	TECHNICAL NOTICE **TN 03-2021** **(ISM Code)**	**Issue date:** 27-01-2021 **Validity date:** - **Page:** 1 of 2

Subject: Implementation of Maritime Cyber Risk Management in Safety Management Systems.

1. Applicability.

The provisions of this Technical Notice are applicable to the Company's Safety Management Systems (SMS), approved in accordance with the objectives and functional requirements of the ISM Code.

2. Background.

.1 Through Resolution MSC.428(98), and recognizing the urgent need to raise awareness on cyber risk threats and vulnerabilities to support safe and secure shipping, which is operationally resilient to cyber risks, the Maritime Safety Committee affirms that an approved SMS should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code.

.2 Cyber risk management, as part of an approved SMS, should be carried out in accordance with Guidelines on maritime cyber risk management established in **MSC-FAL.1/Circ.3**, which provides high-level recommendations for maritime cyber risk management to safeguard shipping from current and emerging cyberthreats and vulnerabilities. The Guidelines also include functional elements that support effective cyber risk management.

.3 Cyber risk management means the process of identifying, analysing, assessing, and communicating a cyber-related risk and accepting, avoiding, transferring, or mitigating it to an acceptable level, considering costs and benefits of actions taken to stakeholders.

.4 Cybertechnologies have become essential to the operation and management of numerous systems critical to the safety and security of shipping and protection of the marine environment. In some cases, these systems are to comply with international standards and Flag Administration requirements. However, the vulnerabilities created by accessing, interconnecting or networking these systems can lead to cyber risks which should be addressed. Vulnerable systems could include, but are not limited to:

a) Bridge systems;
b) Cargo handling and management systems;
c) Propulsion and machinery management and power control systems;
d) Propulsion and machinery management and power control systems;
e) Access control systems;
f) Passenger servicing and management systems;
g) Passenger facing public networks;
h) Administrative and crew welfare systems; and
i) Communication systems.

.5 Threats are presented by malicious actions (e.g. hacking or introduction of malware) or the unintended consequences of benign actions (e.g. software maintenance or user permissions). In general, these actions expose vulnerabilities (e.g. outdated software or ineffective firewalls) or exploit a vulnerability in operational or information technology. Effective cyber risk management should consider both kinds of threat.

.6 Effective cyber risk management should ensure an appropriate level of awareness of cyber risks at all levels of an organization. The level of awareness and preparedness should be appropriate to roles and responsibilities in the cyber risk management system.

.7 For detailed guidance on cyber risk management, users of the Guidelines on maritime cyber risk management established in MSC-FAL.1/Circ.3, should also refer to Member Governments' and Flag Administrations' requirements, as well as relevant international and industry standards and best practices.

3. Relevant documentation.

.1 Resolution MSC.428(98)-Maritime Cyber Risk Management in Safety Management Systems.
.2 MSC-FAL.1/Circ.3- Guidelines on maritime cyber risk management.
.3 ICS Class Technical Instructive PO02-TI06-Statutory Certification for ISM Code-Company (DOC).

4. Provisions.

.1 After 01 January 2021, and no later than the first applicable Document of Compliance (DOC) verification (interim, initial, annual, renewal), the ISM auditor should verify the implementation of Maritime Cyber Risk Management in Safety Management System, in accordance with the Guidelines on maritime cyber risk management established in MSC-FAL.1/Circ.3.

5. Updated Forms.

In accordance with the Guidelines on maritime cyber risk management established in MSC-FAL.1/Circ.3, the following forms have been updated:

.1 ISM Code/DOC-Checklist for Company Review (2021/01)- Added new Section 13.
.2 ISM Code/DOC-Checklist for Annual Verification (2021/01)- Added new Section 13.
.3 ISM Code/DOC-Checklist for Interim Certification (2021/01)-Added new items from Nº. 30 to 35.

Jose A. Pérez Samper.
Principal Surveyor / samper@intermaritime.org
Tel. +507 322-0013 / Fax +507 226-5386
www.InterMaritime.org