Guidance for Cyber Resilience of Ships and Systems

(Development Review : For external opinion inquiry)

2025. 09.

Machinery Rule Development Team

Effective Date : 1 October 2025

(The contract date for ship construction)

Present	Amendment	Remark
CHAPTER 1 GENERAL **Section 1 General** **101. - 103. 〈same as the present Rules〉** **104. Class notations *(2025)*** Ships complying with the Guidance will be assigned with an additional following notation **1. 〈same as the present Rules〉** **2. Cyber Resilience+**: Ships having Cyber Resilience and implementing essential cyber security management system(CSMS) based on cyber risk management process in accordance with the requirements in **Ch 2, Sec 1** through **Sec 5** of this Guidance. **3. 〈same as the present Rules〉** 4. 〈newly added〉 **Section 2 - 3 〈same as the present Rules〉**	**CHAPTER 1 GENERAL** **Section 1 General** **101. - 103. 〈same as the present Rules〉** **104. Class notations *(2026)*** Ships complying with the Guidance will be assigned with an additional following notation **1. 〈same as the present Rules〉** **2. Cyber Resilience~~+~~(CSMS)**: Ships having Cyber Resilience and implementing essential cyber security management system(CSMS) based on cyber risk management process in accordance with the requirements in **Ch 2, Sec 1** through **Sec 5** of this Guidance. **3. 〈same as the present Rules〉** 4. IT systems additionally requested by the applicant may be included within the scope of applicable systems in accordance with **103. 2**, and the class notation "**+**" may be additionally assigned to such ships (e.g., Cyber Resilience (CSMS)+). However, unless explicitly specified in this guidance for the additionally included IT systems, the requirements of **Ch 2** and **Ch 3** shall not be applied to such systems. **Section 2 - 3 〈same as the present Rules〉**	(Amended) -Revised that the name of the class notation in paragraph 2 is changed from "Cyber Resilience+" to "Cyber Resilience(CSMS)" (Newly added) -Add new provision to assign the additional class notation "+" to ships that include IT systems within the scope of application. -Add new provision that IT systems will be subject to separate regulations.

Present	Amendment	Remark
CHAPTER 2 CYBER RESILIENCE OF SHIPS **Section 1 General** **101. 〈same as the present Rules〉** **102. Application** **1. – 3. 〈same as the present Rules〉** **4.** The requirements of **Sec 4** of this Chapter additionally apply to ships having Class Notation of Cyber Resilience+. *(2025)* **5. 〈newly added〉**	**CHAPTER 2 CYBER RESILIENCE OF SHIPS** **Section 1 General** **101. 〈same as the present Rules〉** **102. Application** **1. – 3. 〈same as the present Rules〉** **4.** The requirements of **Sec 4 5** of this Chapter additionally apply to ships having Class Notation of Cyber Resilience~~+~~(CSMS). *(2026)* **5.** For ships assigned with the class notation of "**Cyber Resilience+**" or "**Cyber Resilience(CSMS)+**", the following requirements shall apply to the additionally included IT systems, as far as applicable: (1) 401.1 Vessel Asset Inventory (2) 402.1 Security Zones and Network Segmentation (3) 402.2 Network Protection Safeguards (4) 402.3 Antivirus, Antimalware, Antispam and Other Protections from Malicious Code (5) 402.4 Access Control (6) 402.7 Use of Mobile and Portable Devices	(Amended) –Modify the wording according to the change of the name of the class notation (Newly added) –Add new provision to be applicable to IT systems in the scope of application of ships with the class notation "+"

Present	Amendment	Remark
Section 2 Survey *(2025)*	**Section 2 Survey *(2025)***	
201. 〈same as the present Rules〉	**201. 〈same as the present Rules〉**	
202. Classification Survey	**202. Classification Survey**	
1. During Design and Construction phase	**1. During Design and Construction phase**	
(1) – (4) 〈same as the present Rules〉 (5) 〈newly added〉	(1) – (4) 〈same as the present Rules〉 (5) For ships assigned with the class notation "**Cyber Resilience(CSMS)**", the following documents shall be additionally submitted for approval: (A) Ship Cyber Risk Assessment Report (B) Ship Cyber Risk Management Plan and Corrective Action Results (if applicable) (C) Ship Cyber Incident Response and Recovery Manual	(Newly added) –Add drawing list to be additionally approved during the newbuilding stage for ships with the class notation Cyber Resilience (CSMS).
2. 〈same as the present Rules〉	**2. 〈same as the present Rules〉**	
203. 〈same as the present Rules〉	**203. 〈same as the present Rules〉**	
Section 3 – 4 〈same as the present Rules〉	**Section 3 – 4 〈same as the present Rules〉**	

