


보안 절차서 **SECURITY PROCEDURE**

문서번호 : PR - 19

Doc. No. : PR - 19

<input checked="" type="checkbox"/>	관 리 본 CONTROLLED	<input type="checkbox"/>	비 관 리 본 UNCONTROLLED
-------------------------------------	---------------------	--------------------------	-------------------------

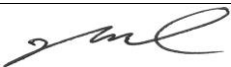

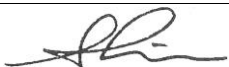
코린스타(주)
KORIN STAR CO., LTD.


	보안 절차서 SECURITY PROCEDURE	DOC NO. : PR - 19 REV. NO. : 0
F-1	목차 INDEX	PAGE 1 / 1

번호 No.	제 목 TITLE
F-1	목차 INDEX
F-2	개정이력 REVISION HISTORY
제 1 장 CH. 1	일반사항 GENERAL
제 2 장 CH. 2	방침 및 목표 POLICY AND OBJECTIVE
제 3 장 CH. 3	조직 및 책임과 권한 ORGANIZATION, RESPONSIBILITY AND AUTHORITY
제 4 장 CH. 4	보안 위협, 사고, 침해 대응 RESPOND TO SECURITY THREAT, INCIDENT, INFRINGEMENT
제 5 장 CH. 5	보안 교육 및 훈련 SECURITY TRAINING AND DRILL
제 6 장 CH. 6	보안 조치 SECURITY MEASURES
제 7 장 CH. 7	보안 기록 및 보안정보 관리 RECORD MAINTENANCE AND MANAGEMENT OF SECURITY INFORMATION
제 8 장 CH. 8	보안 평가 및 보안 심사 SECURITY ASSESSMENT AND SECURITY AUDIT
제 9 장 CH. 9	보안 위반에 대한 징계 DISCIPLINARY ACTION AGAINST SECURITY VIOLATION
제 10 장 CH. 10	비상 대응 지침 EMERGENCY RESPONSE GUIDELINE
APP - 1	사이버 보안 지침 CYBER SECURITY INSTRUCTION
APP - 2	위험 요소 식별 IDENTIFY THREATS
APP - 3	사이버 보안 관련 시스템 SYSTEM RELATED WITH CYBER SECURITY
APP - 4	위험 노출 평가 ASSESS RISK EXPOSURE
APP - 5	사이버 보안 조치 CYBER SECURITY MEASURES
APP - 6	사이버 보안 대응 사건 대응 RESPONSE TO CYBER SECURITY INCIDENT

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>F-2</p>	<p style="text-align: center;">개정이력 REVISION HISTORY</p>	<p>PAGE 1 / 1</p>

No.	장 번호 Chapter	개정번호 Rev. No.	시행일자 Enforced Date	개 정 내 용 REVISION CONTENTS
0	All chapters	0	2019.01.01	- 제정 Establishment

	작 성 WRITTEN BY	검 토 REVIEWED BY	승 인 APPROVED BY
직책 RANK	SQT LAEDER	DP	PRESIDENT
서명 SIGN			
일자 DATE	2018.12.20	2018.12.20	2018.12.20

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 1</p>	<p style="text-align: center;">일반사항 GENERAL</p>	<p>PAGE 1 / 4</p>

1.1 도입 Introduce

- 1) 최근 선박 운항 관리를 비롯한 전반적인 해사 산업에 최신 정보 통신 기술(ICT, Information & Communication Technology)이 광범위하게 적용됨에 따라 해운 회사 및 선박에 대한 사이버 공격 위험 또한 증가하고 있다. 선박과의 통신 및 선박 관리 전산 프로그램이 해킹을 당하거나 랜섬웨어 감염등으로 마비 될 경우 발생 가능한 손실에 대한 전사적 대응이 필요하다.

As ICT(Information & Communication Technology) continues to develop, the risk of cyber attacks on shipping companies and vessels is also increasing. There is need for countermeasures against possible losses if communications with vessels and ship management computer programs are hacked or paralyzed by Ransomware infection.

- 2) 해운 관련 업계의 대응으로 발틱국제해운협회(BIMCO)가 선박 사이버 보안 적용 지침(The Guidelines on Cyber Security Onboard Ships)을 배포하였고, 2017년 국제 해사 기구(IMO)의 MSC 98차 회의에서는 ISM Code 에 따른 위험성평가 절차에 향후 사이버 보안 위협에 대한 관리 항목을 포함시켜 시스템을 이행할 것을 결의 하였다.

As response to the maritime industry BIMCO has issued the guidelines on Cyber Security Onboard Ships and the MSC 98th Session of IMO has decided to implement the system by including management items for future cyber security threats in the risk assessment procedure.

- 3) 특히 전세계 주요 화주 협회에서는 2018년부터 OIL MAJOR (탱커선화주검사) 및 RIGHTSHIP (벌크선화주검사) Vetting 검사시 회사 및 선박의 ‘사이버 보안 대응 절차’ 보유 여부와 관리 수준을 점검 항목에 포함시킬 것으로 발표하였다.


In particular, major shippers'associations around the world will include in the checklist the existence and management level of Cyber Security Response Procedure for companies and vessels during Oil Major and

- 4) 이에 따라 당사는 본 ‘회사보안절차서’를 통해 사이버 보안을 포함하여 식별된 보안 위험을 완화하고 대응 체계 구축을 위한 지침을 작성하였다.

Accordingly, the company has developed guidelines for mitigating identified security risks including cyber security and established a response system through the ‘Company Security Procedure’.

1.2 대외비 요건 Confidentiality requirement

- 1) 회사 보안 절차서 내용의 공유 및 회람은 회사 및 선박 내 모든 임직원에게 한하며, 외부에 공개하지 않는다

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 1</p>	<p style="text-align: center;">일반사항 GENERAL</p>	<p>PAGE 2 / 4</p>

Sharing and circulation of the contents of company security procedures shall be limited to all employees in the company.

- 2) 단, 보안 심사 수검 또는 보안 이행 확인이 필요한 있는 경우, 회사 보안 책임자 혹은 선박 보안 책임자의 허락을 득하고 열람할 수 있다.

However, if there is a need for a security audit or confirmation of security implementation, the CSO and SSO may permit the right of reading the company security procedure.

- 3) 기록의 열람 및 외부로의 유출은 회사보안책임자의 허가를 득해야 한다.

The perusal and disclosure of records shall be done under the permission of CSO.

- 4) 본 회사보안절차서 및 보안관련 정보는 선박보안계획서와 함께 보관한다.

