Marina cyber checklist: fifteen points for a small team

Fifteen points, one line each. Walk the harbour office with the harbour master, whoever looks after the computers (staff member or outside provider) and, if you can, the provider of the booking or access system. 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. It takes about one working session; start with the points marked « start here ».

Scope. Written for a marina or small harbour run by a small team without an IT department: the harbour office computers, the guest Wi-Fi, card payment at the desk, the fuel dock and online, the cameras, the pontoon gates and showers access system, and the customer and boat records. It does not replace a payment provider's compliance programme, a data protection impact assessment, the security plan of a port facility, or advice on the law of your country.

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• partial · the practice exists but the evidence is missing, out of date or covers only part of the marina

• missing · nothing yet

• not applicable · write down why

Summary sheet · marina: _____ · date: _____

Point	Area	Status	Owner
A1 · The guest Wi-Fi is separate from everything else **(start here)**	Guest Wi-Fi		
A2 · The Wi-Fi equipment has its own password and is up to date	Guest Wi-Fi		
A3 · Wi-Fi encryption is current, staff Wi-Fi codes change	Guest Wi-Fi		
B1 · You know who handles card data, and you have it in writing **(start here)**	Card payment		
B2 · Card terminals are on their own network and checked	Card payment		
C1 · Cameras and recorder are not open to the Internet **(start here)**	Cameras		
C2 · People are told, footage is kept only as long as needed	Cameras		
C3 · The cameras have their own network	Cameras		
D1 · The access control system is managed like a security system	Pontoon access control		
D2 · Badges and codes follow the contracts, and there is a fallback	Pontoon access control		
E1 · You know what customer data you keep, where and for how long **(start here)**	Customer data		
E2 · You know what to do if customer data leaks	Customer data		
F1 · One person owns cyber, with the list of providers **(start here)**	A small team without IT		
F2 · Named accounts and a second factor on what matters	A small team without IT		
F3 · Updates are on, backups exist and have been restored	A small team without IT		

A · Guest Wi-Fi

Boaters get Internet; they never get a path to the office, the tills, the cameras or the gates.

A1 · The guest Wi-Fi is separate from everything else · start here

Check: The network the boaters use has no route to the harbour office computers, the card terminals, the camera recorder or the access control system. Test it: from a phone on the guest Wi-Fi, try to reach the office printer or the recorder's web page; it must fail.

Why: A guest network is shared with people you do not know. If it reaches the office, any infected laptop on a boat reaches the office too.

Evidence to hold: [ ] A simple drawing of the networks (guest, office, payment, cameras, gates), dated · [ ] The date and result of the test from the guest Wi-Fi

Sources: NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (February 2012); ENISA, Cybersecurity guide for SMEs: 12 steps to securing your business (28 June 2021)

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

A2 · The Wi-Fi equipment has its own password and is up to date

Check: The routers and access points have their default administrator password changed, their administration page is not reachable from the Internet, and their software is updated (automatic updates on where available).

Why: Default passwords are among the first things attackers try. CISA asks manufacturers to stop shipping them; until every device does, changing them is the owner's job.

Evidence to hold: [ ] The list of Wi-Fi devices with their software version and update date · [ ] The administrator passwords stored in a password manager, not on a sticker

Sources: CISA, Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords (15 December 2023); ENISA, Cybersecurity guide for SMEs: 12 steps to securing your business (28 June 2021)

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

A3 · Wi-Fi encryption is current, staff Wi-Fi codes change

Check: The office Wi-Fi uses WPA2 or WPA3 with a password that is changed when someone leaves. Where the equipment supports it, the guest Wi-Fi uses WPA3 or Wi-Fi Enhanced Open so that boaters' traffic is encrypted even on an open network.

Why: Old or open Wi-Fi lets anyone nearby read or join the traffic. A Wi-Fi password known by former staff is a key that was never returned.

Evidence to hold: [ ] The encryption setting of each Wi-Fi network, read on the device · [ ] The date the office Wi-Fi password was last changed

Sources: Wi-Fi Alliance, Wi-Fi CERTIFIED WPA3 security (25 June 2018); NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (February 2012)

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

B · Card payment

Know who handles card data for you, and keep the payment terminals off every shared network.

B1 · You know who handles card data, and you have it in writing · start here

Check: List every way a customer pays by card: desk terminal, fuel dock, online booking, phone. For each, name the provider, keep its confirmation that it complies with PCI DSS for the service it provides you, and the written agreement that says what it is responsible for.

Why: PCI DSS applies to any business that accepts cards, even when a provider handles all the payment processing; the merchant stays responsible for checking that the provider protects the card data.

Evidence to hold: [ ] The list of payment channels with their provider · [ ] Each provider's current compliance confirmation and the agreement

Sources: PCI Security Standards Council, FAQ: Does PCI DSS apply to merchants who outsource all payment processing operations? (read on 11 November 2026); PCI Security Standards Council, PCI DSS v4.0.1 (11 June 2024)

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

B2 · Card terminals are on their own network and checked

Check: Payment terminals connect through the provider's network or a network of their own, never the guest Wi-Fi. Card numbers are never written down, e-mailed or kept in a spreadsheet. Staff look at the terminals regularly for signs of tampering or substitution and know whom to call.

