

JAPAN P&I NEWS

To the Members

Cyber Security Measures Aboard Ships

We would like to advise Members that ClassNK has recently issued the "Guidelines for Cyber Security Management System for Ships [Second Edition]".

In this second edition, the contents have been updated with reference to the internationally recognised standards ISO/IEC 27001 and ISO/IEC 27002, and the evaluation criteria as well as required objective evidence applied in audits have been clarified. The alignment with external requirements in each evaluation criterion is also indicated. For full details and to download the Guidelines (PDF), please refer to [ClassNK website, "About CSMS Certification"](#).

It is essential for each vessel to ensure that cyber security measures are not treated as a temporary response, but are embedded into daily safety management to maintain and enhance their practical effectiveness. Cyber-attacks pose direct risks of major physical incidents—such as collisions and groundings resulting from a loss of steering or propulsion—as well as marine pollution and cargo damage, going far beyond mere data leaks. When reviewing your Cyber Security Management System (CSMS), which is already integrated into your Safety Management System (SMS), Members are recommended to assume specific, practical risks that are prone to occur in daily vessel operations and to utilise this opportunity to further reflect them into onboard operations and training.

- **Implementation of Risk Assessments and Continuous Improvement Based on Audit Findings**

To properly address cyber risks, it is essential to identify IT (Information Technology) and OT (Operational Technology) systems and to conduct regular risk assessments. Furthermore, regarding observations raised during external inspections or internal audits, it is recommended to receive advice and feedback from IT managers to evaluate the necessity of countermeasures. Rather than treating audit findings merely with temporary measures, it is important to verify system effectiveness through management reviews and maintain a continuous improvement cycle (PDCA) within the CSMS.

- **Handling of Service Engineers/Contractors and Network Management**

In daily ship operations, risks exist such as service engineers asking to print service reports using shipboard PCs or printers, or contractors mistakenly connecting surveillance camera LANs to communication LANs. To prevent the unauthorised connection of equipment, it is important to equip vessels with dedicated devices (terminals) for safe data transfer, establish company procedures for such scenarios and instruct the crew accordingly.

- **Restrictions on Personal Devices/USBs and Enhancement of IT Literacy**

Connecting personal USB drives to shared ship PCs to save or transfer data, accessing business Wi-Fi from personal smartphones or crew members setting up unauthorised private Wi-Fi access points all increase the risk

of malware infection. It is recommended to explicitly restrict such actions and to provide continuous education and awareness raising to continually enhance cyber security awareness among crew members.

- **Prompt Reporting of Incidents and Data Protection**

Operation must be based on the assumption that a vessel could fall victim to cyber incidents. When a cyber incident occurs or is detected, the essential first step to contain damage is to ensure a system for reporting without delay to IT managers and related parties to seek instructions. Furthermore, establishing data protection procedures—such as appropriately backing up ECDIS passage plans and locking them to prevent unauthorised editing—is indispensable.

- **Continuous Crew Education and Retention of Training Records**

To enhance the practical effectiveness of cyber security measures, it is essential not only to prepare manuals and procedures, but also to foster proper understanding and implementation by the crew members who operate them on site. Upon crew sign-on, ensuring thorough familiarisation with shipboard security rules (onboard training) is crucial, alongside conducting regular education and drills. Furthermore, appropriately retaining and managing records of conducted training enables companies to objectively verify and maintain rule adherence, thereby strengthening accident prevention capabilities across both ship and shore.

We will continue to provide the latest information and technical insights to assist our Members in preventing accidents.

Yours faithfully,

The Japan Ship Owners' Mutual Protection & Indemnity Association