

ARTICLE

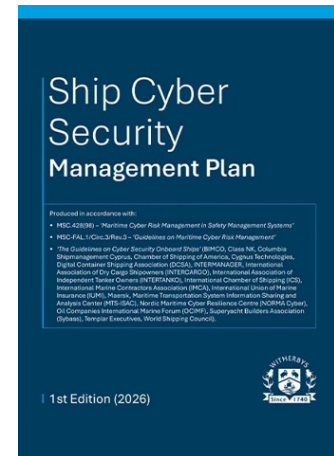
Ship Cyber Security Management Plan – 1st Edition 2026

Number: 6.67.0061

SPECIFICATIONS

Made in: United Kingdom

HS Code: 49011000



DESCRIPTION

This Ship Cyber Security Management Plan provides a structured framework for managing cyber risks to information technology (IT), operational technology (OT), safety and security functions on board ships.

Section 1 establishes the purpose and scope of the plan. The plan supports the incorporation of cyber risk management into the ship's Safety Management System in accordance with the ISM Code. IMO Resolution MSC.428(98) affirms that an approved Safety Management System should take cyber risk management into account in accordance with the objectives and functional requirements of the ISM Code, and encourages Administrations to ensure that cyber risks are addressed in safety management systems. MSC-FAL.1/Circ.3/Rev.3, Guidelines on Maritime Cyber Risk Management, provides the high-level recommendations that inform the structure of this plan.

Section 2 sets out roles, responsibilities and reporting procedures for managing cyber security on board and ashore. The ISM Code requires the company to define and document the responsibility, authority and interrelation of all personnel who manage, perform and verify work relating to and affecting safety and pollution prevention.

Section 3 provides for the identification and cataloguing of IT and OT assets on board. Effective cyber risk management begins with knowing what systems and devices are present, how they function and how they are connected. MSC-FAL.1/Circ.3/Rev.3 calls for companies to identify systems, assets, services, data, capabilities, interdependencies and network connections that, when disrupted, could pose risks to ship operations, safety, security, personnel or the environment.

Section 4 identifies the threat actors, types of threat and sources of threat information relevant to ship cyber security. Understanding the threat environment supports effective cyber risk assessment.

Section 5 sets out the process for assessing cyber risks to IT and OT systems on board using a 5x5 likelihood-impact matrix to assign risk scores ranging from 1 to 25.

Section 6 details the protective measures to be implemented based on the risk assessment results. These measures cover access control, network security, software management, removable media, and email and internet use.

Section 7 addresses the processes for detecting cyber security anomalies and incidents. This section provides for network traffic monitoring, review of system logs, monitoring of antivirus alerts and crew reporting procedures as methods of detection.

Section 8 establishes the procedures for responding to a cyber incident, including initial actions, isolation, notification, evidence preservation, the incident response plan and a reporting form.

Section 9 covers the cyber recovery plan and backup procedures. Recovery time objectives and recovery point objectives are introduced to support structured recovery planning.

Section 10 provides for the design and delivery of a cyber security training programme, including training frequency, drill scenarios, crew familiarisation on joining and a training record.

Systematic use of this plan enables the Master, the shipboard person assigned cyber security duties, and the company to:

- identify, assess and mitigate cyber risks to IT and OT systems on board through a structured risk assessment process;
- maintain a comprehensive, up-to-date inventory of cyber-enabled assets on the ship;
- establish clear roles, responsibilities and reporting procedures for cyber security management at the ship and company level.

Produced in accordance with:

- MSC.428(98) - 'Maritime Cyber Risk Management in Safety Management Systems'
- MSC-FAL.1/Circ.3/Rev.3 - 'Guidelines on Maritime Cyber Risk Management'
- 'The Guidelines on Cyber Security Onboard Ships' (BIMCO, Class NK, Columbia Shipmanagement Cyprus, Chamber of Shipping of America, Cygnus Technologies, Digital Container Shipping Association (DCSA), INTERMANAGER, International Association of Dry Cargo Shipowners (INTERCARGO), International Association of Independent Tanker Owners (INTERTANKO), International Chamber of Shipping (ICS), International Marine Contractors Association (IMCA), International Union of Marine Insurance (IUMI), Maersk, Maritime Transportation System Information Sharing and Analysis Center (MTS-ISAC), Nordic Maritime Cyber Resilience Centre (NORMA Cyber), Oil Companies International Marine Forum (OCIMF), Superyacht Builders Association (Sybass), Templar Executives, World Shipping Council).