

ISPS Code, Parts A and B, as reproduced in Regulation (EC) No 725/2004 (port facility security plan, access control, drills and exercises), 2004-03-31. https://eur-lex.europa.eu/eli/reg/2004/725/oj

CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (Internet exposure, default passwords, remote access, IT/OT segmentation, manual operation), 2025-05-06. https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

CISA, Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords, 2023-12-15. https://www.cisa.gov/resources-tools/resources/secure-design-alert-how-manufacturers-can-protect-customers-eliminating-default-passwords

CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products, 2025-01-13. https://www.cisa.gov/resources-tools/resources/secure-demand-priority-considerations-operational-technology-owners-and-operators-when-selecting

NIST, NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline (device identification, configuration, data protection, interface access, software update, state awareness), 2020-05. https://csrc.nist.gov/pubs/ir/8259/a/final

NIST, SP 800-82 Rev. 3, Guide to Operational Technology (OT) Security, 2023-09. https://csrc.nist.gov/pubs/sp/800/82/r3/final

ENISA, Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, 2017-11-20. https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot

US Coast Guard, 33 CFR part 101 subpart F, Cybersecurity, § 101.650 (account and device security, logs, supply chain and remote connections, resilience, segmentation and physical security), in force since 16 July 2025, 2025-01-17. https://www.ecfr.gov/current/title-33/chapter-I/subchapter-H/part-101/subpart-F

Regulation (EU) 2016/679, General Data Protection Regulation (Articles 5, 9, 13, 28, 32 and 35), 2016-04-27. https://eur-lex.europa.eu/eli/reg/2016/679/oj

EDPB, Guidelines 3/2019 on processing of personal data through video devices, version 2.0 (signs and layered notice, storage periods paragraphs 120-121, impact assessment paragraph 136, system security section 9), 2020-01-29. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

California Civil Code §§ 1798.90.5-1798.90.55, Collection of License Plate Information (added by SB 34, Stats. 2015, Ch. 532, effective 1 January 2016), 2016-01-01. https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.23.&part=4.&chapter=&article=

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/terminal-operators/gate-ocr-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, a data protection impact assessment or advice on the law of your jurisdiction; Port Cyber Alliance does not certify or audit terminals.