2019

GUIDANCE FOR MARITIME CYBER SECURITY SYSTEM

GC-24-E

KR

APPLICATION OF "GUIDANCE FOR MARITIME CYBER SECURITY SYSTEM"

1. Unless expressly specified otherwise, the requirements in the Guidance apply to companies and ships when the application for certification of maritime cyber security systems is dated on or after 1 March 2018.

2. The amendments to the Guidance for 2019 edition and their effective date are as follows;

Effective Date : 1 March 2019

CHAPTER 1 GENERAL

Section 1 General

- 101. 1 has been amended.
- 102. 1 and 13 have been amended.
- 102. 16, 17 and 18 have been newly added.
- 103. 1 and, 2 Notations have been amended. The following notations are unified.
- 103. 3, 4 and 5 have been newly added.

CHAPTER 2 CLASSIFICATION SURVEYS

Section 1 General

- 101. 4 has been newly added.
- 101. 5 (3) has been newly added.
- 101. 6 has been newly added.

Section 2 Surveys for registration of company

- 201. 1 has been newly added.
- 202. 1, 2, 3 and 4 have been amended.
- 202. 1 (2), (4), (9), (16), (17), (22), (24) and (25) have been amended.
- 202. 2 (3) has been amended.
- 203. 4, 5, 6 and 7 have been amended.
- 203. 4 (2), (4), (11) and (18) have been amended.
- 203. 4 (19), (20) and (21) have been deleted.
- 203. 5 (1) has been deleted.
- 203. 7 (1) and (2) have been amended.
- 204. 2 (3) and (4) have been amended.

Section 3 Surveys for registration of ship

- 301. 1 has been amended.
- 302. 1 has been newly added.
- 302. 2, 3, 4 and 5 have been amended.
- 302. 2 (9), (10) and (12) have been amended.
- 302. 3 (1) has been deleted.
- 303. 3 has been newly added.
- 303. 4, 5, 6 and 8 have been amended.

- 303. 4 (3), (5), (11), (18), (19) and (20) have been amended.
- 303. 4 (21) has been deleted.
- 304. 1 has been amended.
- 304. 2 (3) and (4) have been amended.

Section 4 Surveys for certification maintenance

- 401. 2 (2) has been amended.
- 402. 1 (1), (2) and (3) have been amended.
- 402. 1 (1) (C), (F) and (J) have been amended.
- 403. 1 (1), (2) and (3) have been amended.
- 403. 1 (1) (C) and (F) have been amended.

CHAPTER 3 REQUIREMENTS FOR CYBER SECURITY SYSTEM OF THE COMPANY

- "CHAPTER 3 REQUIREMENT FOR CSMS" has been divided into "CHAPTER 3 REQUIREMENTS FOR CS SYSTEM OF THE COMPANY" and "CHAPTER 4 REQUIREMENTS FOR CS SYSTEM OF THE SHIP."

CHAPTER 4 REQUIREMENTS FOR CYBER SECURITY SYSTEM OF THE SHIP

- "CHAPTER 3 REQUIREMENT FOR CSMS" has been divided into "CHAPTER 3 REQUIREMENTS FOR CS SYSTEM OF THE COMPANY" and "CHAPTER 4 REQUIREMENTS FOR CS SYSTEM OF THE SHIP."

CONTENTS

CHAPTER 1 GENERAL ····· 1
Section 1 General ····· 1

CHAPTER 2 CLASSIFICATION SURVEYS ····· 3
Section 1 General ····· 3
Section 2 Surveys for registration of company ····· 4
Section 3 Surveys for registration of ship ····· 6
Section 4 Surveys for certification maintenance ····· 9

CHAPTER 3 REQUIREMENTS FOR CS SYSTEM OF THE COMPANY ····· 11
Section 1 General ····· 11
Section 2 COMPANY CYBER SECURITY COMPLIANCE 1 ····· 11
Section 3 COMPANY CYBER SECURITY COMPLIANCE 2 ····· 16
Section 4 COMPANY CYBER SECURITY COMPLIANCE 3 ····· 18

CHAPTER 4 REQUIREMENTS FOR CS SYSTEM OF THE SHIP ····· 19
Section 1 General ····· 19
Section 2 CS Ready ····· 19
Section 3 CS1 (CS1(C)) ····· 22
Section 4 CS2 (CS2(C)) ····· 26
Section 5 CS3 (CS3(C)) ····· 28

CHAPTER 1 GENERAL

Section 1 General

101. Application

1. This Guidance is to apply to companies and ships with cyber security management ssystem for information and operating technologies.
2. This Guidance defines the level of cyber security management and its requirement according to the level, and the application scope is determined by request of the ship owner.
3. Items not specified in this Guidance are to be in accordance with each relevant requirement in **the Rules for the Classification of Steel Ships**(hereafter referred to as "**the Rules for Steel Ships**") except for the requirements inapplicable to cyber security system.
4. Items not included in this Guidance may comply with ISO, IEC or equivalent recognized standards by the appropriate consideration of the Society.
5. Where the specific requirements in international regulation such as IMO are or as Information technology & operating technology develops, when it deems necessary, additional requirements to this Guidance may be required.
6. This Guidance specifies the minimum requirements for cyber security system in companies and onboard of ships, which does not mean that all cyber security incidents can be prevented.

102. Definitions

The definitions of terms are to follow **the Rules for Steel ships**, unless otherwise specified in this Guidance.

1. Cyber security refers to process for protecting cyber assets by preventing, detecting and responding to cyber attacks.
2. Cyber security system refers to comprehensive system for maintaining the cyber security level required by the organization on the assets based on cyber security risk assessment.
3. Information technology refers to any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
4. Operation technology refers to devices, sensors, software and associated networking that monitor and control onboard systems.
5. Cyber incident refers to an occurrence, which actually or potentially results in adverse consequences to an onboard system, network and computer or the information that they process, store or transmit, and which may require a response action to mitigate the consequences.
6. Confidentiality refers to the property that information is not disclosed to system entities (users, processes, devices) unless they have been authorized to access the information.
7. Integrity refers to the property whereby an entity has not been modified in an unauthorized manner.
8. Availability refers to the property of being accessible and useable upon demand by an authorized entity.
9. Capability refers to the ability to perform certain actions.
10. Policy refers to the overall intent and direction of the company in related to the goals and ways officially mentioned by top management.
11. Risk refers to the likelihood that anticipated threats will occur and the expected loss incurred by those threats.
12. Ship Owner refers to the owner of the ship, the chaterer of the ship, the agents of the owner or the charterer and captain of the ship.

13. Recommendation refers to requirements to the effect that specific measures, repairs, surveys are to be carried out within a specific time limit in order to retain Classification.

14. Major Change refers to the change of major documents and assets related to cyber security system and the case that critical cyber threat was identified.

15. Change Management refers to the change of the configuration due to new installation of hardware and software, firmware update, patch, etc.

16. Primary Essential Services refers to those services which need to be in continuous operation to maintain propulsion and steering.

17. Secondary Essential Services refers to those services which need not necessarily be in continuous operation to maintain propulsion and steering but which are necessary for maintaining the vessel's safety.

18. Network refers to a single physical Ethernet network with one Internet address space. It consists of supporting equipment such as network nodes, switches, cables, and power supplies

103. Notation

1. Ships satisfying the requirements of this Guidance may be given a notation as additional special feature notations as follows:

(1) Where the ship is with basic cyber security system satisfying the requirements in **Ch. 4 Sec. 3**, a notation **"CS1(Cyber Security System 1)"** may be assigned.

