What terminals ask before connecting your software

For a vendor: answer every question of the eight families before the terminal asks, attach the evidence listed under "prepare", and adapt the model answer to what you really do. An honest "not yet, here is the date" is better than a vague "yes". For a terminal: send the questions, and score each answer with the scale below.

Answer scale: Yes, with evidence attached · Yes, no evidence yet · Not yet, planned with a date and an owner · No · Not applicable, with the reason

Families: 1. Access · 2. Data · 3. Logs · 4. Backups · 5. Incidents · 6. Subcontractors · 7. Penetration tests · 8. End of contract

1. Access

Remote access by suppliers is one of the ways into a terminal's network. The terminal wants to know who at your company can reach its systems, how, and how that access ends.

Question	Answer	Evidence / comment
Who in your company can reach our systems or our data, by role, and how many people is that?		
How do they connect (our VPN, a jump host, your own remote tool), and can we approve or cut each session?		
Is multi-factor authentication required for every person, including administrators and support staff?		
Are accounts named and personal, with no shared or default passwords?		
How fast is access removed when someone leaves your team, and how often do you review the list with us?		

What to prepare: A list of roles with access, and what each role can do · A diagram of the remote-access path, through the terminal's own entry point · The multi-factor method used, and single sign-on if you support it · Your joiner and leaver procedure, with the time to remove access

> **Model answer** (fill in the brackets with what you really do): Our support engineers reach your environment only through the path you choose, your VPN or your jump host, and each session can be approved and closed by your team. Every person has a named account with multi-factor authentication; there are no shared accounts and no default passwords. Access is granted for a ticket and removed within [time] of a person leaving the team. We review the list of people with access with you every [period].

Sources: CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (2025-01-13) · CISA, Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem (2024-08) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

2. Data

The terminal stays responsible for its data, and often for personal data of drivers, crews and staff. It needs to know what you hold, where, and who can read it.

Question	Answer	Evidence / comment
What data of ours do you store or process, and which of it is personal data?		
In which countries is it hosted, and by which hosting provider?		
Is it encrypted in transit and at rest, and who holds the keys?		
How is our data kept apart from your other customers' data?		
How long do you keep each kind of data, and can we change that?		

What to prepare: A data-flow diagram from the terminal's systems to yours and back · The hosting locations and providers · The encryption used in transit and at rest, and the key management · A retention table by kind of data

> **Model answer** (fill in the brackets with what you really do): We process [list of data], of which [list] is personal data. It is hosted in [country] by [hosting provider]. Data is encrypted in transit and at rest; keys are managed by [who]. Each customer's data is kept in a separate [database / tenant] and our staff read it only for a support ticket you opened. We keep [data] for [period], and you can ask for a shorter period.

Sources: ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13) · NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01)) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

3. Logs

Without logs, a terminal cannot see what happened in your software, nor send it to its own monitoring. Logging that costs extra or cannot leave your platform is a common blocker.

Question	Answer	Evidence / comment
What do you log (logins, administrator actions, changes of settings, API calls, data exports)?		
How long do you keep the logs, and are they protected against change?		
Can we receive the logs in our own monitoring tool (SIEM), in a standard format, at no extra cost?		
Are the clocks of your systems synchronised, so that times match ours?		

What to prepare: A catalogue of the events you log, with one example of each · The retention period and how logs are protected · The export options (syslog, JSON over HTTPS, a file drop) and their format

> **Model answer** (fill in the brackets with what you really do): We log logins, administrator actions, changes of settings, API calls and data exports, with the user, the time and the source address. Logs are kept [period] and cannot be changed by the people they record. We send them to your SIEM by [syslog / HTTPS] in [format], at no extra cost. All our servers are time-synchronised.

Sources: CISA, Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem (2024-08) · CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (2025-01-13) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28)

4. Backups

A terminal works around the clock. If your service stops or its data is encrypted by ransomware, the terminal wants to know how fast it comes back and with how much data lost.

Question	Answer	Evidence / comment
How often is our data backed up, and where are the backups kept?		
Are backups separated from the production systems, so that one attack cannot reach both?		
When did you last restore from a backup as a test, and what was the result?		
How long does it take to restore the service, and how much data can be lost at most?		

What to prepare: The backup schedule and the backup locations · How backups are isolated (offline, immutable, another account) · The date and the report of the last restore test · The restore time and the maximum data loss you commit to

> **Model answer** (fill in the brackets with what you really do): Your data is backed up every [frequency] to [location], separate from production and protected against deletion for [period]. We tested a full restore on [date]; it took [time]. We commit to restore the service within [time] with at most [time] of data lost, and we will show you the next restore test.

Sources: IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13)

5. Incidents

In the European Union, an operator in scope of NIS2 sends an early warning within 24 hours of becoming aware of a significant incident, and a notification within 72 hours. It can only meet that if its suppliers tell it fast.