Why: A terminal on a shared network can be reached by anyone on it. Card numbers outside the provider's system bring the whole office into scope.

Evidence to hold: [ ] The list of terminals (location, serial number) and the date of the last visual check · [ ] A short written rule: no card numbers on paper, in e-mail or in files

Sources: PCI Security Standards Council, PCI DSS v4.0.1 (11 June 2024); NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (February 2012)

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

C · Cameras

Cameras are network devices that film people: secure them, tell people, keep footage only as long as needed.

C1 · Cameras and recorder are not open to the Internet · start here

Check: Every camera and the recorder have their default password changed, are not reachable directly from the Internet (no port opened on the router for them), and remote viewing goes through a secure app or a VPN with a strong login. Their software is updated.

Why: Cameras and recorders exposed with default or weak passwords are found by automated scans. CISA, the FBI, the EPA and the DOE (6 May 2025) put removing Internet exposure and changing default passwords first.

Evidence to hold: [ ] The list of cameras and the recorder with software versions · [ ] The router's port-forwarding page showing no rule for them, dated

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (6 May 2025); CISA, Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords (15 December 2023)

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

C2 · People are told, footage is kept only as long as needed

Check: Signs at the entrances and on the pontoons say who films and why, and where to find more information. A retention period is written for the footage and the recorder is set to it. Only named people can view or export footage, and every export is noted.

Why: In the EU, video of people is personal data. The EDPB guidelines on video devices ask for layered signs and say footage should in most cases be erased after a few days; the longer the period, especially beyond 72 hours, the more it must be justified.

Evidence to hold: [ ] A photo of the signs · [ ] The written retention period and the recorder setting · [ ] The list of people who can view or export, and the export log

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

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

C3 · The cameras have their own network

Check: Cameras and the recorder sit on a network of their own (or a separate VLAN), not on the guest Wi-Fi and not mixed with the office computers.

Why: Cameras rarely get updates as often as computers. Keeping them apart means a weak camera does not open the rest of the marina.

Evidence to hold: [ ] The network drawing of point A1 showing the camera network

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (6 May 2025); EDPB, Guidelines 3/2019 on processing of personal data through video devices, version 2.0 (29 January 2020)

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

D · Pontoon access control

Gates, badges and codes are a security system: control who manages it and what happens when it fails.

D1 · The access control system is managed like a security system

Check: The controller of the pontoon gates, showers and car park barriers has its default password changed, is not open to the Internet, and the supplier's remote access is switched on only when needed, with its own login, and noted.

Why: An access controller is operational technology: if someone else can manage it, they can open the gates or lock everyone out. Remote access is one of the five priorities CISA and its partners list for these systems.

Evidence to hold: [ ] Who administers the system (name, supplier contact) and how the supplier connects · [ ] The log or notes of the supplier's remote sessions

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (6 May 2025); CISA, Secure by Design Alert: How Manufacturers Can Protect Customers by Eliminating Default Passwords (15 December 2023)

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

D2 · Badges and codes follow the contracts, and there is a fallback

Check: Badges and codes are cancelled when a berth contract ends or a staff member leaves; shared codes are changed on a schedule. A written fallback says what happens when the system fails (keys, who holds them, how openings are recorded) and it has been tried once.

Why: A badge that still works after the contract ended is an open door. A system that fails with no fallback leads to gates propped open. CISA and its partners ask that manual operation be possible and practised.

Evidence to hold: [ ] The last review of active badges against current contracts, dated · [ ] The written fallback and the date it was tried

Sources: CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (6 May 2025); ENISA, Cybersecurity guide for SMEs: 12 steps to securing your business (28 June 2021)

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

E · Customer data

Know what you keep about boat owners and crews, where, for how long, and what you do if it leaks.

E1 · You know what customer data you keep, where and for how long · start here

Check: List what you keep about boat owners and crews (identity, contact details, boat papers, insurance, payment history, passport copies if any) and where (booking software, e-mail, spreadsheets, paper). Keep only what you need, write a retention period for each, and have a contract with every software provider that processes it.

Why: The GDPR asks to collect only what the purpose needs, keep it no longer than needed, secure it and have a contract with every processor (Articles 5, 28 and 32). A passport copy forgotten in an inbox is data you hold without needing it.

Evidence to hold: [ ] The list of data and where it is, with retention periods · [ ] The processor agreements of the booking software and other providers

Sources: Regulation (27 April 2016); ENISA, Cybersecurity guide for SMEs: 12 steps to securing your business (28 June 2021)

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

E2 · You know what to do if customer data leaks

Check: A one-page note says who decides, whom to call (IT provider, booking software provider, insurer), how to notify the data protection authority within 72 hours where the GDPR requires it, and when to inform the customers concerned.