Present	Amendment	Remark
Section 5 Requirements for Ship Cyber Security Management System *(2025)* **1.1.1.** **501. General** **1. Application** (1) The requirements in this Section specify additional requirements for implementing the essential Cyber Security Management System(CSMS) based on the cyber risk management process in the operational phase of the ship. In addition to the requirements of this Section, the relevant requirements for Maintenance Survey in **Ch 2, 203.** for ship cyber resilience shall be basically complied with. (2) The requirements in this Section support compliance with the regulation for cyber risk management of ships as per IMO Resolution MSC.428(98). (3) 〈newly added〉	**Section 5 Requirements for Ship Cyber Security Management System *(2025)*** **1.1.2.** **501. General** **1. Application** (1) ~~The requirements in this Section specify additional requirements for implementing the essential Cyber Security Management System(CSMS) based on the cyber risk management process in the operational phase of the ship. In addition to the requirements of this Section, the relevant requirements for Maintenance Survey in **Ch 2, 203.** for ship cyber resilience shall be basically complied with.~~ The requirements of this section specify the requirements for Cyber Security Management System (CSMS) of ships assigned with the class notation "**Cyber Resilience(CSMS)**". (2) ~~The requirements in this Section support compliance with the regulation for cyber risk management of ships as per IMO Resolution MSC.428(98).~~ Ships complying with the requirements of this section shall be deemed to satisfy the requirements for ship cyber risk management in accordance with IMO Resolution MSC.428(98). (3) Ships complying with the requirements of this Section shall, as a baseline, also comply with the relevant requirements of **Ch 2, Sec 1** through **4**, regarding ship cyber resilience.	(Amended) -The wording is revised to enhance clarity, and part of the existing requirements is included in new (3).

Present	Amendment	Remark
2. Limitation If any cyber security-related regulation required by International Conventions, flag state laws, or domestic laws of ports of call are not specified in this Guidance, they will not be included in the Surveys conducted by this Society, and the responsibility for the compliance with such regulations lies with the shipowner. (2) 〈newly added〉	**2. Limitation** (1) If any cyber security-related regulation required by International Conventions, flag state laws, or domestic laws of ports of call are not specified in this Guidance, they will not be included in the Surveys conducted by this Society, and the responsibility for the compliance with such regulations lies with the shipowner. (2) The requirements of this Section specify the minimum requirements for a cyber security management system based on the ship cyber risk management process during operation and do not imply the prevention of all cyber incidents.	(Newly added) -Added new disclaimer provision regarding the application of these requirements
3. Definition (1) Initial Survey: the first survey conducted upon the request of the shipowner for additional application of the requirements of this Section.	**3. Definition** (1) **CSMS** Initial Survey: the first survey conducted in accordance with the requirements of this Section after delivery of the ship. ~~upon the request of the shipowner for additional application of the requirements of this Section.~~ (Note) For ships assigned with the class notation "**Cyber Resilience(CSMS)**" during the construction, the CSMS initial survey shall be conducted at the time of the first annual survey.	(Amended) -Modifying the term "Initial Survey" to "CSMS Initial Survey" -Add the note to provide an interpretation of the timing of the CSMS initial survey for ships assigned for class notation Cyb0er Resilience(CSMS) during construction
502. Approval documents **1. Ship cyber security and resilience program** The Ship cyber security and resilience program shall conform to the requirements in **504.1**.	**502. Approval documents** **1. Ship cyber security and resilience program (hereinafter, CSMS Manual)** ~~The Ship cyber security and resilience program shall conform to t~~ ~~he requirements in **504.1**.~~ (1) Cyber security organization chart and job descriptions of security personnel (2) Cyber risk management policy (3) Cyber security education and training policy (4) Physical security policy (5) Outsider security policy (6) Internal audit procedures for ship cyber security	(Amended) -Added new abbreviation "CSMS Manual"

Present	Amendment	Remark
2. Documents or data for reference Shipowner shall submit the following for reference. (1) Ship cyber risk assessment report and risk management plan (2) Cyber security organization chart and job description of security personnel **3. Subsequent Annual Survey** The survey shall be carried out in accordance with the requirements of **503. 1** (2).	~~**2. Documents or data for reference**~~ ~~Shipowner shall submit the following for reference.~~ ~~(1) Ship cyber risk assessment report and risk management plan~~ ~~(2) Cyber security organization chart and job description of security personnel~~ **2. Ship Cyber Risk Assessment Report** (1) List of cyber threats (2) Cyber risk assessment results (3) Cyber risk management plan and corrective action results (if applicable) ~~**3. Subsequent Annual Survey**~~ ~~The survey shall be carried out in accordance with the requirements of **503. 1** (2).~~ **3. Cyber Incident Response and Recovery Plan** (1) Organization chart and emergency contact network for cyber incident response (2) Cyber incident response and recovery procedures **4. Data for reference** (1) Cyber security training record (2) Software security-related patch update records (3) Internal audit plan or results for cyber security	(Amended) -The list of approval documents specified in 504.1 is incorporated into 502.1 -The "Cyber security organization chart and job description" in the existing 502.2.(2) as a reference document, is included in the list of approval documents under 502.1 -Ship Cyber Risk Assessment Report in existing 502.2.(2) as a reference document is included in the list of approval documents under 502.2. (Newly added) -Added new provision to include “cyber incident response and recovery plan” in the list of approval documents under 502 (Amended) -Revised the wording in 4 to ensure consistency with the requirements in Appendix 2

