MAVERICK SECURITY

COMPLIANCE READINESS · MARITIME CYBER

USCG 33 CFR 101.650 CREW CYBER-TRAINING READINESS CHECKLIST

A practical, plain-English checklist to confirm your vessel or facility can demonstrate compliant crew cybersecurity training — before an inspector asks.

The U.S. Coast Guard's cybersecurity requirements at 33 CFR Part 101 are now in effect. The questions below mirror what an inspector or auditor can reasonably expect you to answer. Work through them per vessel or facility; any unchecked box is a gap worth closing now.

1 · KNOW YOUR OBLIGATION

- [ ] **Confirm the rule applies to your operation.** U.S.-regulated vessels and facilities under the Maritime Transportation Security Act fall within scope.
- [ ] **Identify who is accountable.** A designated person (e.g., CySO / DPA) owns the cyber requirements. §101.650(d)(2)
- [ ] **Confirm your training timeline.** Initial crew training was due by the rule's deadline; new personnel must be trained within the required window after joining.

2 · COVER THE REQUIRED TRAINING TOPICS

- [ ] **Threat recognition & awareness.** Crew can recognize phishing, social engineering, and suspicious activity. §101.650(d)(1)(i)
- [ ] **Detection & reporting of incidents.** Crew know what a cyber incident looks like and how to escalate it. §101.650(d)(1)(ii)
- [ ] **Cyber hygiene practices.** Passwords/MFA, removable media, personal device discipline. §101.650(d)(1)(iii)
- [ ] **Reporting procedures.** The chain and method for reporting, consistent with the SMS/security plan. §101.650(d)(1)(iv)

3 · HOLD THE RECORDS

- [ ] **Each crew member has a dated training record.** Tied to the named individual, not a generic roster note. §104.235 / §105.225 / §106.230
- [ ] **Records survive crew turnover.** Not paper logs that leave with the person — centrally retained and retrievable.
- [ ] **Records are independently verifiable.** An inspector can confirm authenticity without relying on your word alone.

4 · KEEP IT CURRENT

- [ ] **Training recurs on schedule.** Aligned with the annual cadence expected under IMO MSC-FAL.1/Circ.3 and your SMS.
- [ ] **New joiners are trained promptly.** A documented process catches every new crew member within the required window.
- [ ] **Content reflects current threats and rules.** Material is reviewed and updated, not frozen at first issue.

5 · BE INSPECTION-READY

- [ ] **You can produce records on request — today.** Port State Control can ask at any time; "we have a policy" is not the same as evidence.
- [ ] **Training is reflected in your SMS cyber-risk framework.** Crew training is one documented element of the wider system. `IMO MSC.428(98)`

NEED TO CLOSE THESE GAPS FAST?

DeckSecure delivers documented, verifiable crew cyber-awareness training mapped to every topic above — about two hours per crew member, in any browser. Maverick Security can also scope the wider SMS and compliance work. `mavericksecurityllc.com/decksecure`

> *This checklist is general guidance to support compliance planning and is not legal advice. Confirm specific obligations against the current regulatory text and your flag/Class requirements.*