Why: Under the GDPR, a personal data breach that is likely to put people at risk must be notified to the authority without undue delay and where feasible within 72 hours (Article 33). Deciding this during the incident costs time.

Evidence to hold: [ ] The one-page note, dated, with the contacts · [ ] A register of incidents, even if it is empty

Sources: Regulation (27 April 2016); UK NCSC, Small organisations guide to cyber security (read on 11 November 2026)

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

F · A small team without IT

One owner, strong logins, updates and backups: the basics that stop most incidents.

F1 · One person owns cyber, with the list of providers · start here

Check: One named person (often the harbour master or the office manager) owns this checklist, even part-time. They keep the list of IT, Wi-Fi, payment, camera, access control and booking providers with their contacts and contracts, and staff know to report a suspicious e-mail or call to them.

Why: In a small team, cyber is no one's job until someone is named. ENISA's guide for small businesses starts with culture, training and managing third parties.

Evidence to hold: [ ] The name of the owner and the date of appointment · [ ] The list of providers and contacts, dated

Sources: ENISA, Cybersecurity guide for SMEs: 12 steps to securing your business (28 June 2021); UK NCSC, Small organisations guide to cyber security (read on 11 November 2026)

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

F2 · Named accounts and a second factor on what matters

Check: Each person has their own login (no shared « office » account) on the computers, e-mail and booking software. Multi-factor authentication is on for e-mail, the booking software, the bank and every remote access. Accounts are removed the day someone leaves.

Why: Stolen or guessed passwords are a frequent way in; the NCSC recommends two-step verification on important accounts, and named accounts tell you who did what.

Evidence to hold: [ ] The list of accounts per system, checked against the staff list, dated · [ ] Screenshots or notes showing multi-factor authentication switched on

Sources: UK NCSC, Small organisations guide to cyber security (read on 11 November 2026); ENISA, Cybersecurity guide for SMEs: 12 steps to securing your business (28 June 2021)

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

F3 · Updates are on, backups exist and have been restored

Check: Automatic updates are on for computers and phones. The booking, accounting and customer data are backed up, one copy is kept offline or in a separate account, and a restore has been tried in the last year.

Why: Ransomware turns a small office into a closed office. A backup that has never been restored is a hope, not a plan. IMO Rev.4 (28 May 2026) asks ports and ships to keep backups that can be restored.

Evidence to hold: [ ] Where the backups are and how often they run · [ ] The date and result of the last restore test

Sources: UK NCSC, Small organisations guide to cyber security (read on 11 November 2026); ENISA, Cybersecurity guide for SMEs: 12 steps to securing your business (28 June 2021); IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (28 May 2026)

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

Sources (public, dated)

NIST SP 800-153, Guidelines for Securing Wireless Local Area Networks (WLANs), February 2012. https://csrc.nist.gov/pubs/sp/800/153/final

Wi-Fi Alliance, Wi-Fi CERTIFIED WPA3 security (and Wi-Fi CERTIFIED Enhanced Open for open networks), 25 June 2018. https://www.wi-fi.org/news-events/newsroom/wi-fi-alliance-introduces-wi-fi-certified-wpa3-security

ENISA, Cybersecurity guide for SMEs: 12 steps to securing your business, 28 June 2021. https://www.enisa.europa.eu/publications/cybersecurity-guide-for-smes

UK NCSC, Small organisations guide to cyber security (backups, devices, accounts, phishing), read on 11 November 2026. https://www.ncsc.gov.uk/collection/small-business-guide

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

CISA, FBI, EPA and DOE, Primary Mitigations to Reduce Cyber Threats to Operational Technology (Internet exposure, default passwords, remote access, segmentation, manual operation), 6 May 2025. https://www.cisa.gov/resources-tools/resources/primary-mitigations-reduce-cyber-threats-operational-technology

PCI Security Standards Council, PCI DSS v4.0.1 (general reference, no text reproduced), 11 June 2024. https://blog.pcisecuritystandards.org/just-published-pci-dss-v4-0-1

PCI Security Standards Council, FAQ: Does PCI DSS apply to merchants who outsource all payment processing operations?, read on 11 November 2026. https://www.pcisecuritystandards.org/faq/articles/Frequently_Asked_Question/does-pci-dss-apply-to-merchants-who-outsource-all-payment-processing-operations-and-never-store-process-or-transmit-cardholder-data/

Regulation (EU) 2016/679, General Data Protection Regulation (Articles 5, 13, 28, 32 and 33), 27 April 2016. 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, 29 January 2020. https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en

IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4, 28 May 2026. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

Directive (EU) 2022/2555 (NIS2): scope, Articles 2 and 3, and the sectors of its Annexes, 14 December 2022. https://eur-lex.europa.eu/eli/dir/2022/2555/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/marinas/marina-cyber-checklist/ . Generic: no marina, port, client or vendor is named and no figure is invented. This checklist is not legal advice and does not replace a payment provider's compliance programme, a data protection impact assessment or advice on the law of your country; Port Cyber Alliance does not certify or audit marinas.