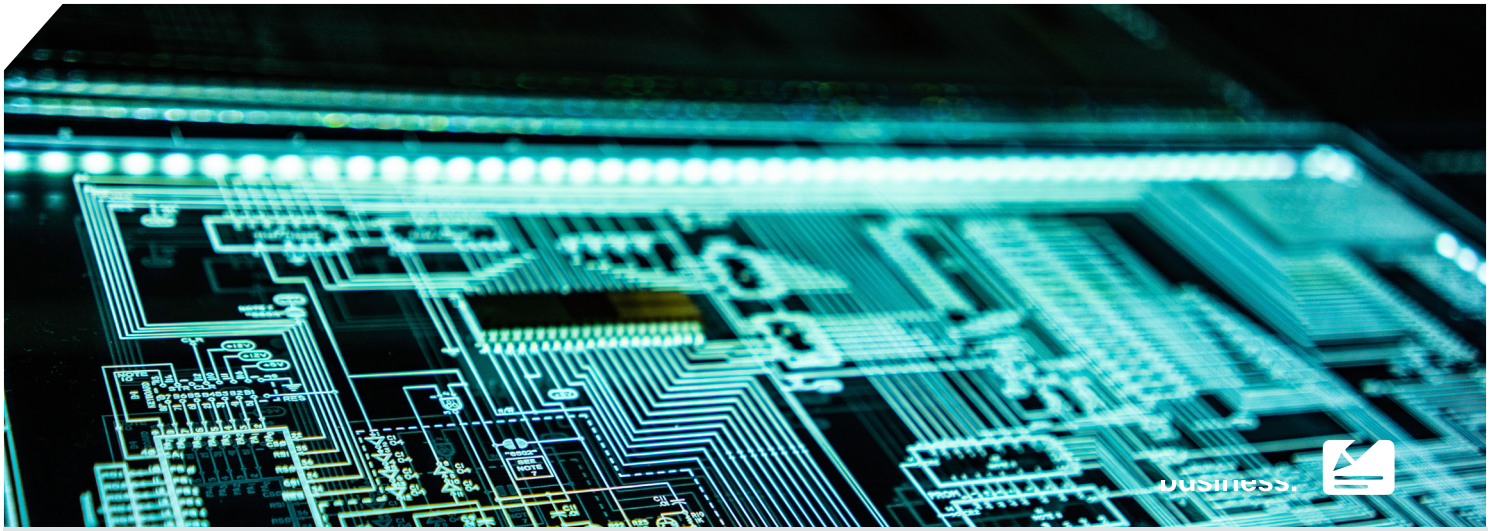

SMARTEN YOUR SHIP

Checklist Cyber Security.

Onboard security is one of the most important aspects you should consider when working in shipping, and technology obviously plays a very important role in this matter. If your software and installations are not secure, not compliant, nor adjusted to laws and regulations, you might find yourself in quite a few predicaments. But fear not, advanced security systems and software can help you identify and eliminate potential security threats or breaches to the ship. Even at sea, you are part of cyberspace, and this means security measures needs to be taken seriously. If you are uncertain about your security levels, please feel free to use this checklist to make sure you are all set and prepared to battle any upcoming cybervisits from pirates.

- ☐ Do I have routines for security breaches?
- ☐ Am I compliant? Is my security applicable to laws and regulations?
- ☐ Do I know what to do in case of a cyber attack?
- ☐ Do you have fire walls installed onboard?
- ☐ How do crew members use internet onboard?
- ☐ Do you transfer data between your ships or external partners that could carry a cybersecurity risk? How do you make sure this is secure?
- ☐ Do you know how to securely store your details on data transfer activities in the cloud?
- ☐ Do you utilize web interfaces to gain full control of your single data transfers?
- ☐ Do you keep a list of everyone receiving your security documents?
- ☐ Do you have essential reporting tools?
- ☐ Do you have full control that your CyberSecurity is “up-to-date”?
- ☐ Do you have full control that you are GDPR compliant with all your data onboard?
- ☐ Do you have state-of-the-art security systems in place onboard?
- ☐ Are all your security elements “up-to-date”? (and can you easily prove it)
- ☐ Do you have full control of all servers and clients?
- ☐ Do you have full control of backup/restores?
- ☐ Do you have automated setup of systems for new vessels?
- ☐ Do you have fully automated and monitored transfer systems of critical data?
- ☐ Do you have license management?
- ☐ How is Governance, Risk and Compliance handled in your company? GRC should be an ongoing, management-driven process that results in actionable security steps.
- ☐ Are you up-to-date on current vulnerabilities? The attackers are…
- ☐ Is information security left to the IT department, or is management actively involved?

Amesto
Smeltedigelen 1
0152 Oslo

t: +47 922 03 214
e: kontakt@amesto.no
w: amestosolutions.no

amesto