KR
KOREAN REGISTER OF SHIPPING

TECHNICAL INFORMATION

NO. 2017-ETC-05 (E)

36,Myeongji ocean city 9-ro
Gangseo-gu, Busan, 618-814
Republic of Korea

Phone : +82-70-8799-8343
Fax : +82-70-8799-8339
E-mail : conaudit@krs.co.kr
Date : 25 July 2017

Person in charge: Jeong, Minyoung

Subject: Guidelines for cyber security in TMSA, RIGHTSHIP and ISM.

1. Outline

1) MSC 96 approved MSC.1/Circ.1526 ‘Interim guideline on maritime cyber risk management’ first. After then, ‘Circular on Guidelines on maritime cyber risk management’(MSC-FAL.1/Circ.3) was approved in MSC 98, and MSC 98 adopted a MSC resolution that administrations are encouraged to ensure that cyber risks are appropriately addressed in safety management systems.

2) TMSA3 (Tanker Management and Self-Assessment)
OCIMF updated the KPI (Key Performance Indicator) and BP (Best Practice) as part of the existing TMSA2 streamlining and published the TMSA3 with the addition of the Element 13 (Maritime Security) item including cyber security.

3) RIGHTSHIP INSPECTION (INSPECTION AND ASSESSMENT REPORT FOR DRY CARGO SHIPS)
RIGHTSHP updated the RIGHTSHIP checklist (FOD06 (11) /11 May 2017) to reflect the additional check items including the cyber security on the existing ship checklist (FOD06 (10)).

Therefore, All shipping companies are recommended to reflect cyber security risk management to safety management system of the company, and, especially, shipping companies that inspect the above Oil Major and Rightship audit/inspection should review the added cyber security related audit/inspection items and reflect them in the company system.

2. Applicability

1) ISM applicable shipping company

2) Tanker company scheduled for the TMSA3 audit

3) Company and ships scheduled for the Rightship inspection
- Ships classified as High Risk
- PSC detention vessel
- Owner and Technical manager change
- Major part repair and modifications
- All Cape sized vessels over 18 years
- All Panamax sized vessels over 18 years
- All Handy sized vessels over 25 years
- The vessel requested by the Customer for inspection (no tonnage limit)

3. Effective date

1) It was agreed that administrations are encouraged to ensure that cyber risks are appropriately addressed in safety management systems no later than the first annual verification of the company's Document of Compliance after 1 January 2021. (This resolution is recommendatory in nature)

2) TMSA3 : 1 January 2018

① Since 1 January 2018
- Use of TMSA 3 (Only)

② From 10 April 2017 to 31 December 2017
- Select between TMSA 2 continuous use or TMSA 3 introduction
- When introducing the TMSA 3 for the first time,
  - ► Enter TMSA3 content in blank template
  - ► Or, move data (TMSA 2 → TMSA 3)

3) RIGHTSHIP: 11 May 2017

4. Requirements for ship owners and operators

Ship owners and operators should refer to MSC 98, TMSA3 and RIGHTSHIP decision and revisions related to cyber security to ensure that the company system can be established and implemented in terms of company's cyber security policies, procedures, instruction, threat identification, personnel training, and security system inspection and etc.

5. Reference information(Attachments)

1) MSC. Res.428(98) MARITIME CYBER RISK MANAGEMENT IN SAFETY MANAGEMENT SYSTEMS
2) TMSA3 and RIGHTSHIP Cyber security Guideline

-END-

Executive Vice President of Statutory Division

Distributions : Ship owners & Operators

Disclaimer : Although all possible efforts have been made to ensure correctness and completeness of the contents contained in this information service, the Korean Register of Shipping 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.