(2) Where the ship is with enhanced cyber security system satisfying the requirements of CS1 and in **Ch. 4 Sec. 4**, a notation **"CS2(Cyber Security System 2)"** may be assigned.

(3) Where the ship is with advanced cyber security system satisfying the requirements of CS2 and in **Ch. 4 Sec. 5**, a notation **"CS3(Cyber Security System 3)"** may be assigned.

2. Additional notation is assigned to CS for the ship where the company certifies cyber security system. The notations are expressed as **CS1(C), CS2(C) or CS3(C)**.

3. New ships with the cyber security system satisfying the requirements in **Ch. 4 Sec. 2**. of this Guidance may be given a notation **"CS Ready."** However, CS Ready notation may be replaced with corresponding CS notation when the cyber system satisfies the requirements in **Ch. 4 Sec. 3**, **4** and/or **5**. of this Guidance at the request of the ship owners after the delivery.

4. Non-KR-classed ships satisfying the requirements of this Guidance will be issued a Certificate of Cyber Security System.

5. A Company with cyber security system satisfying the requirements in **Ch. 3** of this Guidance will be issued a Certification of Cyber Security Compliance. 1, 2 or 3 may be added to the Certificate depending on the security capabilities of the cyber security system.

104. Equivalence

Special equipment, which is not appropriate to apply the requirements of this Guidance or not specified in this Guidance, may be accepted by the Society provided that the Society is satisfied that such equipment is equivalent to or above those complying with the requirements of this Guidance.

105. Exclusion from the Guidance

The Society cannot assume responsibility for other technical characteristics for cyber security systems not covered by this Guidance. However, the Society may advise on such matters upon inquiry. ⚓

CHAPTER 2 SURVEYS

Section 1 General

101. General

1. Application

Surveys for cyber security system not specified in this Chapter are to be in accordance with each relevant requirement in **Pt 1 of the Rules for Steel Ships**. In addition, relevant requirements in ISM Code and ISPS Code should be satisfied.

2. Kinds of surveys

Kinds of surveys are as follows:

(1) Surveys for initial certification(hereinafter referred to as "Initial Surveys")
(2) Surveys for certification maintenance
  (A) Annual Surveys
  (B) Special Surveys
  (C) Occasional Surveys

3. Survey intervals

Surveys are to be carried out in accordance with the following requirements.

(1) Surveys for certification are to be carried out at the time when application for certification on cyber security system in companies and onboard of ships is made.
(2) Surveys for registration maintenance are to be carried out at the times as prescribed below.
  (A) Annual Surveys are to be carried out at intervals specified in **PT 1, Ch 2, 201** of the Rules for Steel Ships.
  (B) Special Surveys are to be carried out at intervals specified in **PT 1, Ch 2, 401** of the Rules for Steel Ships.
  (C) Occasional Surveys are to be carried out at the time specified in **401. 3**.

4. Survey targets

Survey targets of the ships are as follows:

(1) Systems for accessing ship information through remote access from land
(2) Control and monitoring systems for primary essential services transferring data to and from other onboard systems over via network connection
(3) Control and monitoring systems for secondary essential services transferring data to and from other onboard systems over via network connection
(4) Navigation and communication systems, required by SOLAS Chapter IV and V, transferring data to and from other onboard systems over via network connection
(5) Systems requested for survey by the shipowner

5. Duties of ship owners

(1) In case of any change affecting the cyber security system in companies and onboard of ships certified by the Society, the ship owners should notify the Society without delay.
(2) The documents related to cyber security system should be updated whenever they are revised, and they should be confirmed at survey.
(3) Ship owners are responsible for defining the system in consultation with the shipbuilder when applying for cyber security certification on the new ships.

6. Duties of shipbuilders

Ship builders should collect, maintain and update the documents related to the cyber security systems produced by the equipment companies or ship builders for obtaining the CS notation after delivery of the new ship on behalf of the ship owner, and provide them to the ship owners at the time of delivery.

Section 2 Initial Surveys for Company

201. General

1. In case of the company who wants to receive initial surveys on cyber security system in company to the Society, the application should be made after implementing cyber security system for more than 3 months.

2. Facilities and equipments of cyber security system in company are to be examined in accordance with the requirements in this Guidance.

202. Document review

1. The company applying the certification corresponding to Company Cyber Security Compliance 1 should submit three copies of the following documents for review.

(1) List and contacts of external cooperating organizations
(2) Policies, procedures and guidances related to cyber security system
(3) Cyber security organization chart and job description of security personnel
(4) Cyber security training plan and report
(5) List of Cyber security threats
(6) Cyber security risk management plan
(7) Cyber security related asset vulnerability diagnosis results
(8) Cyber security risk assessment report
(9) Improvement plan and results report
(10) List of assets and equipments and Status of the personnel in charge of assets
(11) Data importance classification table
(12) Access authority management policy
(13) Physical security policy
(14) Incident response and recovery policies
(15) Incident response organization chart and emergency contact network
(16) Mobile security policy
(17) Security policy for outsourcer
(18) Software introduction procedure
(19) Patch work / approval statements
(20) Remote Access Security Policy
(21) Encryption criteria
(22) Network configuration
(23) Change management procedures and application for change
(24) Cyber security operating statement
(25) Functional requirements / specifications
(26) Data backup and recovery criteria

2. In addition to **202. 1**, the company applying the certification corresponding to Company Cyber Security Compliance 2 should submit three copies of the following documents for review.

(1) Policy making/amendment approval statements
(2) Company security guidances and manuals
(3) Cyber security incident investigation analysis procedures
(4) Incident criteria classification table
(5) Organization chart for Cyber security investigation analysis
(6) Disaster recovery plan / scope definition
(7) Development security requirements
(8) Penetration test report
(9) Abnormal signs monitoring procedures and results

3. In addition to **202. 2**, the company applying the certification corresponding to Company Cyber Security Compliance 3 should submit three copies of the following documents for review.

(1) Policy and plan for cyber security audit
(2) Cyber security council structure chart
(3) Disaster recovery simulation training report
(4) Encryption key management procedure
(5) Security requirements for developed software source code

4. The companies should inform the Society of the results of the corrective action against any recommendations found during the document review and, if necessary, resubmit the document containing the results of the corrective action.

203. On-site surveys

1. Based on the company's cyber security related materials collected, the on-site surveys are to survey whether the confidentiality, integrity and availability of the cyber security system and related assets in the company can be maintained.
2. On-site surveys should be conducted after document review is completed.
3. The company should keep the materials on site for on-site surveys so that it can be confirmed on site by surveyors.
4. The following items should be surveyed during the on-site surveys for certification corresponding to Company Cyber Security Compliance 1.
   (1) Cyber security issue notices
   (2) Cyber security training plan and report
   (3) Results of absentee / special security training
   (4) Cyber security risk assessment and management report
   (5) Retiree security pledge
   (6) Outsourcer asset return document
   (7) Access authority change record
   (8) Special authorization classification table
   (9) Log monitoring procedures and results
   (10) Physical control measures
   (11) Intrusion prevention system policy status (if applicable)
   (12) Anti-virus program status
   (13) Data and communication encryption status
   (14) Remote access control status
   (15) Log archiving and monitoring procedures and results
   (16) Data backup management register
   (17) Data storage media discard management register
   (18) New software test and transfer report (if applicable)
5. In addition to **203. 4**, the following items should be surveyed during the on-site surveys for certification corresponding to Company Cyber Security Compliance 2.
   (1) Change management record
   (2) Remote user management register
   (3) Amendment history of cyber security guidances and manuals
   (4) Training and check results for the outsourcers
   (5) Approval statements for issuance of outsourcers' account
   (6) Vulnerability action plans and results
6. In addition to **203. 5**, the following items should be surveyed during the on-site surveys for certification corresponding to Company Cyber Security Compliance 3.
   (1) Special cyber security training report
   (2) Disaster recovery plan status
   (3) Network access control monitoring history
   (4) Encryption key change history
7. Recommendations corrective action and confirmation
   (1) The company should submit the results of corrective actions for the recommendations found through the on-site surveys of the requirements of this Guidance to the Society within 3 months after the on-site surveys, and the adequacy of the results should be reviewed by the Society.
   (2) The corrective actions and the security system should be finally verified by on-site re-surveys within 3 months after the notification of the corrective action, and the final result should be included in the survey report.

