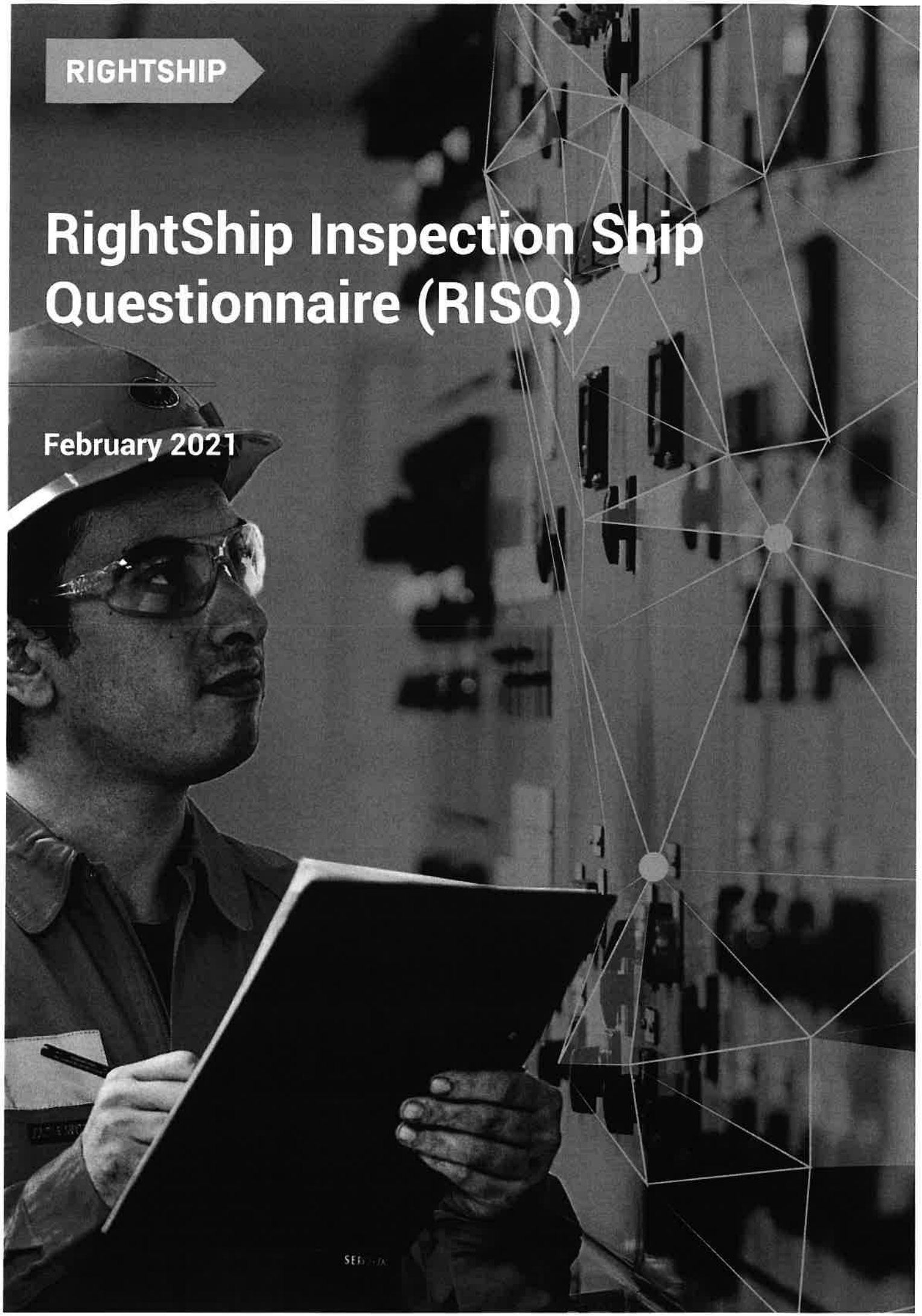
RIGHTSHIP

RightShip Inspection Ship Questionnaire (RISQ)

February 2021



12.6 **Have preventive measures been taken by the master and crew during the stay in port and prior to departure to prevent stowaways? (V)**

☐ Yes ☐ No ☐ N/A ☐ N/V

Guide to Inspection
The issue of stowaways is one which has existed ever since vessels began to trade. Procedures for the prevention of stowaways should be incorporated in the Safety Management System and should be effectively implemented by the master and the crew on board the ship.

12.7 **Are cyber security policies and procedures being incorporated in the safety management system and was the cyber security management system evaluated and certified by Class? (V)**

☐ Yes ☐ No ☐ N/A ☐ N/V

Guide to Inspection
Record N/C if cyber risk management has not been incorporated into the vessel's SMS by the company's first annual verification of the DOC after January 1, 2021. The cyber security management shall: > Identify the roles and responsibilities of users, key personnel, and management both ashore and on board > Identify the systems, assets, data and capabilities, which if disrupted, could pose risks to the ship's operations and safety > Implement technical measures to protect against a cyber-incident and ensure continuity of operations. This may include configuration of networks, access control to networks and systems, communication and boundary defence and the use of protection and detection software > Implement activities and plans (procedural protection measures) to provide resilience against cyber incidents. This may include training and awareness, software maintenance, remote and local access, access privileges, use of removable media and equipment disposal > Implement activities to prepare for and respond to cyber incidents. (The Guidelines on Cyber Security On board Ships, 2017) The cyber security management system shall be evaluated and certified based on international standards such as ISA 62443 4-2, IEC 61162-460.

12.8 **Are measures in place for controlling the use of removable media such as USB memory sticks, CDs, DVDs, and diskettes on shipboard computers? (V)**

☐ Yes ☐ No ☐ N/A ☐ N/V

Guide to Inspection
Removable media is a collective term for all methods of storing and transferring data between computers. This includes laptops, USB memory sticks, CDs, DVDs, and diskettes. Transferring data from uncontrolled systems to controlled systems represents a major risk of introducing malware. Removable media can be used to bypass layers of defences and can be used to attack systems that are otherwise not connected to the internet. A clear policy for the use of such media devices is essential; it must ensure that media devices are not normally used to transfer information between un-controlled and controlled systems. To avoid unauthorised access, removable media blockers should be used on all physically accessible computers and network ports. (The Guidelines on Cyber Security on board Ships, 2017) Critical equipment such as ECDIS should be protected from malware and virus attack. Access to USB and RJ-45 ports shall be controlled – i.e., disable or lock the ports.