This company security procedure and security information shall be kept together with SSP.

1.3 적용 Application

- 1) 본 회사 보안 절차서는 테러 및 불법행위를 방지하기 위하여 관련 기관과 상호협력 및 조정을 하여 회사 및 선박에서 보안활동을 수행하는데 적용된다.

In order to prevent terrorism and illegal acts, this CSP applies to security activities undertaken on the ship and the company through mutual cooperation with other parties concerned.

- 2) 회사 내의 모든 조직과, 선박 및 직원을 모두 포함한 회사 활동의 모든 부분이 회사보안 절차의 적용 대상이 된다.

All of the entities in the company including activities of all organizations, shore staff and crew are subject to the Company Security Procedure.

1.4 용어의 정의 Term definition

- 1) 보안 Security


회사 비밀을 효율적으로 보호 관리하는 제반 행위를 말한다

All activities that efficiently protect and manage company secrets

- 2) 사이버 보안 Cyber security

사이버 보안은 네트워크, 장치, 프로그램 및 데이터를 공격, 손상 또는 무단 접근(Access)으로부터 보호하기 위해 고안된 기술, 프로세스 및 관행의 집합체를 의미한다. 사이버 보안은 정보 기술 보안이라고도 한다.

Cyber security refers to the body of technologies, processes, and practices designed to protect networks, devices, programs, and data from attack, damage, or unauthorized access. Cyber security may also be referred to as information technology security

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 1</p>	<p style="text-align: center;">일반사항 GENERAL</p>	<p>PAGE 3 / 4</p>

3) 악성 코드 Malignant code

정당한 사유 없이 정보통신시스템, 데이터 또는 프로그램 등을 훼손·멸실·변경·위조하거나 그 운용을 방해할 수 있는 프로그램

Programs that can damage, destroy, alter or counterfeit information communication systems, data or programs

4) 위험성 평가 Risk assessment

위험하거나 선박, 선원 및 화물에 손상 또는 손실을 줄 가능성이 있는 위협을 식별 하고 분석하는 과정

Identifying and analyzing threat to damage or loss to vessels, crew and cargo

5) 취약성 Weakness

시스템의 기능 명세, 설계 또는 구현 단계의 오류나 시동, 설치 또는 운용상의 문제점으로 인하여 시스템이 지니게 되는 보안상의 약한 부분을 의미

It means a weak part of the system's security due to system functional specification, design or implementation phase errors, startup, installation or operational problems

6) 기밀성 Confidentiality

자산이 인가된 당사자에 의해서만 접근하는 것을 보장하는 것

Ensure that assets are accessed only by authorized parties

7) 무결성 Integrity

자산이 인가된 당사자에 의해서 인가된 방법으로만 변경 가능한 것

The asset can be changed only in an authorized manner by the authorized party

8) 가용성 Fusibility

자산이 적절한 시간에 인가된 당사자에게 접근 가능해야 하는 것

The asset can be accessible to authorized parties at the appropriate time

1.5 절차의 개정 Revision of procedure

1) 본 절차서의 주요 사항을 제 개정 승인자

Person who approve establish/revision of this procedure


회사 보안 책임자

Company Security Officer

2) 절차서의 개정은 법률 법령 및 지침의 개정뿐만 아니라 새로운 보안위협에 대한 대응 및 경감 조치를 위해 이루어지도록 한다

절차 개정 시에는 하기 사항을 포함한 검토가 시행되어야 한다.

The amendment of the procedure shall be carried out not only to amend the laws and

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 1</p>	<p style="text-align: center;">일반사항 GENERAL</p>	<p>PAGE 4 / 4</p>

regulations but also to respond and mitigate new security threats.

A review including for following shall be carried out when this procedure is revised.

① 개정 필요성 분석

Analysis of need for revision

② 실무자의 적용 가능성 검토

Applicability review by staff

③ 관련 분야 외부전문가 검토 (필요 시)

External experts review (if need)

④ 보안협의회의 승인 (필요 시)

Security committee approval (if need)

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 2</p>	<p style="text-align: center;">방침 및 목표 POLICY AND OBJECTIVE</p>	<p>PAGE 1 / 2</p>

2.1 회사의 보안 방침

Company security policy

(1) 회사보안절차서 및 선박보안계획서의 목표

Objectives of Company Security Procedure& Ship Security Plan

1) 회사 보안 절차서

Company security procedure

- ① 회사 보안 절차서는 일반 보안위협 및 사이버 보안 위협에 대해 회사 및 선박의 공동 대응 절차를 마련하고 관련 보안체계를 구축하기 위한 것 이다

The company security procedures are established to arrange the response procedure for the company/ship security threats and cyber security threats and security system.

- ② 이 절차서는 우리 회사의 보안 업무 수행에 필요한 세부 시행절차를 규정함으로써, 비밀의 사외유출을 사전에 방지하여 경영 활동을 보호하고 나아가 회사발전에 기여함을 목적으로 한다.

The purpose of this procedure is to protect the management activities and to contribute the development of company by describing the detailed implementation procedures required to carry out security work of our company.

- ③ 사이버 보안 위협으로부터 회사와 선박이 보유한 정보 자산의 기밀성, 무결성, 가용성을 보장하는데 목적이 있다

It aims to ensure the confidentiality, integrity and availability of the information assets from cyber security threats.

2) 선박 보안 계획서

Ship security plan

- ① 선박의 보안을 증진하여 해상에서의 테러 위협을 방지하고 각종 불법 행위에 대하여 적절히 대응하기 위한 것 이다.

The objectives of Ship security plan are in promoting the security of ship so as to prevent terrorism at sea and to cope with other illegal acts in an appropriate manner.

The ship security plan complies with the SOLAS

- ② 선박 보안 계획서는 국제 해사 기구(IMO)의 해상인명안전협약(SOLAS) 11-2장 및 ISPS Code 요건을 준수한다.

The ship security plan complies with the SOLAS II-2 and ISPS Code.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 2</p>	<p style="text-align: center;">방침 및 목표 POLICY AND OBJECTIVE</p>	<p>PAGE 2 / 2</p>

2.2 보안 임무 및 보안조치 개발

Security duties & development of security measures

- (1) 회사 및 선박의 보안을 유지하며 이를 계속해서 수행하여야 하는 것은 회사 육상직원 및 해상직원의 임무이다.

To maintain the security of the company and ship is the duty of the shore staff and crew.

- (2) 만일, 대처할 수 없는 잠재적인 새로운 위협이 존재한다면, 대응 가능한 추가적인 보안조치를 식별하여 이행하여야 한다.