204. Survey report and certification issue

1. In case of the on-site survey items required in the Guidance have been passed, the Society provides the survey report and the certification for Cyber security system.
2. The survey report for cyber security should include at least following:
   (1) List of cyber security system and assets in company
   (2) List of documents for cyber security system in company
   (3) Operating statement
   (4) Corrective action results
   (5) Types, time and checklist of next surveys to maintain the certification for cyber security system

Section 3 Initial Surveys for Ship

301. General

1. In case of the Ship Owner who wants to receive initial surveys on cyber security system onboard of the ship to the Society, the application should be made after implementing cyber security system for more than 3 months. For a new ship, however, the application for survey may be made by the ship builder.
2. The Society reserves the right to decline the application for the survey where deemed necessary by the Society such as where the requested survey is not progressed after the application has been submitted so the intention of the survey application is not clear, where the survey fees are not paid, where the ship does meet the requirements of the Society, etc.

302. Document review

1. The ship builder who applies the CS Ready notation for the new ship should submit three copies of the following documents for review.
   (1) Basics of the ship
   (2) System functional requirements / statements / user manuals
   (3) List of cyber security related assets and equipments
   (4) Network configuration
   (5) Asset vulnerability diagnosis results
   (6) Penetration test results (if applicable)
   (7) List of cyber security threats
   (8) Cyber security risk assessment report
   (9) Corrective action plan and results
   (10) Software registry and quality plan
   (11) Incident response and recovery manuals
   (12) Cyber security test procedures
2. The ship owner who applies the CS1 notation for the ship should submit three copies of the following documents for review. However, a part of documents may be omitted for the ship with CS Ready notation.
   (1) Cyber security organization chart and job description of security personnel
   (2) Cyber security training report
   (3) Data backup and recovery criteria
   (4) Functional requirements / specifications
   (5) Mobile security policy
   (6) Basics of the ship
   (7) List of cyber security related assets and equipments and Status of the personnel in charge of assets
   (8) Cyber security risk assessment report
   (9) Network configuration
   (10) Operating statements
   (11) Policies, procedures and guidances related to cyber security system
   (12) Security policy for outsourcer
   (13) Physical security policy

(14) Incident response and recovery policies
(15) List of Cyber security threats
(16) Risk management plan
(17) Asset vulnerability diagnosis results
(18) Corrective action plan and results
(19) Data importance classification table
(20) Access authority management policy
(21) Software introduction procedure
(22) Patch work / approval statements
(23) Encryption criteria
(24) Change management procedures and application for change

3. In addition to **302. 2**, the ship owner who applies the CS2 notation for the ship should submit three copies of the following documents for review.

(1) Cyber security guidances and manuals
(2) Cyber security training plan
(3) Incident criteria classification table
(4) Disaster recovery plan / scope definition
(5) Penetration test report
(6) Abnormal signs monitoring procedures and results

4. In addition to **302. 3**, the ship owner who applies the CS3 notation for the ship should submit three copies of the following documents for review.

(1) Policy and plan for cyber security audit
(2) Disaster recovery simulation training report
(3) Encryption key management procedure

5. The ship owner should inform the Society of the results of the corrective action against any recommendations found during the document review and, if necessary, resubmit the document containing the results of the corrective action.

303. On-site surveys

1. Based on the company's cyber security related materials collected, the on-site surveys are to survey whether information technology, operation technology and other assets onboard of the ship meet the requirements in the Guidance or not.

2. On-site surveys should be conducted after document review is completed.

3. The following items should be surveyed during the on-site surveys for CS Ready notation.

(1) Risk management report
(2) Special authorization classification table
(3) Log monitoring procedures and results
(4) Physical control measures
(5) Intrusion prevention system policy status (if applicable)
(6) Anti-virus program status
(7) Data and communication encryption status
(8) Remote access control status
(9) Data backup management register
(10) New software test and transfer report (if applicable)
(11) System operation manuals

4. The following items should be surveyed during the on-site surveys for CS1 notation.

(1) Cyber security issue notices
(2) Cyber security training report
(3) Results of special cyber security training
(4) Risk management report
(5) Security pledge for persons board a ship getting on and off a ship
(6) Outsourcer asset return document
(7) Access authority change record
(8) Special authorization classification table
(9) Log monitoring procedures and results
(10) Physical control measures

(11) Intrusion prevention system policy status (if applicable)
(12) Anti-virus program status
(13) Data and communication encryption status
(14) Remote access control status
(15) Log archiving and monitoring procedures and results
(16) Data backup management register
(17) Data storage media discard management register
(18) New software test and transfer report (if applicable)
(19) System operation manuals
(20) Operating statements

5. In addition to **303. 4**, the following items should be surveyed during the on-site surveys for CS2 notation.

(1) Change management record
(2) Remote user management register
(3) Amendment history of cyber security guidances and manuals
(4) Cyber security training and check results for the outsourcers
(5) Approval statements for issuance of outsourcers' account
(6) Vulnerability action plans and results

6. In addition to **303. 5**, the following items should be surveyed during the on-site surveys for CS3 notation.

(1) Special cyber security training report
(2) Disaster recovery plan status
(3) Network access control monitoring history
(4) Encryption key change history

7. The installation status of the facilities related to the cyber security system onboard of the ship should be verified at the on-site surveys to ensure that it meets the requirements of the Rules for Steel Ships.

8. Recommendation corrective action and confirmation

(1) The ship owner should submit the results of corrective actions for the recommendations found through the on-site surveys of the requirements of this Guidance to the Society within 3 months after the on-site surveys, and the adequacy of the results should be reviewed by the Society.
(2) The corrective actions and the security system should be finally verified by on-site re-surveys within 3 months after the notification of the corrective action. However, it can be accepted by the Society if the defect is minor, or if it can be replaced by a document review.

304. Survey report and certification issue

1. In case of the on-site survey items required in the Guidance have been passed, the Society provides the survey report and the classification certification for cyber security system to the ship and the notation is issued. However, the non-KR-classed ships will be issued a certification of cyber security system

2. The survey report for cyber security should include at least following:

(1) List of cyber security system and assets onboard of the ship
(2) List of documents for cyber security system onboard of the ship
(3) Operating statements
(4) Corrective action results
(5) Types, time and checklist of next surveys to maintain the certification for cyber security system

Section 4 Surveys for certification maintenance

401. General

1. Annual surveys

(1) Annual surveys should be carried out to ensure that cyber security system and related facilities are being implemented or maintained in a satisfactory condition in accordance with the requirements of the Guidance.