Present	Amendment	Remark
503. Surveys	**503. Surveys**	
1. Initial Survey	**1. CSMS Initial Survey**	
(1) Approval of a document The shipowner shall submit the documents specified in **502.** and be approved by this Society before the initial survey according to this Section.	(1) Approval of a document The shipowner shall submit the documents specified in **502.** and be approved by this Society before the initial survey ~~according to this Section~~.	(Amended) -Revised the wording
(2) Survey During the initial survey, the shipowner shall provide this Society with the following evidence demonstrating the appropriate implementation of the requirements in **504.** However, the evidence is not limited to these items.	(2) Survey ~~During the initial survey, the shipowner shall provide this Society with the following evidence demonstrating the appropriate implementation of the requirements in **504.** However, the evidence is not limited to these items.~~ During the CSMS initial survey, the shipowner shall present to the attending surveyor the following evidence or objective records, demonstrating compliance with the relevant requirements of **504.** of this Chapter, based on the approved CSMS Manual.	(Amended) -Revised the wording of (1) for consistency by referring to the requirements in Appendix 2 -With regard to the survey items in (2), the items for "Implementation Status of Physical Security " and "Status of outsider security management" have been added by referring to the requirements in Appendix 2, and the item for "Cybersecurity Incident Report" has been removed.
(A) Ship cyber risk assessment report and risk management result	(A) Ship cyber risk assessment report and ~~risk management result~~ implementation status of cyber risk management plan	
(B) Cyber security training plan and result	(B) Cyber security training ~~plan and result~~ record	
(C) Cyber security incident report (if any)	(C) ~~Cyber security incident report (if any)~~ Implementation status of physical security	
(D) 〈newly added〉	(D) Status of outsider security management	
(D) Internal audit result related to cyber security	(E) Internal audit result related to cyber security	
(3) 〈newly added〉	(3) Issuance of CSMS Statement of Compliance (SoC) A CSMS Statement of Compliance shall be issued to a ship upon completion of the initial survey in accordance with the requirements of this Section.	(Newly added) -Added new provision for the issuance of a CSMS SoC
2. - 3. 〈same as the present Rules〉	**2. - 3. 〈same as the present Rules〉**	

Present	Amendment	Remark
504. Additional requirements **1. Cyber security policy** (1) Ship cyber security and resilience program The Ship cyber security and resilience program specified in **Ch 2, 203. 1** (2) shall additionally address the following policies: (A) Policy for cyber risk management (B) Roles and responsibilities for cyber security management (C) Policy for Crew Awareness and Training (D) Policy for internal audit regarding cyber security (2) The shipowner shall place, review and manage the Ship cyber security and resilience program onboard. (3) The shipowner shall designate and assign responsibility and authority to the personnel who have the competencies to operate and manage the program.	**504. Additional requirements** **1. Ship cyber security management policy** ~~(1) Ship cyber security and resilience program~~ ~~The Ship cyber security and resilience program specified in **Ch 2, 203. 1** (2) shall additionally address the following policies:~~ ~~(A) Policy for cyber risk management~~ ~~(B) Roles and responsibilities for cyber security management~~ ~~(C) Policy for Crew Awareness and Training~~ ~~(D) Policy for internal audit regarding cyber security~~ ~~(2) The shipowner shall place, review and manage the Ship cyber security and resilience program onboard.~~ ~~(3) The shipowner shall designate and assign responsibility and authority to the personnel who have the competencies to operate and manage the program.~~ (1) A CSMS manual, specifying the methods, procedures, and responsible personnel for the operation of the ship's CSMS shall be kept on board, regulary reviewed, and properly managed. (2) Personnel with the necessary competence to operate and manage the ship's CSMS shall be designated, with clear assignment of responsibilities and authority.	(Amended) -The list of approved documents previously included in 504.1.(1) shall be moved to 502.1 and removed from 504.1.(1). -The relevant requirement wording have been revised for consistency by referring to the requirements in Appendix 2