In case where new potential threat to the security of ship exists, the company shall ensure that additional measures to deal with such threat can be identified and carried out. In particular cyber security threat, identify

- (3) 특히 사이버 보안 위협의 경우, 대응 가능한 추가적인 보안조치를 식별하고 IT 시스템에 대한 SW 및 펌웨어에 대한 검토 등 보안위협에 상응하는 보안조치를 이행하여야 한다.

In particular cyber security threat, identify additional security measures and implement security measures such as reviewing SW and firmware for IT system.

2.3 보안 유지


Security maintenance

- (1) 본 회사 보안 절차서 및 보안 관련 정보는 도난, 화재 또는 파괴로부터 보호되고 비인가자의 접근을 방지할 수 있는 적절한 서버에 보관한다.

This company security procedure and security information shall be protected from robbery, fire, destruction and kept in server to prevent from unauthorized access or disclosure.

- (2) 기록의 열람 및 외부로의 유출은 회사 보안 책임자의 허가를 득해야 한다.

The perusal and disclosure of records shall be done under the permission of CSO.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
Ch. 3	<p style="text-align: center;">조직 및 책임과 권한 ORGANIZATION, RESPONSIBILITY AND AUTHORITY</p>	<p>REV. NO. : 0</p> <p>PAGE 1 / 5</p>

3.1 회사 보안 조직

Company Security Organization

(1) 회사의 의무

Obligation of the company

: 회사는 회사 보안 책임자 및 선박 보안 책임자가 의무와 책임을 수행할 수 있도록 필요한 지원을 제공해야 한다.

The company should provide the necessary support to fulfill their duties and responsibilities to Company Security Officer and Ship Security Officer.

(2) 회사 보안 책임자

CSO, Company Security Officer

1) 임명

Designation

: 회사 보안 책임자는 회사 내 보안활동에 대하여 총괄하는 자이며, 부재 시 대행자가 회사 보안 책임자의 업무를 수행한다.

The Company Security Officer is responsible for the security activities in the company, in the case of absence, the Alternative Company Security Officer shall acting as the CSO.

① 회사 보안 책임자 Company Security Officer

성명 Name - 이종석 Lee, Jongseok

연락처 Contact - Mobile : +821020751236 E-mail : jslee@korinstar.com

② 대행자 Alternative Company Security Officer

성명 Name - 하휘영 Ha, Hwiyoung

연락처 Contact - Mobile : +821028177924 E-mail : hyha@korinstar.com


2) 책임과 의무

Responsibilities and duties

: 회사 보안 책임자는 “코린스타㈜”의 모든 보안에 대한 책임이 있으며 주요 업무는 다음과 같다.

The CSO is responsible for all security of the Korin Star Co., Ltd. and the main tasks are as follows;

③ 회사 보안 계획 수립 및 이행 총괄

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 3</p>	<p style="text-align: center;">조직 및 책임과 권한 ORGANIZATION, RESPONSIBILITY AND AUTHORITY</p>	<p>REV. NO. : 0</p> <p>PAGE 2 / 5</p>

Establishment and implementation of company security plan

- ④ 회사 및 선박의 사이버 보안 활동 총괄

Generalization of cyber security activities in company and ship

- ⑤ 주관청 또는 인증기관에 대한 심사 및 적합성 검증

Examination and verification for compliance with the administration or certificate authorities

- ⑥ 위기 대응 관리 체계 구축 및 보안사고 지휘

Establishment of security crisis response management system and command security incident

- ⑦ 회사 보안 교육총괄

Generalization of enterprise security education

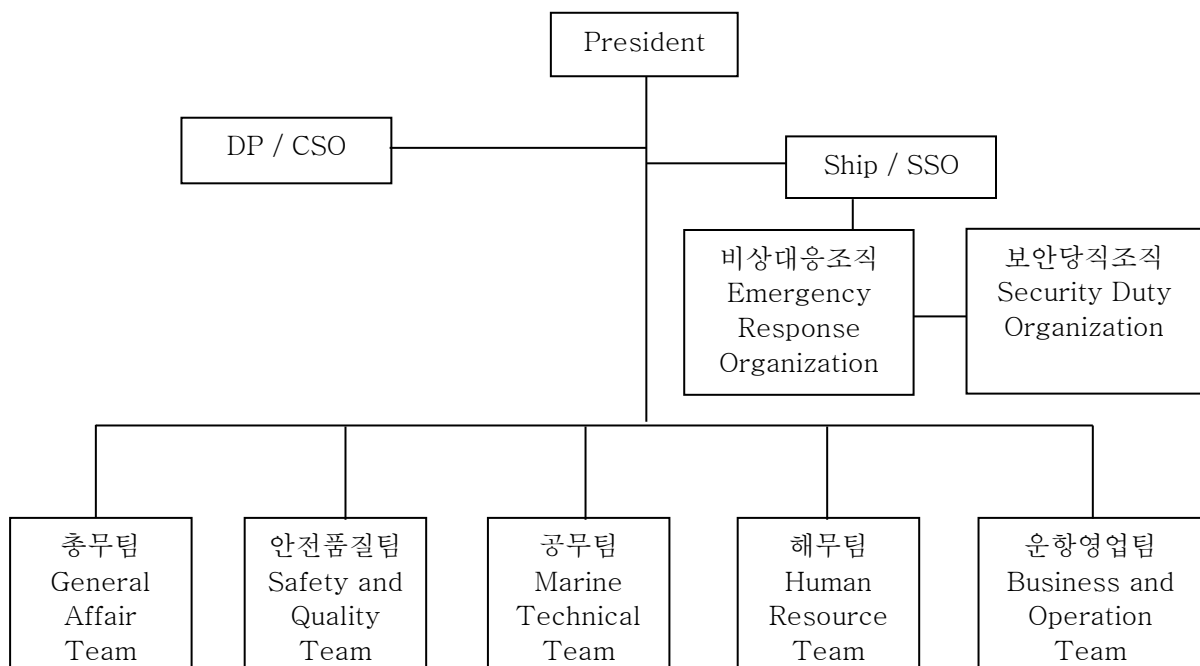
3.2 선박 보안 조직

Vessel Security Organization

- (1) 회사 보안 업무의 효율적 수행을 위하여 보안 업무 조직을 구성 및 운영한다.