(2) After the prior survey, the surveyor should check whether there have been any unauthorized changes of cyber security system.

(3) Operation manual for cyber security should be kept onboard and all changes should be reflected. The surveyor should identify the operational manual as a basis for the survey, paying particular attention to the survey records and their contents.

2. Special surveys

(1) Special surveys should be conducted to check whether the cyber security system is being implemented satisfactorily and whether the related security facilities are operating normally during the new certification period of 5 years designated as the periodical survey period. Special survey should be conducted like initial survey.

(2) In case of Company Cyber Security Compliance 2 or CS2 or higher, a simulated penetration test should be performed to identify possible penetration, extortion, deformation, destruction, damage or other communication deficiencies of the major assets included in the cyber security system and the test results should be reported and confirmed.

3. Occasional surveys

(1) Occasional surveys are to be carried out in the following cases other than when the company or ship certified by the Society receives annual or special surveys.
  (A) If there is damage or potential damage to facilities related to Cyber security system
  (B) When facilities related to major cyber security system are repaired or replaced
  (C) When major changes have occurred in the Cyber security system

(2) In the occasional surveys, the necessary matters in accordance with (1) are tested and surveyed.

402. Surveys for certification maintenance of the company

1. Companies with Cyber security system certification should be received annual surveys to maintain certification.

(1) The following items should be surveyed during the on-site surveys for maintaining the certification corresponding to Company Cyber Security Compliance 1.
  (A) System user access log
  (B) Cyber security incident action report
  (C) Change management record
  (D) Log monitoring procedures and results
  (E) System patch management record
  (F) List of changed assets
  (G) Physical security implementation status
  (H) Access control implementation status
  (I) Cyber security risk assessment report and implementation status of risk management plan
  (J) Cyber security training record
  (K) Cyber security related facilities operating status

(2) In addition to **402. 1 (1)**, the following items should be surveyed during the on-site surveys for maintaining the certification corresponding to Company Cyber Security Compliance 2.
  (A) Abnormal signs monitoring results
  (B) Cyber security policies, procedures and guidances making/amendment history
  (C) Amendment history of Cyber security policy and manual
  (D) Penetration test plan and results

(3) In addition to **402. 1 (2)**, the audit results should be surveyed during the on-site surveys for maintaining the certification corresponding to Company Cyber Security Compliance 3.

2. Special surveys should be conducted in every 5 years to renew the certification for Cyber security system in company. The details follows **Ch. 2 202.** and **203.** in the Guidance.

403. Surveys for certification maintenance of the ship

1. Ships with Cyber security system certification should be received annual surveys to maintain certification.

(1) The following items should be surveyed during the on-site surveys for maintaining the CS1 notation.
(A) System user access log
(B) Cyber security incident action report
(C) Change management record
(D) Log monitoring procedures and results
(E) System patch management record
(F) List of changed assets
(G) Physical security implementation status
(H) Access control change (creation, deletion, etc.) record
(I) Access authority review report
(J) Performance monitoring results
(K) Cyber security risk assessment report and implementation status of risk management plan
(L) Cyber security training record
(M) Cyber security related facilities operating status
(N) Access control implementation status

(2) In addition to **403. 1. (1)**, the following items should be surveyed during the on-site surveys for maintaining the CS2 notation.
(A) Abnormal signs monitoring results
(B) Cyber security policies, procedures and guidances making/amendment history
(C) Amendment history of Cyber security policy and manual
(D) Penetration test plan and results
(E) Cyber security incident report or Cyber security incident investigation analysis procedures

(3) In addition to **403. 1. (2)**, the following items should be surveyed during the on-site surveys for maintaining the CS3 notation.
(A) Cyber security audit results
(B) Disaster recovery simulation training results

2. Special surveys should be conducted to renew the certification for Cyber security system onboard of the ship according to the special survey period of the ship. The details follows **Ch. 2 302.** and **303.** in the Guidance. ⚓

CHAPTER 3 REQUIREMENTS FOR CS SYSTEM OF THE COMPANY *(2019)*

Section 1 General

101. General

1. This chapter defines the requirements and organizational procedures for the cyber security system of the company.
2. This chapter describes the essential requirements related to cyber security within the organization's information technology area for compliance with cyber security system and specifies the competencies of the members within the organization.

Section 2 Company Cyber Security Compliance 1

201. Case review

1. The Company should cooperate with government, security specialists, etc. to share the latest information on changes in external environment factors such as cyber security threats and cases.
2. The Company should share with the employees and employees without delay any information on changes in external environmental factors such as cyber security threats and cases.

202. Security policy

1. The company should designate the person responsible for establishing and continually reviewing and managing the security policy in accordance with the security operation procedures.
2. Security organization should designate and assign responsibility and authority to the personnel who have competencies related to security activities.

203. Security training

1. The personnel involved in security activities should conduct security training at least once a year in accordance with the security training plan.
2. Security training for new employees (including contractors and temporary workers) and retirees should be carried out. In particular, training should be provided for domestic and overseas business trips and absentees.
3. The company should provide specialized training on security technologies to the personnel operating information technology.

204. Risk management

1. External environmental factors affecting the environments of internal information technology should be identified and cataloged as threats.
2. Risk management plans including risk assessment methods and procedures should be established to manage cyber security risks.
3. The company should periodically diagnose the vulnerability of its assets related to cyber security.
4. Risk assessment should be carried out at least once a year, linking the threat identification and vulnerability diagnosis results to all assets related to cyber security.
5. Priorities for risk level should be determined according to risk assessment and improvement actions should be taken.

6. The results of the risk assessment should be shared with all stakeholder and be able to support improvement actions.

205. Asset management

1. All assets related to cyber security to be protected, such as systems, facilities, data, etc. should be established and classified.
2. The company should designate the person responsible for each asset, such as the equipment and facilities requiring security, and define the role.
3. The importance of data should be classified and documented in consideration of criteria such as influence of asset leakage and damage.
4. Information assets should be protected in separate storage areas according to their importance.
5. At the end of employment, contract and work of all employees and outside parties, including sailors, the assets owned by the internal and external employees should be returned.

206. Access Control

1. Access control policies should be established, including standards, principles, and procedures for system access rights.
2. Users who can connect to the system should be given minimum privileges and listed and managed.
3. The privileges of the general user and the administrator should be differentiated and the authority standard for each task should be defined.
4. Access rights of users should be managed in a formal procedure according to the access control policy.
5. Privileges granted for special purposes should be classified, identified and controlled separately.
6. A security function should be established to clarify the responsibility for each user account(ID) and to maintain the confidentiality.
7. Access record of users to the system should be retained for at least six months and reviewed periodically. *(2019)*

207. Physical Security

1. The company should establish policies that define the physical security standards for system equipment, facilities, and so on.
2. The company should provide physical controls to access protected areas containing assets related to cyber security only to authorized persons.
3. The company should monitor and track illegal intrusions when working on key assets related to cyber security in the protected area.
4. If a device such as CCTV is installed to monitor the protected area, it is necessary to classify the users through the authentication means and block the connection of unauthorized persons.
5. The main system should manage the authority of the person who has physical and logical access separately and control the access of the unauthorized person.
6. The company should ensure that at least the same physical security as the existing system is applied when installing the new system.
7. Equipment essential for major system operation such as communication lines should be protected from physical attack and periodic inspection should be carried out.
8. The company should control its internal assets and network connections through portable storage media such as USB by using the methods like physical port locking and unused port inactivation
9. The company should provide protective measures to prevent information leakage by theft or loss of portable equipment such as notebook computers.

