



## Technical Information

Code: TI-20-13

Date: 19.07.2020

# Iranian Classification Society

### **Subject: MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS by Resolution MSC.428(98)**

#### **Introduction:**

The era of digitalization and rapid development of technologies in the maritime sector has called for immediate action, for the protection of the seafarers and the whole industry, which led the International Maritime Organization (IMO) to issue and implement a series of regulations and guidelines on cyber risk management, with, last but not least, the adoption of the Resolution MSC.428(98) which AFFIRMING that an approved safety management system should take into account cyber risk management in accordance with the objectives and functional requirements of the ISM Code. Cyber risk management means the process of identifying, analyzing, 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

#### **Compliance date:**

The resolution encourages administrations to ensure that cyber risks are appropriately addressed in existing safety management systems (as defined in the ISM Code) **no later than the first annual verification of the company's Document of Compliance after 1 January 2021.**

#### **IMO decision:**

- As the maritime community is becoming increasingly connected and vessel operators are growing dependent on digital solutions for optimization of operations, then, increasing number of control systems, communication and navigation systems, information management systems and devices are applied in ship cyber to realize external information interaction, cause rise to mounting potential cyber threats of ships. Cyber security is key to ensuring safe operation of vessels; and safeguarding people, cargo and the environment.
- In support of the Resolution, the IMO has issued a guideline on maritime cyber security management and recommend that all DOC holders carefully consider the guidance given. Below listed IMO guidance are attached.
  1. MSC-FAL.1/Circ.3 (GUIDELINES ON MARITIME CYBER RISK MANAGEMENT)
  2. IMO Cyber Risk Site:  
[http://www.imo.org/en/OurWork/Security/Guide\\_to\\_Maritime\\_Security/Pages/Cyber-security.aspx](http://www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/Cyber-security.aspx)
- DOC holders must assess their safety management systems' effectiveness for handling cyber security and develop appropriate measures.
- It must be noted that the DOC holder will remain responsible for having measures needed to ensure ongoing compliance and meeting objectives in the ISM Code and that decisions on compliance will remain with the formal statutory audits (DOC and SMC).

For any questions about this Technical Information, please contact:

Iranian Classification Society (ICS)

Convention & Legislation Department

Phone: +98-21-42186210

Fax: +98-21-88837744

E-Mail: [cld@ics.org.ir](mailto:cld@ics.org.ir)

Person in charge: Ehsan Ghoreifi

**Disclaimer:**

Although all possible efforts have been made to ensure correctness and completeness of the contents contained in this information service, the Iranian Classification Society is not responsible for any errors or omissions made herein, nor held liable for any actions taken by any party as a result of information retrieved from this information service