To conduct the company security tasks efficiently the company security organization is operated

- (2) 회사 / 선박 보안 조직도 Company/ship security organization chart



- (3) 보안 관리자

Security Manager

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
Ch. 3	<p style="text-align: center;">조직 및 책임과 권한 ORGANIZATION, RESPONSIBILITY AND AUTHORITY</p>	<p>REV. NO. : 0</p> <p>PAGE 3 / 5</p>

- 1) 회사보안책임자의 지시를 받아 보안업무를 수행하는 관리자로 다음과 같은 업무를 일반적으로 수행한다.

As a manager performing security tasks under the direction of the company security officer, the following tasks are performed;

2) 안전품질팀장


Leader of Safety and quality team

- ① 회사 / 선박 사이버보안 대응
Company and vessel cyber security response
- ② 사이버 보안 관련 규정 검토
Cyber security regulation review
- ③ 사이버 보안 동향 파악
Cyber security trends identification
- ④ 보안 조직 관리 및 운영
Manage the security organization
- ⑤ 보안 사고 발생 시 대응 운영
Response actions in case of security incident
- ⑥ 보안 관련 대외업무 수행
Implement the external business regarding the security
- ⑦ 보안대책 마련
Arrange the security measure
- ⑧ 보안계획의 수립 및 운영
Establishment and operation of security plan
- ⑨ 보안 관련 국제 규정 검토
Review the international security regulation
- ⑩ 보안 절차 및 지침 제/개정
Legislate & amend the security procedure & instruction

3) 총무팀장

Leader of General affair team

- ① 사내 보안구역 및 시설 관리
Manage the security area and facilities in office
- ② 교육 및 훈련
Education and training

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
Ch. 3	<p style="text-align: center;">조직 및 책임과 권한 ORGANIZATION, RESPONSIBILITY AND AUTHORITY</p>	<p>REV. NO. : 0</p> <p>PAGE 4 / 5</p>

4) 해무팀장

Leader of Human resource team

① 보안사고 관련 인사업무 지원

Personnel support regarding security incident

(4) 부서별 보안 담당자

Departmental Security Officer at each team

- 1) 부서별 보안담당자를 지정하여 운영 할 수 있으며, 부서별 보안 담당자는 다음과 같은 업무를 수행한다.

The departmental security officer can be designated and operated, the departmental security officer performs the following tasks;

- 2) 보안정책 및 지침 이행 및 보안담당자 보고

Implement the security policy and instruction & report to the security officer

- 3) 보안정책에 대한 부서별 의견 제시

Presentation of opinion for the security policy

(5) 보안위원회

Security committee

- 1) 회사 내 보안 업무와 관련된 정책 및 활동의 심의, 의결을 위하여 보안협의회를 구성한다.

보안협의회는 필요 시 위원회를 개최하여 아래의 내용을 검토한다

To deliberate and decide the policies and activities regarding to security activities in the company the security committee shall be composed.

The security committee reviews as follows;

- ① 보안규정 및 절차서 개정 심의

Review the security regulation and procedure revision

- ② 보안사고 대응 및 위규자 심사

Response the security incident and screen the violation


- ③ 기타 보안업무 수행상 협의 조정을 요하는 사항

Other matters regarding to security tasks

- 2) 보안 협의회 구성

Construction of security council

- ① 위원장

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 3</p>	<p style="text-align: center;">조직 및 책임과 권한 ORGANIZATION, RESPONSIBILITY AND AUTHORITY</p>	<p>REV. NO. : 0</p> <p>PAGE 5 / 5</p>

Chairman

: 회사 보안 책임자

Company Security Officer

② 구성원

Members

: 각팀 팀장

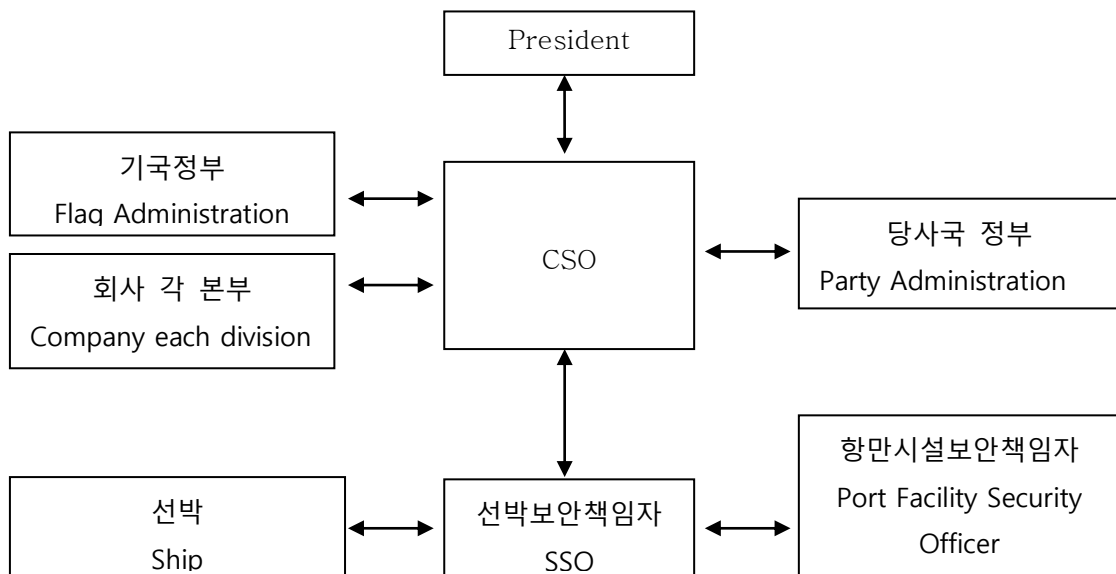
Each team leaders

(6) 외부이해 관계자

External interested parties

회사는 내부 보안 업무 관계자와 선박 기국 정부, 당사국 정부, 선박 보안 책임자, 항만 보안 책임자등 이해 관계자와 교섭하여야 하며 이들은 선박 보안 등급 책정, 보안 조치 및 절차와 관련하여 이러한 이해관계자와 적절한 교섭을 하여야 한다.

The company shall have a consultation with external interested parties like governments, SSO, PFSO about the security level, security measures and security policies.




(7) 선박보안조직

Ship security organization

: 각 선박의 선박보안계획서에 따른다.

Refer to the security plan for each ship

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 4</p>	<p style="text-align: center;">보안 위협, 사고, 침해 대응 RESPOND TO SECURITY THREAT, INCIDENT, INFRINGEMENT</p>	<p>REV. NO. : 0</p> <p>PAGE 1 / 4</p>

4.1 보안 위협 대응

Respond to security threats

(1) 보안 위협의 식별

Identification of security threats

- 1) 회사 사무실, 선박 항행 구역에 적용되는 보안 위협을 식별하여야 하며 식별된 위협은 환경이 변화함에 따라 재검토 및 수정되어야 한다.