10. Standards should be established for reusing all hardware assets, and countermeasures should be taken to ensure safe destruction if not reused.

11. Clean desk operation and terminal screen protection policy of the area where documents and portable storage media are stored should be prepared and applied.

208. Incident Response and Recovery

1. The Company should establish an incident response and recovery policy, including the types of incidents and their corresponding methods and procedures.

2. The company should define the roles and responsibilities of the organization or persons responsible for immediate response and recovery activities to system operation and security issues. In addition, an emergency communication system should be established to enable rapid communication with internal and external stakeholder, and the emergency communication network should be updated and managed.

3. The operating system in the ship should have an emergency operation function so that it can be operated even in case of an emergency.

4. In case of an incident, relevant functions should be provided and the manual should be documented so that the system can be operated safely and continuously.

5. System design should reflect security requirements against operational failures.

209. Outside Parties' Security

1. The company should establish a security policy for information technology equipment and data of outside parties in order to prepare for security incidents by the outside parties.

2. The company should specify the security requirements, management and supervision during the project period when contracting with outside parties.

3. The company should follow the approval procedure by the person in charge if the outside party should be granted the right to access the system.

4. The outside parties should use the system in compliance with company security requirements and perform the security function check before connecting the equipment owned by the outside parties to the system.

210. Data Security

1. Important data should be backed up in a separate space and stored securely.

2. Data should be limited in user access according to its importance, and physical and logical access control should be performed.

3. Private use of the Internet should be restricted to prevent unauthorized attack and data access through the use of personal e-mail, illegal site access.

4. When discarding the equipment in which the data is stored, the stored data should be deleted in a non-reproducible manner.

211. Log Management

1. Categorizing the system-specific logs by type, the necessary logs should be stored securely for a certain period of time.

2. When storing logs, it should be confirmed whether or not the log data integrity is maintained.

3. The system in which the logs are stored should be physically and logically controlled to prevent unauthorized access.

4. Company-run software and hardware should be synchronized at the same time.

5. Monitoring should be performed to prevent the excess of system performance and capacity, and in the event of a failure, prompt action should be taken.

212. Software Development and Testing

1. Procedures should be established to conduct security test before the introduction of software and applications.
2. Software test should be carried out to identify defects. If the software fails the test, it should be forbidden to apply to the actual operating system.
3. The environment for test execution should be established and tested according to the procedures.
4. The software that has passed the test should be applied to the operating system after obtaining approval from the responsible person.
5. It is only necessary to use the storage specified by the company when developing the software, and to obtain prior approval when using external storage such as cloud service.

213. System Management

1. It should be ensured whether unauthorized interfaces, ports, or services exist in the operating system.
2. When transferring file information in the operating system, it is necessary to confirm whether information provision standard is defined and applied.
3. When introducing information assets, the default value should be newly set or changed according to the security policy or change management standard of the company, and the use of the assets should be prohibited before the security setting is changed.
4. Before changing the system, the relevant data should be backed up in case of system failure.
5. Installation of operating system software should be restricted by the security department, and unauthorized software updates or update methods should not be applied
6. All software accessing information assets should be configured not to run automatically.
7. When performing change management, pre-test should be conducted and change management records should be kept and managed.

214. Patch Management

1. The company should select the patch priority in the system patch, execute the patch through the approved procedure, and list the known vulnerabilities and obstacles before the patch.
2. If the automatic patching tool is not available or if the system is incompatible, the system should be managed separately.
3. Patches should be performed without a missing system, and patch versions for each system should be recorded and managed.

215. Mobile Security

1. The company should establish security policies to control the use of corporate mobile devices and employee owned mobile devices.
2. The company should define the mobile devices and functions available in the company and identify the devices in use.
3. Network and system connections to mobile devices should be restricted and the use of non-call features of mobile devices such as photo shooting should be controlled.
4. The company should prevent mobile devices used by employees from accessing unauthorized access points(Rogue Access Points) that are exploited for malicious code infections or hacking.

216. Encryption

1. An environment in which data can be communicated in an encrypted manner should be established.
2. Encryption standards for data protection should be established and planned.
3. Data classified as important should be encrypted and stored.

217. Malicious code response

Controls to protect networks, information systems, operating systems, and terminals from malicious code should be provided.

218. Network Management

1. Vulnerabilities of network equipment should be periodically checked so that it does not affect other networks due to communication channel flaws.
2. To protect the internal network, an intrusion prevention system should be installed and operated to block external unauthorized access, and should be managed continuously.
3. The wireless network environment should be configured separately from the wireless network that can be accessed by outside parties.
4. The information technology system should be restricted from being accessed through the wireless network.
5. The internal and external communication interfaces of the information system should be controlled to limit the connection.
6. When connecting to a system via an external network, a secure connection method using an enhanced authentication technique should be applied.
7. It should have a graphical network flow that can identify the network path.
8. When building network related equipment, it is necessary to remove the default value and activate the security related function, which may be requested by the supplier if necessary.
9. When establishing a communication line, the communication path, connection priority, and protocol should be defined in advance to minimize the defect, and the service level agreement, etc. should be included in the supplier contract.

219. Cyber security internal audit

1. The company should conduct a half-yearly security check.
2. Policy violations should be reported in accordance with cyber security internal audit plan.

Section 3 Company Cyber Security Compliance 2

301. Establishment of threat information collection system

Company should review the change in external environment factors such as cyber security threats and cases and reflect them in company policy.

302. Continuous management of security policy and manual

1. The company's guidelines and manuals should be periodically reviewed to meet company's policy and requirements of flag stats or IMO, etc. and the amendments should be recorded and managed.
2. The company should document the policies and guidelines taking into account the procedures and standards to be referenced.

303. Enhanced security organization

1. The company should designate the Chief Security Officer or higher to oversee the cyber security of the company.
2. A security organization should be organized to carry out security activities on the company taking into consideration the size of assets and characteristics of the company.

304. Special security training

1. The enhanced security training plans for the company should be established in consideration of internal and external environment factors and change of the assets, etc.
2. The company should provide training for test procedures and standards to the personnel performing software application tests.

305. Abnormal signs detection

1. The company should periodically review whether changes in authority have been properly made in accordance with changes in the user's job.
2. An intrusion detection function should be provided to detect unauthorized access or anomalies to the information system.
3. In case of a system with remote access, the safe functional requirements should be reflected and the function's safety should be checked periodically.
4. Network access control technology should be applied to all communication methods including existing network, remote and wireless network.
5. If the equipment with data is discarded, the stored data should be deleted in a non-reproducible manner.

306. Physical control improvement in ships

1. In case of CCTVs are installed in security areas in the ship, the performance of CCTVs should be periodically examined.
2. In case of CCTVs are installed in security areas in the ship, their communication network should be separated from that of main system.

307. Response capability enhancement against cybersecurity incident

1. The company should classify the types of incidents according to the importance of tasks or duties and types of threats, and establish and maintain incident response procedures for each type.
2. The company should identify and take action against known major system vulnerabilities to prevent incidents caused by external attacks.