Question	Answer	Evidence / comment
How and how fast will you tell us about an incident that affects our data or our service?		
Who is our contact during an incident, and can we reach them at any hour?		
What will your first notice contain, and how will you keep us updated?		
Will you help us with our own notifications to the authorities, and share what you learned afterwards?		

What to prepare: Your incident response plan, or its summary · A 24/7 contact and the escalation path · A template of the first notice · An example of a post-incident report, anonymised

> **Model answer** (fill in the brackets with what you really do): We notify your named contact by [phone and e-mail] within [time] of confirming an incident that affects your data or your service. Our first notice says what happened, what is affected, what we have done and what we ask you to do; updates follow every [period] until it is closed. Our incident line answers at any hour. We give you the facts you need for your own notifications, and a written report within [period].

Sources: Directive (EU) 2022/2555 (NIS2), Articles 21 and 23 (2022-12-14) · IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4 (2026-05-28) · NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01))

6. Subcontractors

Your suppliers become the terminal's suppliers. The risk does not stop at your company, and the terminal needs to know who else touches its data or its systems.

Question	Answer	Evidence / comment
Which subcontractors (hosting, support, development, monitoring) touch our data or our systems?		
Where are they, and what do they have access to?		
Do your security requirements apply to them in their contracts?		
Will you tell us before you add or change a subcontractor?		

What to prepare: The list of subcontractors, their role, their country and their access · The security clauses you pass on to them · Your rule for telling customers about a change

> **Model answer** (fill in the brackets with what you really do): [Number] subcontractors touch your data or systems: [hosting provider] for hosting in [country], [provider] for [role]. Each is bound by the same security requirements we accept with you, in their contract. We will tell you [period] before adding or changing one, and you may object.

Sources: NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01)) · ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13) · Directive (EU) 2022/2555 (NIS2), Articles 21 and 23 (2022-12-14)

7. Penetration tests

A terminal wants proof that someone outside your team has tried to break your software, and that what they found was fixed. It also wants to know how you handle vulnerabilities found later.

Question	Answer	Evidence / comment
When was your software last tested by an independent penetration tester, and what was in scope?		
Can we see a summary of the findings and how each one was fixed?		
May we, or a tester we choose, test the service we use?		
Do you publish a vulnerability disclosure policy, and how fast do you fix critical vulnerabilities?		

What to prepare: The date, the scope and the tester of the last test · A summary of findings and fixes that you can share · Your rules for a test by the customer · Your vulnerability disclosure policy and your patching times

> **Model answer** (fill in the brackets with what you really do): An independent firm tested [scope] on [date]. We share the summary of findings and the fix for each one under non-disclosure. You may test the service you use, with [notice] notice and the rules of engagement we agree. Our vulnerability disclosure policy is published at [URL]; we fix critical vulnerabilities within [time].

Sources: CISA, Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem (2024-08) · CISA and partner agencies, Secure by Demand: Priority Considerations for Operational Technology Owners and Operators when Selecting Digital Products (2025-01-13) · NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01))

8. End of contract

The day the contract ends, the terminal must get its data back, and be sure your company no longer holds it or can reach its systems.

Question	Answer	Evidence / comment
In which format do we get our data back, and how long do you take?		
How do you delete our data, including backups, and do you confirm it in writing?		
How are your accesses, accounts and keys to our systems removed?		
What help do you give to move to another system?		

What to prepare: The export formats and the time to deliver them · Your deletion procedure, backups included, and a deletion certificate template · The checklist of accesses and keys removed at the end · The transition support you offer

> **Model answer** (fill in the brackets with what you really do): At the end of the contract, we deliver your data in [format] within [time]. We then delete it from production and from backups within [period], and confirm it in writing. All our accounts, accesses and keys to your systems are removed on the last day, and we send you the checklist. We support the move to another system for [period].

Sources: ENISA, Good Practices for Supply Chain Cybersecurity (2023-06-13) · NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations (2022-05 (updated 2024-11-01))

Sources (public, dated)

IMO, Guidelines on maritime cyber risk management, MSC-FAL.1/Circ.3/Rev.4, 2026-05-28. https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.4.pdf

NIST SP 800-161 Rev. 1, Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations, 2022-05 (updated 2024-11-01). https://csrc.nist.gov/pubs/sp/800/161/r1/upd1/final

ENISA, Good Practices for Supply Chain Cybersecurity, 2023-06-13. https://www.enisa.europa.eu/publications/good-practices-for-supply-chain-cybersecurity

CISA, Secure by Demand Guide: How Software Customers Can Drive a Secure Technology Ecosystem, 2024-08. https://www.cisa.gov/resources-tools/resources/secure-demand-guide

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

Directive (EU) 2022/2555 (NIS2), Articles 21 and 23, 2022-12-14. 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 grid, including commercially, if you credit Port Cyber Alliance and link to https://portcyberalliance.org/resources/vendor-cyber-onboarding/ . Generic and anonymised: no terminal, port, client or vendor is named. Port Cyber Alliance does not certify vendors or audit terminals.