Identified threats which are applied to office and vessel navigation area should be reviewed and modified as the environment changes.

- 2) 보안 위협 종류

Kind of security threat

: 정보유출, 기물파손, 밀항자, 화물 절도, 사이버보안 위협, 항만보안 취약성, 밀수, 해적행위, 테러 등

information leakage, vandalism, stowaways, cargo stealing, cyber security threats, port security vulnerabilities, smuggling, piracy and terrorism.

(2) 취약성 분석

Vulnerability Analysis

- 1) 회사는 회사 및 선박 항해 구역 내 모든 자산에 대한 관리적 기술적 취약점을 분석하여야 한다.

The company should analyze the managerial and technical vulnerability of all assets within the company and the ship's navigation area.

- 2) 기술적 취약점의 경우 시스템에서 직접 확인하는 수작업, 자동화 도구 등 모의해킹의 수단을 이용하여 분석을 수행할 수 있다.


In case of technical weakness, the analysis can be performed by means of simulation hacking such as manual and automated tools that are directly identified in the system.

- 3) 취약점 분석 결과는 기밀사항으로 간주되며 회사보안책임자는 이를 위험평가에 반영할 수 있다

Vulnerability analysis results are considered to be confidential and the Company Security Officer can incorporate them into the risk assessment.

(3) 보안 위험성 평가

Security Risk Assessment

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
Ch. 4	<p style="text-align: center;">보안 위협, 사고, 침해 대응 RESPOND TO SECURITY THREAT, INCIDENT, INFRINGEMENT</p>	<p>REV. NO. : 0</p> <p>PAGE 2 / 4</p>

- 1) 회사 및 선박 내 시스템 자산에 대한 보안 위협은 의도적이나 비인가된 위반, 의도적이지 않으나 돌발적인 위반, 시스템 완전성 결여 등과 같은 위협을 포함한다.

Security threats to company and shipboard system assets include threats such as intentional or unauthorized violations, unintentional but unexpected violations, and lack of system integrity.

- 2) 항해, 엔지니어링, 기관제어 및 통신 시스템의 직간접적 통신에 대한 외부 위협이나 부적절한 사용에 대한 취약점을 식별하여야 한다.

Therefore, it should identify vulnerabilities to external threats or improper use of direct or indirect communications in navigation, engineering, institutional control and communication systems.

(4) 보안위협 대응 및 관리방안

Security Threat Response and Management Plan

- 1) 회사는 보안위협을 경감하기 위하여 전사적인 대응방안을 수립하여야 한다.

The company should establish enterprise-wide countermeasures to mitigate security threats.

- 2) 회사보안책임자는 위험평가에서 도출된 보안위협에 대하여 소요비용, 적용 용이성 등 내/외부 환경을 고려한 우선순위를 정하여 위험관리방안을 수립해야 한다.

The Company Security Officer should establish a risk management plan by prioritizing the security threats derived from the risk assessment, taking into account the internal and external environment, such as cost and ease of application.

- 3) 회사보안책임자는 위험관리방안이 일관성 있게 수립 및 이행되도록 관련 사항을 감독하고 문서화하여 주기적으로 검토한다.


The Company Security Officer oversees documents and periodically reviews relevant matters to ensure that risk management practices are established and implemented consistently.

4.2 보안사고 및 보안침해 보고

Reporting of security incident and infringement

- (1) 선박보안책임자는 다음과 같은 경우 즉시 회사보안책임자 및 당사국정부에게 보고 하고 수신자는 접수 사실을 회신하여야 한다.

The Ship Security Officer should immediately report to the Company Security Officer and to the Government of the Parties in the following cases and the recipient shall reply to the receipt.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
Ch. 4	<p style="text-align: center;">보안 위협, 사고, 침해 대응 RESPOND TO SECURITY THREAT, INCIDENT, INFRINGEMENT</p>	<p>REV. NO. : 0</p> <p>PAGE 3 / 4</p>

- 1) 항해나 정박 중 외부로부터 보안 침입 또는 보안침입시도가 발생한 경우

When a security intrusion or security intrusion attempt occurs from the outside while sailing, docking or anchored

- 2) 선박보안경보장치의 오작동, 비상연안국의 오호출

Malfunction of the ship security alarm system

- 3) 선박보안계획서 관리상의 중대한 잘못 및 운용상의 위반

Significant mistakes and operational violations in the management of the ship security plan

(2) 보고서 내용 및 형식

Report content and format

: 보안 관련 보고서의 내용은 간단명료하게 작성되도록 한다.

Make sure that the contents of the security report are simple and clear.

(3) 보고 절차

Reporting procedure

- 1) 보안과 관련하여 작성된 보고서는 팩스, 이메일 등 가급적 빠른 수단을 이용하여 전달하고, 수신자는 무선 또는 유선상으로 수신여부를 확인해야 한다.

The security- related reports should be delivered by using Fax, E-Mail, etc.. as soon as possible, and receiver should confirm by wire or wireless means.

① 선박 내부

Internal ship reporting

모든 보안 관련 사고 및 침해는 선박 보안 책임자에게 즉시 보고한다.

All Security Incident and Infringement should be reported to SSO.


② 선박에서 회사로의 보고

Vessel to the company

보안 관련 부적합 사항, 보안사건 및 보안 침해는 즉시 회사 보안 책임자에게 보고한다.

Non-conforminty, Security Incident and Infringement should be reported to CSO immediately.

③ 선박에서 외부기관으로의 보고

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
Ch. 4	<p style="text-align: center;">보안 위협, 사고, 침해 대응 RESPOND TO SECURITY THREAT, INCIDENT, INFRINGEMENT</p>	<p>REV. NO. : 0</p> <p>PAGE 4 / 4</p>

Vessel to the external authorities

긴급한 경우를 제외하고, 회사 보안 책임자에게 사전 보고 후 지침에 따라 보고한다.

Except of emergency cases, all reporting shall be done to company first, then vessel follow company instruction

④ 회사에서 외부 기관으로의 보고

Company to external authorities

회사 보안 책임자 지시하에 해양수산부 종합 상황실에 보고한다.