3. The company should monitor the signs related to the incident and take preliminary action considering the internal influence.
4. The information generated when investigating and responding to the incident should be recorded and reported to management including its impact and action plan.
5. The company should have personnel, equipment or technology for incident response and analysis.
6. The company should designate the personnel to carry out the analysis of the cyber security incident investigation and be familiar with the relevant contents.
7. The company should define the severity of the cyber security incident in advance and take countermeasures according to the severity.
8. The company should define the scope of the investigation analysis by analyzing the related assets according to the degree of damage in the analysis of the investigation of the cyber security incident.
9. All log data within the scope of the cyber security incident analysis should be investigated.
10. The company should periodically conduct simulated training or penetration test to check security and establish relevant plans.
11. The scopes of simulated training or penetration test should be defined not to affect the operational continuity of the operating system.
12. Penetration tests should be carried out according to a preliminary plan and all possible resources should be used for testing.

309. Change management

1. The company should record the change management history by system and manage the unusual so that the problems are not repeated.
2. Pre-test should be performed considering system impact, business impact, and expected failure prior to system patching.
3. System patching only allows reliable network connections and should be monitored when work is being done remotely.
4. The company should define the enhanced security requirements for developing secured software.
5. The company should limit and monitor data accessed by software developers, including external developers.

310. Business continuity enhancement

1. The system operation manual should be periodically reviewed for internal policies and linkages and linked to the risk management process.
2. The company should establish a disaster recovery plan for a contingency in order to maintain business continuity.

311. Mobile security management

For controlling mobile device usage, technical security should be applied through automated control tools and anti-virus program for mobile.

312. Security investment

1. The budget should be determined taking into account the system life cycle and security technology requirements.
2. For budgets that require technology acquisitions, the technology acquisition budgets that meet system-specific requirements and industry standards should be budgeted.
3. The budget should be established taking into consideration the risk assessment results and the risk management plan.

Section 4 Company Cyber Security Compliance 3

401. Unification of security system

1. The company should monitor changes in related laws, standards, technical guides, etc. and incorporate them into its policies.
2. The company should establish a security consultative group to share and discuss security issues between security organizations, information technology and operational technical personnels.

402. Security engineering

1. Training to periodically test security-related issues learned through training should be conducted.
2. During development, security of the code should be reviewed and security requirements of data stored and transmitted through the developed application should be checked.

403. Business continuity assurance

1. The company should periodically check and, if necessary, update the system for supporting incident response.
2. The company should continuously review and improve the contingency plans taking into account changes in internal and external environmental factors and assets, etc.
3. Security requirements of the system for recovery should be applied, and regularly inspected and took actions.
4. Recovery capability should be tested and virtual simulation should be periodically conducted to verify recovery plan.
5. Before penetration test, vulnerability should be eliminated through preliminary evaluation.
6. The results of penetration test should be reviewed and the effectiveness of the company security should be measured and reported.
7. The company should provide relevant policies, research facilities, and technical tools for the analysis of cyber security incidents.

404. Real-time monitoring capability enhancement

1. Network access control techniques should be used to monitor abnormal communications and implement restriction measures.
2. The company should monitor the various traffic to the network in real time and recognize and response the abnormal behavior in advance.
3. A real-time monitoring and response system should be established and operated to prevent infection and spread by malicious code that exploits new vulnerabilities.

405. Cyber security audit

1. The company should establish a policy to carry out cyber security audits by the company and cyber security specialized organization.
2. The company should periodically establish and conduct cyber security audit plans by the company and cyber security specialized organization.

406. Encryption key management

Encryption key should be managed by a procedure and stored in separate place in accordance with access control policy. ⚓

CHAPTER 4 REQUIREMENTS FOR CS SYSTEM OF THE SHIP *(2019)*

Section 1 General

101. General

1. This chapter defines the requirements and organization procedures of information technology and operation technology for cyber security system of the ship.
2. This chapter describes the essential requirements related to cyber security within the organization's information technology and operation technology areas for compliance with cyber security system and specifies the competencies of the members within the organization.

Section 2 CS Ready

201. Risk management

1. External environmental factors affecting the environments of information technology and operation technology in ships should be identified and cataloged as threats.
2. Risk management plans including risk assessment methods and procedures should be established to manage cyber security risks.
3. The ship should diagnose the vulnerability of its assets related to cyber security.
4. Risk assessment should be carried out linking the threat identification and vulnerability diagnosis results to all assets related to cyber security.
5. Priorities for risk level should be determined according to risk assessment and improvement actions should be taken.

202. Asset management

All assets to be protected, such as systems, facilities, data, etc. should be established and classified.

203. Access Control

1. Users who can connect to the system should be given minimum privileges and listed and managed.
   (1) The system should provide the capabilities to authenticate users.
   (2) The privileges of the general user and the administrator should be differentiated and the authority standard for each task should be defined.
   (3) The system should provide the capability to support the management of all privileges by authorized users, including adding, modifying and removing privileges.
2. A security function should be established to clarify the responsibility for each user account(ID) and to maintain the confidentiality.
   (1) The system should provide the capability to enforce configurable password strength based on minimum length and variety of character types.
   (2) The system should provide the capability to obscure feedback of authentication information during the authentication process.
   (3) The system should provide the capability to enforce a limit of a configurable number of consecutive invalid access attempts.
   (4) The system should provide the capability to display a system use notification message before authenticating.
   (5) The system may provide the capability to employ multi-factor authentication depending on importance of the system.
3. Access record of users to the system should be retained for at least six months and reviewed periodically.

204. Physical Security

1. If a device such as CCTV is installed to monitor the protected area, it is necessary to classify the users through the authentication means and block the connection of unauthorized persons.
2. The main system should manage the authority of the person who has physical and logical access separately and control the access of the unauthorized person.
3. Equipment essential for major system operation such as communication lines should be protected from physical attack and periodic inspection should be carried out.
4. The ship should control its internal assets and network connections through portable storage media such as USB by using the methods like physical port locking and unused port inactivation.
5. External devices accessing the system (portable storage media, smart phones, etc.) should be prevented and controlled from automatic execution.

205. Incident response and recovery

1. The operating system in the ship should have an emergency operation function so that it can be operated even in case of an emergency.
   (1) The emergency power supply system, etc. should always be operable for system operation.
   (2) The system should provide the capabilities to recover to a secure state after disruption or failure.
2. In case of an incident, relevant functions should be provided and the incident response and recovery manual for should be documented so that the system can be operated safely and continuously.

206. Data Security

1. Data should be limited in user access according to its importance, and physical and logical access control should be performed.
2. An environment in which data can be communicated in an encrypted manner should be established.
3. Encryption standards for data protection should be established and planned.
4. Data classified as important should be encrypted and stored.

207. Log Management

1. Categorizing the system-specific logs by type, the necessary logs should be stored securely for a certain period of time.
2. When storing logs, it should be confirmed whether or not the log data integrity is maintained.
3. The system in which the logs are stored should be physically and logically controlled to prevent unauthorized access.
4. Software and hardware operated in the ship should be synchronized at the same time.
5. Monitoring should be performed to prevent the excess of system performance and capacity, and in the event of a failure, prompt action should be taken.

208. System Management

1. It should be ensured whether unauthorized interfaces, ports, or services exist in the system.
2. When transferring file information in the operating system, it is necessary to confirm whether information provision standard is defined and applied.
3. When introducing cyber security assets, the default value should be newly set or changed according to the security policy or change management standard of the ship, and the use of the assets should be prohibited before the security setting is changed.
4. Before changing the system, the relevant data should be backed up in case of system failure.

5. All software accessing cyber security assets should be configured not to run automatically.
6. Change management records for hardware and software should be kept and managed.
7. The system should provide the capability to create audit log.
   (1) The system should allocate sufficient audit record storage.
   (2) The system should protect audit information from unauthorized access, modification and deletion.
   (3) The system should provide the capability for authorized users to access audit logs on a read-only basis.