Present	Amendment	Remark
2. Cyber risk management (1) The shipowner shall establish a cyber risk management process, including identification, analysis, evaluation, and processing of cyber risks to CBS and networks in a ship. (2) Internal and external cyber threats that may adversely affect the operation of CBSs and networks on board ship shall be identified and listed. (3) The Cyber risk assessment for CBSs and networks on board ship shall be conducted periodically taking into account cyber threats and vulnerabilities. (4) Priorities for risk level shall be determined based on the results of the Cyber risk assessment, and improvement actions shall be taken if deemed necessary.	**2. Ship cyber risk management process** ~~(1) The shipowner shall establish a cyber risk management process, including identification, analysis, evaluation, and processing of cyber risks to CBS and networks in a ship.~~ ~~(2) Internal and external cyber threats that may adversely affect the operation of CBSs and networks on board ship shall be identified and listed.~~ ~~(3) The Cyber risk assessment for CBSs and networks on board ship shall be conducted periodically taking into account cyber threats and vulnerabilities.~~ ~~(4) Priorities for risk level shall be determined based on the results of the Cyber risk assessment, and improvement actions shall be taken if deemed necessary.~~ (1) A cyber risk management process, specifying the methods and procedures for identifying, analyzing, assessing, and addressing cyber risks related to onboard systems, equipment, and networks, shall be established and implemented. (2) Internal and external cyber threats that may negatively impact the operation of onboard systems, equipment, and networks shall be identified and documented. (3) A periodic cyber risk assessment shall be conducted, considering cyber threats and vulnerabilities affecting assets within the cyber security management scope. (4) Based on the results of cyber risk assessment, a risk management plan shall be established by prioritizing cyber risks, and appropriate mitigation measures shall be implemented.	(Amended) –The titles and requirement wording have been revised for consistency by referring to the requirements in Appendix 2.

Present	Amendment	Remark
4. Incident Response and Recovery (1) The shipowner shall define the roles and responsibilities of the organization or crews responsible for immediate response and recovery activities to system operation and security issues in a ship. (2) An emergency contact network shall be established and kept it up to date to enable prompt communication with internal and external personnel. (3) In the event of a cyber incident onboard ship, procedures shall be established and implemented to notify the appropriate competent authorities and report to the relevant person in charge.	~~**4. Incident Response and Recovery**~~ ~~(1) The shipowner shall define the roles and responsibilities of the organization or crews responsible for immediate response and recovery activities to system operation and security issues in a ship.~~ ~~(2) An emergency contact network shall be established and kept it up to date to enable prompt communication with internal and external personnel.~~ ~~(3) In the event of a cyber incident onboard ship, procedures shall be established and implemented to notify the appropriate competent authorities and report to the relevant person in charge.~~ **4. Physical Security** (1) Physical security policies shall be established and implemented to control unauthorized access to onboard systems, equipment, and facilities. (2) Physical access control measures shall be provided to ensure that only authorized personnel can access protected areas containing critical assets on board. (3) where access monitoring devices, such as CCTV, are installed for surveilience of protected areas, unauthorized access to the recording devices of such monitoring systems shall be controlled. (4) Upon installation of new systems on board, it shall be verified that at least the same level of physical security as existing systems is applied.	(Amended) -The requirement has been moved from 4 to 6. (Newly added) -A new requirement related to physical security has been established in 4 by referring to the requirements in Appendix 2.

Present	Amendment	Remark
5. Cyber security internal audit (1) Cyber security internal audit procedure shall be established and conducted periodically.	~~**5. Cyber security internal audit**~~ ~~(1) Cyber security internal audit procedure shall be established and conducted periodically.~~ **5. Outsider Security** (1) In order to prevent security incidents caused by outsiders on board, a security policies shall be established and implemented to control the use of mobile devices, data, as well as maintenance activities, by outsiders. (2) Outsiders shall be restricted from accessing shipboard systems and equipment, except where access is permitted under the supervision of onboard personnel. (3) Where temporary system access rights must be granted to outsiders on board, an appropriate approval procedure by the responsible person shall be followed. (4) Outsiders shall use the systems in compliance with the shipboard security procedures, and when connecting outsider-owned equipment to the systems, a prior security inspection shall be conducted.	(Amended) -The requirments in 5 has been moved to 7 (Newly added) -New provision related to outsider security has been added in 5 by referring to the requirements in Appendix 2.
6. 〈newly added〉	**6. Cyber Incident Response and Recovery Plan** (1) A cyber incident response and recovery plan, including the types of incidents and corresponding response methods and procedures, shall be maintained on board and kept up to date. (2) An organization and designated personnel responsible for immediate response to and recovery from cyber incidents affecting shipboard systems shall be established, and their roles and responsibilities shall be defined. (3) An emergency contact network shall be established and kept up to date to enable prompt communication with internal and external stakeholders. (4) Procedures shall be established and implemented for reporting to the appropriate competent authority and notifying the responsible persons in the event of a cyber incident. ⚓	(Amended) -The requirement has been moved from paragraph 4 to paragraph 6, and the title and wording have been revised for consistency by referring to the requirements in Appendix 2.