All Security Incident and Infringement should be reported to Korea Ministry of Oceans and Fisheries under CSO's order.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 5</p>	<p style="text-align: center;">보안 교육 및 훈련 SECURITY TRAINING AND DRILL</p>	<p>PAGE 1 / 5</p>

5.1 교육 및 훈련내용 식별

Identification of training and drills contents

(1) 보안교육 계획 및 이행

Security training plan and implementation

- 1) 회사는 회사 및 선박 내 모든 인력을 대상으로 보안교육 계획을 수립하고 보안업무 전반에 대한 교육을 실시하여야 한다.

The Company shall establish a security education plan for all personnel in the Company & vessels and conduct education on the entire secure task.

- 2) 보안교육은 신규 채용자, 해외주재원 발령자, 해외 출장자 등 모든 직원을 대상으로 연 1회 이상 실시하여야 한다.

Security education should be carried out at least once a year for all employees who are new employees, overseas employees and overseas travelers.

- 3) 선박 내 보안교육의 경우 최소 3개월 주기로 1회 이상 실시하여야 하며 승선인원의 4분의 1 이상이 교대된 경우에는, 지난 3개월 내에 선박에서 수행된 어떠한 훈련에도 참여 하지 아니한 인원들과 함께 선원교대가 이루어진 날로부터 일주일 이내에 교육 및 훈련을 실시한다.

Security drill within vessels should be conducted at least once every 3 months and in case more than 1/4 of crew has been changed, the education with the participation of new crew as well as the crew who have not undertaken any drill in the last 3 months shall be carried out within a week from the date of such crew change.

- 4) 보안 전담 인력의 경우 연 1회 이상 보안교육 및 세미나를 실시하여 회사 및 선박 보안에 대한 지속적인 경각심을 가지도록 한다.

Person in charge of security should conduct annual security training and seminars at least once a year to ensure continuous awareness of the company and vessel security.

- 5) 육해상(주관청, 회사보안책임자 등이 참여하는) 합동연습은 연 1회 실시하며 실시간격이 18개월을 초과할 수 없다.

A ship/shore joint exercise(with the participation of authority and the CSO) should be once a year and no more than 18 months between the exercise.

- 6) 회사는 아래 예시와 같은 보안활동 장려정책 등 효과적인 방안을 강구하여 육상, 선박 및 외주 업체 직원들의 보안 및 사이버 보안에 대한 인식이 증진될 수 있도록 하여야 한다. The Company should promote effective measures of security and cyber security for the promotion of security activities such as the following examples, to promote awareness of the security and cyber security of shore staff, ship's crew, and subcontractor employees.

	<div> <div>보안 절차서</div> <div>SECURITY PROCEDURE</div> </div>	<div>DOC NO. : PR - 19</div> <div>REV. NO. : 0</div>
<div>Ch. 5</div>	<div>보안 교육 및 훈련</div> <div>SECURITY TRAINING AND DRILL</div>	<div>PAGE 2 / 5</div>

(2) 교육훈련계획

Training, drills and exercises plan

구분 Lists	대상 To whom	내용 Contents	주기 Interval	비고 Remark
교육 Training	회사보안책임 자/대행자 CSO & Alternative CSO	회사보안책임자의 책임과 의무, 지식 Role and responsibilities, duties, company's activities and knowledge of the CSO and ISPS Code	최초1회 Before being appointed as CSO	
교육 Training	내부심사자 Internal auditor	내부심사자의 책임과 의무, 지식 Role and responsibilities, duties and knowledge of the internal auditor and ISPS code	최초1회 Before being appointed as internal Auditor	
	전 직원 All staff	보안 브리핑/세미나 Security briefing and seminar	1년 1 year	회사보안책임자 CSO
	선박보안책임 자 SSO	선박보안책임자의 책임과 의무,지식 Responsibilities, duties and knowledge of the SSO	최초1회 Once at the first designation	
	기관장, 일항사 C/E, C/O	특정 보안임무 Ship specific security duties	승선 1주일 내 Within a week of joining the ship	선박보안책임자 SSO
	전 승무원 All crews	선박보안 숙지 Ship security familiarization	1년 1 year	승선 전 친숙교육 또는 선상교육 Pre-Joining education or shipboard training
		보안 브리핑 Security briefing	필요 시 If needed	선박보안책임자 SSO

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 5</p>	<p style="text-align: center;">보안 교육 및 훈련 SECURITY TRAINING AND DRILL</p>	<p>PAGE 3 / 5</p>

<p>훈련 Drills</p>	<p>전 승무원 All crews</p>	<p>폭발장치, 방화, 파괴행위 등에 의한 선박손상 또는 파괴 Damage or destruction of the ship by explosive devices, arson, sabotage or vandalism</p>	<p>3개월 및 승무원 1/4이상 교대 시 1주일내 3 months and within a week of the change, if crew changed more than 25%</p>	<p>1년에 전 항목 시행 All contents should be conducted within 1 year</p>
		<p>선박 또는 승무원의 납치 또는 강탈 Hijacking or seizure of the ship or of persons on board</p>		
		<p>화물, 필수적인 선박장비나 시스템 또는 선용품에 대한 조작 Tampering with cargo, essential ship equipment or systems or ship's stores</p>		
		<p>허가받지 아니한 접근 또는 사용 (밀항자 포함) Unauthorized access or use, including presence of stowaways</p>		
		<p>무기 또는 설비의 밀수 Smuggling weapons or equipment</p>		
		<p>보안사건을 일으킬 목적으로 범인 또는 그들의 개인장비의 운송 수단으로 선박사용 Use of the ship to carry those intending to cause a security incident and/or their equipment</p>		
		<p>선박자체를 무기로 사용 Use of the ship itself as a weapon</p>		
		<p>접안/묘박 중 해상으로부터의 공격 Attacks from seaward whilst at berth or at anchor</p>		
		<p>해상에 있는 동안의 공격 Attacks whilst at sea</p>		

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 5</p>	<p style="text-align: center;">보안 교육 및 훈련 SECURITY TRAINING AND DRILL</p>	<p>PAGE 4 / 5</p>

<p>연습 Exercises</p>	<p>선박/육상 Ship/shore</p>	<p>육해상 합동연습 Ship/shore joint exercises</p>	<p>1년 1 year</p>	<p>가능하면 당사국, 항만시설보안책 임자 등 참여 Including participation of PFSO, relevant authorities of Contracting Government</p>
-------------------------	-----------------------------	--	----------------------	--

(3) 사이버 보안 교육 및 훈련

Cyber Security Education and Training

: 회사는 사이버 보안에 대하여 효과적으로 대응하기 위하여 다음과 같은 교육과정을 고려할 수 있다.