209. Patch Management

1. The ship should select the patch priority in the system patch, execute the patch through the approved procedure, and list the known vulnerabilities and obstacles before the patch.
2. If the automatic patching tool is not available or if the system is incompatible, the system should be managed separately.
3. Patches should be performed without a missing system, and patch versions for each system should be recorded and managed.

210. Malicious Code Response

Controls to protect networks, information systems, operating systems, and terminals from malicious code should be provided.

211. Network Management

1. Vulnerabilities of network equipment should be periodically checked so that it does not affect other networks due to communication channel flaws.
2. To protect the internal network, an intrusion prevention system should be installed and operated to block external unauthorized access, and should be managed continuously.
3. The wireless network environment should be configured separately from the wireless network that can be accessed by outside parties.
4. The operating system should be restricted from being accessed through the wireless network.
5. The internal and external communication interfaces of the systems should be controlled to limit the connection. Connection limitation devices include proxies, gateways, routers, firewall, unidirectional gateways and VPN.
6. The networks of IT systems and OT systems should be operated separately.
7. When connecting to a system via an external network, a secure connection method using an enhanced authentication technique should be applied.
8. It should have a graphical network flow that can identify the network path.
9. When building network related equipment, it is necessary to remove the default value and activate the security related function, which may be requested by the supplier if necessary.
10. When establishing a communication line, the communication path, connection priority, and protocol should be defined in advance to minimize the defect, and the service level agreement, etc. should be included in the supplier contract.

212. Software Quality Management

1. It is the responsibility of the ship builders to manage software quality and the achievement of this responsibility should be supported by system integrators updating the software registry. The software registry should contain:
   (1) List and versions of software installed in cyber security systems

(2) Results of security audit

2. Software quality system should include the following materials as a minimum:
   (1) Having a specific procedure for verification of software code at the level of systems, sub-systems and programmable devices and modules
   (2) Having schedules including required submittal of documentation, a test event, a technical design review meeting, etc.
   (3) Having a specific procedure for software modification and installation on board the ship defining interactions with stakeholder

213. Cyber security Test

1. Cyber security test such as FAT, SAT, etc. should confirm whether security functions of the system are properly implemented. These security functions should include all items necessary to the requirement specified in this Guidance.
2. It should be verified through vulnerability diagnosis and/or penetration tests whether security functions reflecting the cyber risk assessment are properly implemented

Section 3 CS1 (CS1(C))

301. Case review

The ship should share with the crews without delay any information on changes in external environmental factors such as cyber security threats and cases.

302. Security policy

1. The ship should have, review and manage a cyber security policy that specifies the operational methods, procedures and responsibilities for security operations.
2. The ship should designate and assign responsibility and authority to the personnel who have competencies related to security activities.

303. Security training

1. The personnel involved in security activities should conduct security training at least once a year in accordance with the security training plan.
2. Security training for the person getting on and off the ship should be carried out.
3. The ship should provide specialized training on security technologies to the personnel operating information technology and operation technology.

304. Risk management

1. External environmental factors affecting the environments of internal information technology and operational technology should be identified and cataloged as threats.
2. Risk management plans including risk assessment methods and procedures should be established to manage cyber security risks.
3. The ship should periodically diagnose the vulnerability of its assets related to cyber security.
4. Risk assessment should be periodically carried out by linking the threat identification and vulnerability diagnosis results to all assets related to cyber security.
5. Priorities for risk level should be determined according to risk assessment and improvement actions should be taken.
6. The results of the risk assessment should be shared with all stakeholder and be able to support improvement actions.

305. Asset management

1. All assets to be protected, such as systems, facilities, data, etc. should be established and classified.
2. The ship should designate the person responsible for each asset, such as the equipment and facilities requiring security, and define the role.
3. The importance of data should be classified and documented in consideration of criteria such as influence of asset leakage and damage.
4. Information assets should be protected in separate storage areas according to their importance.

306. Access Control

1. Access control policies should be established, including standards, principles, and procedures for operating system access rights.
2. Users who can connect to the system should be given minimum privileges and listed and managed.
3. The privileges of the general user and the administrator should be differentiated and the authority standard for each task should be defined.
4. Access rights of users should be managed in a formal procedure according to the access control policy.
5. Privileges granted for special purposes should be classified, identified and controlled separately.
6. A security function should be established to clarify the responsibility for each user account(ID) and to maintain the confidentiality.
7. Access record of users to the system should be retained for at least six months and reviewed periodically. *(2019)*

307. Physical Security

1. The ship should establish policies that define the physical security standards for system equipment, facilities, and so on.
2. The ship should provide physical controls to access protected areas containing assets only to authorized persons.
3. The ship should monitor and track illegal intrusions when working on key assets in the protected area.
4. If a device such as CCTV is installed to monitor the protected area, it is necessary to classify the users through the authentication means and block the connection of unauthorized persons.
5. The main system should manage the authority of the person who has physical and logical access separately and control the access of the unauthorized person.
6. The ship should ensure that at least the same physical security as the existing system is applied when installing the new system.
7. Equipment essential for major system operation such as communication lines should be protected from physical attack and periodic inspection should be carried out.
8. The ship should control its internal assets and network connections through portable storage media such as USB.
9. The ship should provide protective measures to prevent information leakage by theft or loss of portable equipment such as notebook computers.
10. Standards should be established for reusing all hardware assets, and countermeasures should be taken to ensure safe destruction if not reused.
11. Clean desk operation and terminal screen protection policy of the area where documents and portable storage media are stored should be prepared and applied.

308. Incident Response and Recovery

1. The ship should establish an incident response and recovery policy, including the types of incidents and their corresponding methods and procedures.
2. The ship should define the roles and responsibilities of the organization or persons responsible for immediate response and recovery activities to system operation and security issues. In addition, an emergency communication system should be established to enable rapid communication with internal and external stakeholder, and the emergency communication network should be updated and managed.
3. The operating system in the ship should have an emergency operation function so that it can be operated even in case of an emergency.
4. In case of an incident, relevant functions should be provided and the manual should be documented so that the system can be operated safely and continuously.
5. System design should reflect security requirements against operational failures.

309. Outside Parties' Security

1. The ship should establish a security policy for cyber security equipment and data of outside parties in order to prepare for security incidents by the outside parties.
2. The ship should follow the approval procedure by the person in charge if the outside party should be granted the right to access the system.
3. The outside parties should use the system in compliance with ship security requirements and perform the security function check before connecting the equipment owned by the outside parties to the system.

310. Data Security

1. Important data should be backed up in a separate space and stored securely.
2. Data should be limited in user access according to its importance, and physical and logical access control should be performed.
3. Private use of the Internet should be restricted to prevent unauthorized attack and data access through the use of personal e-mail, illegal site access.
4. When discarding the equipment in which the data is stored, the stored data should be deleted in a non-reproducible manner.

311. Log Management

1. Categorizing the system-specific logs by type, the necessary logs should be stored securely for a certain period of time.
2. When storing logs, it should be confirmed whether or not the log data integrity is maintained.
3. The system in which the logs are stored should be physically and logically controlled to prevent unauthorized access.
4. Ship-run software and hardware should be synchronized at the same time.
5. Monitoring should be performed to prevent the excess of system performance and capacity, and in the event of a failure, prompt action should be taken.

312. System Management

1. It should be ensured whether unauthorized interfaces, ports, or services exist in the systems.
2. When transferring file information in the operating system, it is necessary to confirm whether information provision standard is defined and applied.

