TMSA 3 (Tanker Management and Self-Assessment)

(The date of revision:2017.04.10 / Date of enforcement:2018.01.01.)

□ Element 13 Maritime Security

1. Main Objective

1) To provide a safe and secure working environment by developing a proactive approach to security management

2) To mitigate security risks and minimize the consequences of any breaches of security affecting, or potentially affecting, personnel and assets at all company locations.

2. Security Management

Effective security management requires the systematic identification of threats in all areas of the company's business, with measures implemented to mitigate risks to the lowest practical level.

1) Security plans cover all aspects of their activities.

2) Procedures are in place to identify threats covering all business activities.

3) Measures to mitigate and respond to identified threats are in place.

4) Security information is managed and reviewed.

5) Procedures are in place for the reporting of actual incidents and potential threats.

6) Personnel receive appropriate security training applicable to their responsibilities.

7) Risk assessment of activities are undertaken to identify and mitigate potential security threats.

- Procedures include identification of threats to cyber security, with appropriate guidance and mitigating measures in place and the active promotion of awareness.

8) The travel policy include provision for minimizing security threats to personnel.

9) Security procedures are regularly updated taking into account latest industry guidance.

10) Security management is included in the internal audit programme.

11) Assessments and exercises are undertaken to test preparedness.

12) Independent specialist support is provided, as appropriate, to respond to identified threats.

13) Vessels are provided with enhanced security and monitoring equipment.

14) Security enhancements are considered for inclusion in refit specifications and new build designs.

15) Innovative security technology is tested and implemented as appropriate.

3. Cyber security requirements(included in Element 13 Maritime Security)

No.	KPI	BP
13.1.2	The company has documented procedures in place to identify security threats applicable to vessels trading areas and shore-based locations.	①Security threats may include: -Petty theft -vandalism -Stowaways -Cargo theft -Cyber threat -Inadequate port security

		-Trafficking of people, arms or drugs. -Smuggling -Piracy -Sabotage and arson -Terrorism and its subsequent effects. ②The identified threats are reviewed as required by changes in circumstance.
13.2.3	Policy and procedures include cyber security and provide appropriate guidance and mitigation measures.	①Risks to IT systems may include: -Deliberate and unauthorised breaches. -Unintentional or accidental breaches -Inadequate system integrity, such as firewalls and/or virus protection ②System with direct or indirect communication links, which may be vulnerable to external threat or inappropriate use, are identified. ③These may include navigation, engineering, control and communication systems. ④In developing procedures, the company may refer to relevant current industry guidance.
13.2.4	The company actively promotes cyber security awareness.	①Effective means are used to encourage responsible behaviour by shore-based personnel, vessel personnel and third parties. ②Such behaviour may include: -Locking of unattended work stations. -Safeguarding of passwords. -No use of unauthorised software. -Responsible use of social media. -Control/prevention of misuse of portable storage and memory sticks.
13.3.2	Security procedures are updated taking into account current guidance.	Industry guidance may include: ▸Guidelines on cyber security from industry and Class.
13.4.5	The company is involved in the testing and implementation of innovative security technology and systems.	①This may include: -Physical measures to improve security -Software enhancement to IT systems.

RIGHTSHIP INSPECTION CHECKLIST

(The date of revision and enforcement : 2017.05.11.)

□ 4.7 Cyber Security

No.	Items
4.7.1.	Does the vessel and/or company have documented software/firmware and hardware maintenance procedures?
4.7.1.1	Are service reports available?
4.7.2	Does the vessel and/or company have any cyber security procedures?
4.7.2.1	Has a Risk Assessment for Cyber attack been completed?
4.7.2.2	Is a Cyber attack Response Plan available?
4.7.3	Does the vessel and/or company provide any cyber security training?