The company can consider the following training courses to effectively respond to cyber security.

- 1) 회사 정보 보안 관리
Company information security management
- 2) 개인 정보 보안 관리
Personnel information security management
- 3) 웹서비스/모바일(이메일, SNS) 관리
Web/Mobile(E-mail, SNS) management
- 4) 출입통제시스템 관리
Access control system management
- 5) 정보유출 신고 방법
Information leakage reporting method

5.2 평가 및 개선

Evaluation and improvement

(1) 보안 평가 및 지원

Evaluation and improvement

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 5</p>	<p style="text-align: center;">보안 교육 및 훈련 SECURITY TRAINING AND DRILL</p>	<p>PAGE 5 / 5</p>

- 1) 선박보안책임자는 실시된 보안 교육에 대하여 평가를 실시하고 평가결과가 만족스럽지 못하다고 판단되었을 시 효과적인 보안교육이 이루어지도록 재교육을 시행하는 등 적극적 인 지원을 하여야 한다.

The SSO should carry out an evaluation after the completion of security training, where the evaluation finds that the training given is unsatisfactory, the SSO should completely support retraining in order that effective security training is implemented.

- 2) 회사보안책임자는 적절한 간격으로 회사 및 선박보안계획서의 효율적인 이행을 보장하여야 한다.

The CSO shall ensure effective implementation of the Company's and Ship's security plans at appropriate intervals.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 6</p>	<p style="text-align: center;">보안 조치 SECURITY MEASURES</p>	<p>PAGE 1 / 8</p>

6.1 회사 보안 조치

Company Security Measures

(1) 회사보안조치

Company security measures

1) 보안장비

Company equipment

① 보안장비의 식별

Identification of security equipment

회사 내 중요 정보 및 선박 통신과 관련한 자산을 다루는 하드웨어(서버, 네트워크, 장비, PC, 프린터 등), 소프트웨어 등 시스템 자산을 보호하기 위하여 시스템 자산 가치의 중요도에 따라서 보안장비를 식별하여야 한다.

Security equipment should be identified according to the importance of the system asset value to protect the system assets such as hardware(network, equipment, PCs, printers, printers, etc.,) and software etc. covering the company's critical information and ship network.

② 보안장비의 관리 및 유지

Management and maintenance of security equipment

회사 내 보안장비는 적절한 운영 여부에 대하여 검토되어야 하며, 특히 회사 업무의 연속성에 영향을 미치는 중요 장비의 경우 운영기록을 주기적으로 점검하고 이에 대하여 지속적으로 모니터링 하여야 한다.


The Company's security equipment shall be reviewed for proper operation, particularly for critical equipment that affects the continuity of the company, and shall periodically monitor and continuously monitor the operation of the Company.

③ 보안장비의 관리 및 유지 기록

Records of security equipment

회사 내 보안장비에 대한 관리 및 유지절차에 대하여 관련 이력을 기록하고 보관하여야 한다.

Records and maintenance procedures shall be recorded regarding the management and maintenance procedures of the Company in the Company.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 6</p>	<p style="text-align: center;">보안 조치 SECURITY MEASURES</p>	<p>PAGE 2 / 8</p>

2) 출입통제

Access control

① 일반적 출입통제 (방문자 통제 및 검색 절차)

General access control (Visitor controls and search procedures)

회사 내 임직원, 파견직, 계약직, 외주용역 직원 등 회사에서 근무하는 모든 근무자 및 방문자에 대하여 출입통제 사항을 관리하고 출입내역에 대하여 기록 및 관리하여야 한다.

The Company shall manage and maintain access control particulars and record entry details for all employees including dispatched staff, contract staff, outsourcing service personnel, etc. and visitors

② 제한구역 통제

Restricted area

회사 내 중요 자산 및 시설에 대한 보안강화를 위하여 제한구역을 지정/운영한다. 제한구역은 비밀 또는 중요시설 및 자재에 대한 비인가자의 접근을 방지하기 위하여 비인가자의 출입이 금지되는 보안상 중요한 구역으로 관리된다.

The restricted areas shall be designated and operated for the strengthening of security of critical assets and facilities in the Company. Restricted area where instructions are required to prevent unauthorized access to confidential or critical facilities and materials as part of the restricted area.

3) 보안감시

Monitoring and surveillance


회사 내 관리적, 기술적, 물리적 보안조치가 적절하게 이루어지고 있는지 주기적으로 모니터링 하여야 하며, 이에 대한 적절한 감시가 이루어지도록 조치하여야 한다.

Regularly monitor whether the maintenance, technical and physical security measures are adequately implemented in the Company, and ensure proper monitoring of them.

4) 통신보안

Communication security

회사 내 관리자, 유지보수 작업자는 회사 및 선박 내 시스템에서 통신암호화를 사용하지 않은 프로토콜 사용을 금지하고 암호화가 적용된 프로토콜 사용하여야 한다. 외부에서 원격으로 통신을 하는 경우 VPN(가상 사설망)을 적용하여 안전한 통신이 이루어질 수 있는 인증 체계를 구축해야 한다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 6</p>	<p style="text-align: center;">보안 조치 SECURITY MEASURES</p>	<p>PAGE 3 / 8</p>

Encrypted protocol shall be used company and ship's communication system. Remote communication shall be carried out by provided VPN(Virtual Private Network) for safe communication.

5) 회사 보안 및 사이버 보안 대응

Company cyber security response plan

① 보안 지침 수립

Establishment of guideline

회사 내 보안관리자 및 보안담당자는 회사 및 선박 상세 보안지침을 수립하여 관리하여야 한다.

Company cyber security officer should establish and manage company and ship's cyber security guideline.

a. 인적 보안

Human security

- a) 모든 임직원의 신규 채용 및 퇴직 시 회사 및 선박 내 영업비밀 및 보안 기밀사항에 대하여 비밀 유지의무를 위한 '영업비밀보호 서약서'를 받아야 한다.

All employees must submit a 'business proprietary confidentiality agreement' for the confidentiality obligation of the company.

- b) 외주업체 등 외부인에 대해서도 '영업비밀보호 서약서'를 받아야 한다.

It is also necessary to collect a 'business proprietary confidentiality agreement' for subcontractors

- c) 모든 임직원은 출장 중 회사 보안절차서를 포함한 보안 지침을 준수하여야 한다.

All employees must comply with security guideline including company security procedure during business trips.

b. 서버 보안

Server security

- a) 서버 및 SWITCH HUB 등 중요 네트워크 설비 설치장소는 통제구역으로 지정하고, 상시 잠금 상태를 유지하여야 하며, 지정된 관리자 외에는 출입을 금지한다.