3. When introducing assets related to cyber seucirty, the default value should be newly set or changed according to the security policy or change management standard of the ship, and the use of the assets should be prohibited before the security setting is changed.
4. Before changing the system, the relevant data should be backed up in case of system failure.
5. Installation of operating system software should be restricted by the security officer, and unauthorized software updates or update methods should not be applied
6. All software accessing assets related to cyber security should be configured not to run automatically.
7. Change management records of the system should be kept and managed.

313. Patch Management

1. The ship should select the patch priority in the system patch, execute the patch through the approved procedure, and list the known vulnerabilities and obstacles before the patch.
2. If the automatic patching tool is not available or if the system is incompatible, the system should be managed separately.
3. Patches should be performed without a missing system, and patch versions for each system should be recorded and managed.

314. Mobile Security

1. The ship should establish security policies to control the use of corporate mobile devices and crew owned mobile devices.
2. The ship should define the mobile devices and functions available in the ship and identify the devices in use.
3. Mobile devices should be restricted to connect network and systems, and the use of non-call features of mobile devices such as photo shooting should be controlled.
4. The ship should prevent mobile devices used by crews from accessing unauthorized access points (Rogue Access Points) that are exploited for malicious code infections or hacking.

315. Encryption

1. An environment in which data can be communicated in an encrypted manner should be established.
2. Encryption standards for data protection should be established and planned.
3. Data classified as important should be encrypted and stored.

316. Malicious code response

Controls to protect networks, information systems, operating systems, and terminals from malicious code should be provided.

317. Network Management

1. Vulnerabilities of network equipment should be periodically checked so that it does not affect other networks due to communication channel flaws.
2. To protect the internal network, an intrusion prevention system should be installed and operated to block external unauthorized access, and should be managed continuously.
3. The wireless network environment should be configured separately from the wireless network that can be accessed by outside parties.
4. The operating system should be restricted from being accessed through the wireless network.

5. The internal and external communication interfaces of the information system or the operating system should be controlled to limit the connection.
6. The networks of information systems and operating systems should be operated separately.
7. When connecting to a system via an external network, a secure connection method using an enhanced authentication technique should be applied.
8. It should have a graphical network flow that can identify the network path.
9. When building network related equipment, it is necessary to remove the default value and activate the security related function, which may be requested by the supplier if necessary.
10. When establishing a communication line, the communication path, connection priority, and protocol should be defined in advance to minimize the defect, and the service level agreement, etc. should be included in the supplier contract.

318. Cyber security internal audit

1. Policy violations should be reported in accordance with cyber security internal audit plan.
2. The ship should periodically inspect and conduct security surveys while outsourcers perform business.

Section 4 CS2 (CS2(C))

401. Establishment of threat information collection system

The ship should review the change in external environment factors such as cyber security threats and cases and reflect them in the ship's policy.

402. Continuous management of security policy and manual

1. The cyber security guidelines and manuals should be periodically reviewed to meet ship's policy and requirements of flag stats or IMO, etc. and the amendments should be recorded and managed.
2. The ship should document the policies and guidelines taking into account the procedures and standards to be referenced.

403. Special security training

The enhanced security training plans should be established in consideration of internal and external environment factors and change of the assets, etc.

404. Abnormal signs detection

1. The ship should periodically review whether changes in authority have been properly made in accordance with changes in the user's job.
2. An intrusion detection function should be provided to detect unauthorized access or anomalies to the system.
3. In case of a system with remote access, the safe functional requirements should be reflected and the function's safety should be checked periodically.
4. Network access control technology should be applied to all communication methods including existing network, remote and wireless network.
5. If the equipment with data is discarded, the stored data should be deleted in a non-reproducible manner.

405. Physical control improvement in ships

1. In case of CCTVs are installed in security areas in the ship, the performance of CCTVs should be periodically examined.
2. In case of CCTVs are installed in security areas in the ship, their communication network should be separated from that of main system.

406. Response capability enhancement against cyber security incident

1. The ship should classify the types of incidents according to the importance of tasks or duties and types of threats, and establish and maintain incident response procedures for each type.
2. The ship should identify and take action against known major system vulnerabilities to prevent incidents caused by external attacks.
3. The ship should monitor the signs related to the incident and take preliminary action considering the internal influence.
4. The information generated when investigating and responding to the incident should be recorded and reported to management including its impact and action plan.
5. The ship should have personnel, equipment or technology for incident response and analysis.
6. The ship should designate the personnel to carry out the analysis of the cyber security incident investigation and be familiar with the relevant contents.
7. The ship should define the severity of the cyber security incident in advance and take countermeasures according to the severity.
8. The ship should define the scope of the investigation analysis by analyzing the related assets according to the degree of damage in the analysis of the investigation of the cyber security incident.
9. All log data within the scope of the cyber security incident analysis should be investigated.
10. The ship should periodically conduct simulated training or penetration test to check security and establish relevant plans.
11. The scopes of simulated training or penetration test should be defined not to affect the operational continuity of the operating system.
12. Penetration tests should be carried out according to a preliminary plan and all possible resources should be used for testing.

407. Mobile security management

For controlling mobile device usage, technical security should be applied through automated control tools and anti-virus program for mobile.

408. Change management

1. The ship should record the change management history of system and manage the unusual so that the problems are not repeated.
2. Pre-test should be performed considering system impact, business impact, and expected failure prior to system patching.

409. Business continuity enhancement

1. The system operation manual should be periodically reviewed for internal policies and linkages and linked to the risk management process.
2. The ship should establish a disaster recovery plan for a contingency in order to maintain business continuity.

Section 5 CS3 (CS3(C))

501. Unification of security system

The ship should monitor changes in related laws, standards, technical guides, etc. and incorporate them into its policies.

502. Security engineering

Training to periodically test security-related issues learned through training should be conducted.

503. Business continuity assurance

1. The ship should periodically check and, if necessary, update the system for supporting incident response.
2. The ship should continuously review and improve the contingency plans taking into account changes in internal and external environmental factors and assets, etc.
3. Security requirements of the system for recovery should be applied, and regularly inspected and took actions.
4. Recovery capability should be tested and virtual simulation should be periodically conducted to verify recovery plan.
5. Before penetration test, vulnerability should be eliminated through preliminary evaluation.
6. The results of penetration test should be reviewed and the effectiveness of the ship security should be measured and reported.
7. The ship should provide relevant policies, research facilities, and technical tools for the analysis of cyber security incidents.

504. Real-time monitoring capability enhancement

1. Network access control techniques should be used to monitor abnormal communications and implement restriction measures.
2. The ship should monitor the various traffic to the network in real time and recognize and response the abnormal behavior in advance.
3. A real-time monitoring and response system should be established and operated to prevent infection and spread by malicious code that exploits new vulnerabilities.

505. Cyber security audit

1. The ship should establish a policy to carry out cyber security audits by the company and cyber security specialized organization.
2. The ship should periodically establish and conduct cyber security audit plans by the company and cyber security specialized organization.

506. Encryption key management

Encryption key should be managed by a procedure and stored in separate place in accordance with access control policy. ⚓

GUIDANCE FOR MARITIME CYBER SECURITY SYSTEM

Published by
KR
36, Myeongji ocean city 9-ro, Gangseo-gu,
BUSAN, KOREA
TEL : +82 70 8799 7114
FAX : +82 70 8799 8999
Website : http://www.krs.co.kr