TUVALU SHIP REGISTRY

Singapore Operations Office:
10 Anson Road #25-16, International Plaza, Singapore 079903
Tel: (65) 6224 2345 Fax: (65) 6227 2345
Email: info@tvship.com Website: www.tvship.com

MARINE CIRCULAR

MC-4/2017/1

04/2026

FOR: Ship Owners, Ship Managers, Ship Operators, Ship Masters, Ship Officers, Recognized Organizations, Flag State Inspectors

SUBJECT: GUIDELINES ON MARITIME CYBER RISK MANAGEMENT

DEFINITIONS:

The following abbreviations stand for:

- "IMO" – International Maritime Organization
- "ISM" – International Safety Management (Code)
- "MSC" – Maritime Safety Committee
- "RO" – Recognized Organization as defined by IMO Resolution MSC.349(92)
- "SMS" – Safety Management System

The term "Administration" shall mean the Tuvalu Ship Registry.

PURPOSE:

This marine circular serves to provide Administration's requirements for incorporating the following IMO guidance on maritime cyber risk management into the SMS (ISM Code) of Company and Tuvalu flagged vessels, ensuring that cyber risks are being addressed and properly identified, assessed and managed as part of the overall safety management framework:

1. IMO Resolution MSC.428(98)
2. IMO MSC-FAL.1/Circ.3/Rev.2
3. IMO MSC-FAL.1/Circ.3/Rev.3

REFERENCES:

a) IMO Resolution MSC.428(98) – Maritime Cyber Risk Management in Safety Management Systems, 16 June 2017
b) IMO MSC-FAL.1/Circ.3/Rev.2 – Guidelines on Maritime Cyber Risk Management, 7 June 2022
c) IMO MSC-FAL.1/Circ.3/Rev.3 – Guidelines on Maritime Cyber Risk Management, 4 April 2025

APPLICATION:

This circular applies to all Tuvalu flagged vessels.

CONTENTS:

1. INTRODUCTION

Cyber technologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and the protection of the marine environment.

The IMO recognizes the vulnerabilities of these technologies to cyber risks and cyber threats and noting that the rapidly changing technologies and threats makes it difficult to address these risks only through technical standards, the IMO has recommended that cyber risks are addressed in existing Safety Management Systems required by the ISM Code.

Thus, on 16 June 2017, the IMO adopted Resolution MSC.428(98), “Maritime Cyber Risk Management in Safety Management Systems”.

2. REQUIREMENTS

2.1. Mandatory Integration into SMS (IMO MSC.428(98))

2.1.1. Companies shall incorporate cyber risk management into their SMS and document processes for:
- 2.1.1.1. Identification of cyber-dependent systems
- 2.1.1.2. Risk assessment and prioritization
- 2.1.1.3. Preventive and protective measures
- 2.1.1.4. Detection, contingency planning, and response
- 2.1.1.5. Recovery and restoration procedures

2.1.2. Cyber risk management shall be addressed during:
- 2.1.2.1. ISM audits
- 2.1.2.2. Interim, initial, annual, and renewal Document of Compliance (DOC) and Safety Management Certificate (SMC) audits

2.2. Alignment with IMO MSC-FAL.1/Circ.3/Rev.2 & Rev.3

2.2.1. The company’s cyber risk management framework should follow the IMO-recommended functional approach, including:
- 2.2.1.1. Identify – Systems, networks, vulnerabilities, and potential threat scenarios
- 2.2.1.2. Protect – Technical, procedural, and physical safeguards
- 2.2.1.3. Detect – Monitoring, alerts, and incident recognition mechanisms
- 2.2.1.4. Respond – Containment, communication, and continuity procedures
- 2.2.1.5. Recover – Restoration, validation, and lessons learned

2.2.2. MSC-FAL.1/Circ.3/Rev.3 (2025 revision) emphasizes:
- 2.2.2.1. Increased cyber-dependence of OT/IT shipboard systems
- 2.2.2.2. Supply-chain and vendor-related cyber risk exposure
- 2.2.2.3. Software/hardware version control
- 2.2.2.4. Network segmentation and hardening
- 2.2.2.5. Enhanced crew competence and awareness
- 2.2.2.6. Integration of cyber risks into emergency drills and exercises

Companies shall ensure their cyber management approach is consistent with this latest revision.

2.3. Minimum cyber risk management elements required

2.3.1. Companies shall, as a minimum, ensure the SMS includes documented procedures covering:
- 2.3.1.1. Asset inventory of critical OT and IT systems
- 2.3.1.2. Assessment of cyber vulnerabilities and threat likelihood
- 2.3.1.3. Procedures for software updates, patching, and configuration control
- 2.3.1.4. Access control measures, including password policy and authorization levels
- 2.3.1.5. Secure communications, including email and data exchange
- 2.3.1.6. Bridge and engine control system protection (navigation, propulsion, ECDIS, GMDSS, etc.)

2.3.1.7. Management of portable devices, removable media, and external contractors
2.3.1.8. Cyber incident response plan, including reporting lines
2.3.1.9. Business continuity and recovery plan
2.3.1.10. Cyber training and drills for crew and office personnel
2.3.1.11. Documentation and record-keeping of cyber-related incidents

2.4. Role of Recognized Organizations (ROs)

2.4.1. ROs shall verify the integration of cyber risk management into the SMS during all ISM audits in accordance with MSC.428(98).

2.4.2. ROs shall ensure that any deficiencies or failures of implementation are to be rectified accordingly.

2.5. Reporting of cyber incidents

2.5.1. Any cyber incident affecting:
2.5.1.1. Safety of navigation
2.5.1.2. Operational capability
2.5.1.3. Security systems
2.5.1.4. Cargo handling
2.5.1.5. Propulsion or steering systems

shall be reported immediately to the RO.

2.5.2. Reports shall include impact assessment, mitigation actions and recovery status.

Yours sincerely,

Deputy Registrar
Tuvalu Ship Registry