Server room shall be designated as restricted area and maintained locked

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 6</p>	<p style="text-align: center;">보안 조치 SECURITY MEASURES</p>	<p>PAGE 4 / 8</p>

condition. And access to server room shall be prohibited except authorized person.

- b) 보안상 위협이 식별된 경우 서버의 업무를 중단하고 이를 즉시 개선해야 한다.

Cyber threat on server shall be improved after ceased operation.

- c) 서버의 설치 또는 제거 시 최적의 방안을 마련하여 회사전산보안 책임자에게 보고하고 승인을 득한 후 시행해야 한다.

Server unit shall be renewed after approved by company cyber security officer.

c. 네트워크 보안

Network

- a) 보안관리자는 회사 내 네트워크를 구성도를 유지 및 관리하여야 한다.

Company cyber security officer shall be managed network diagram.

- b) 외부침입에 대비하여 침입탐지시스템 및 침입차단시스템을 상시 운영하여야 한다.

Intrusion detection system(IDS) shall be maintained to prevent network attack.

- c) 내/외부 전산망의 연결 또는 단락이 필요한 경우 최적의 방안을 마련하여 전산 보안 책임자에게 보고 및 승인을 득한 후 시행해야 한다.

Connection of network shall be operated after approved by company cyber security officer.

d. 응용프로그램 보안

Application program

- a) SW 패키지 또는 SW 개발물을 회사 또는 선박 내 신규로 적용할 경우에는 관련 절차에 따라 위험성평가 후 설치되어야 한다.

New software package shall be installed after carry out risk assessment in accordance with relevant procedure.


- b) 기존 설치된 SW 또는 펌웨어에 변경이 필요할 경우 위험성평가를 실시한다.

Installed software or firmware shall be modified after carry our risk assessment.

e. DB 보안

DB Security

- a) 중요 데이터베이스 및 WAS(WEB APPLICATION SERVER)는 용도에 따라 필요한 PORT 만 연결하고 다른 PORT 는 차단되어야 한다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 6</p>	<p style="text-align: center;">보안 조치 SECURITY MEASURES</p>	<p>PAGE 5 / 8</p>

DB and WAS (Web Application Server) shall be connected by approved port only.

- b) DBMS 관리를 위한 계정은 데이터베이스 관리자(DBA)만이 사용할 수 있고 접근의 타당성에 대하여 주기적으로 검토하여야 한다.

Administrator account shall be used by Database administrator (DBA) only.
Validity of account shall be reviewed periodically.

f. 접근 권한 및 인증

Access right and authentication

- a) 시스템 영역별로 사용자 계정 및 접근권한은 사전 허가된 인원에만 부여하고

변경 이력을 관리해야 한다.

Account and access right shall be furnished to authorized person. History shall be recorded and managed.

- b) 관리자 권한의 계정은 별도의 목록으로 관리하며 사용자 계정은 최소한으로 제한되어야 한다.

Administrator account shall be furnished and managed by assigned list. User account shall be furnished to essential use only.

- c) 시스템에 대한 접근은 사용자 계정 및 패스워드를 이용하여 통제되어야 하며, 매 3 개월마다 주기적으로 패스워드를 변경하여야 한다.

Access to system shall be controlled by user account and password. Password shall be changed every 3 months.

g. 매체보안

Medium Security


- a) 전산보안책임자는 회사 내 시스템 별로 저장매체 처리에 관한 절차를 수립하고 사용현황 및 변경 이력을 관리하여야 한다.

Company cyber security officer shall be established management procedure for storage medium per each IT system. History shall be recorded and managed.

- b) 휴대용 저장매체는 백신프로그램을 이용한 점검으로 악성코드로부터 보호되어야 한다.

Portable storage medium shall be used after checking by vaccine program.

h. 악성 소프트웨어 관리

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 6</p>	<p style="text-align: center;">보안 조치 SECURITY MEASURES</p>	<p>PAGE 6 / 8</p>

Control of Malware

- a) 시스템은 바이러스 등 악성 소프트웨어로부터 보호될 수 있도록 백신 프로그램을 이용하여 점검되어야 한다.

Vaccine program shall be furnished to every IT system for prevent malware.

- b) 모든 시스템은 보안패치 및 최신 업데이트가 적용되어야 하고, 지속적으로 모니터링 되어야 한다.

Security patch and Up-date shall be applied to every IT system and monitored.

- c) 악성 소프트웨어가 침투되었을 경우 피해를 최소화하기 위한 조치가 사전 수립 및 적용되어야 한다.

Response plan for malware infection shall be established and applied.

- d) 회사 내 모든 사용자를 대상으로 악성 소프트웨어 탐지 및 예방 등에 대한 정보를 지속적으로 제공한다

Malware information shall be distributed to all IT system user continuously.

6) 회사 보안장비

Company security equipment

- ① 회사 내 물리적, 기술적, 관리적으로 적용된 보안 요구사항에 대하여서는 별도의 절차나 장비를 통하여 지속적으로 모니터링 하도록 한다.


The company shall continuously monitor the security requirements of the company's physical, technical and administrative requirements through a separate procedure or equipment.

- ② 회사 보안을 위한 대표적인 장비로는 네트워크 방화벽, 시스템 방화벽, 바이러스 백신 등이 있으며, 물리적 보안을 위해서 회사 내 스피드 게이트 등 출입통제 장치 설치, 사원증 발급, CCTV 설치 등이 포함될 수 있다.

Typical equipment for corporate security include network firewalls, system firewalls, virus vaccines, installation of access entrance control systems and CCTV in the office, issuance of employee ID card, etc., for physical security may be included as well

- ③ 해당 보안조치와 장비는 지속적인 관리를 통하여 사이버보안 위협 모니터링 정보로 활용하도록 한다.

Security measures and equipment should be used as a cyber security threat monitoring information through continuous management.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 6</p>	<p style="text-align: center;">보안 조치 SECURITY MEASURES</p>	<p>PAGE 7 / 8</p>

7) 출장 방침

Travel policy

- ① 출장 전 출장지 위험성관련 정보를 아래의 사이트에서 사전 확인한다.

Before business travel, any hazardous and risk at travel area should be checked below web- site

- a. 외교통상부(해외안전여행) : <http://www.0404.go.kr/dev/main.mofa>

Ministry of Foreign Affairs and Trade (MOFAT)

- b. 기상청 : <http://www.kma.go.kr>

Meteorological Administration[Agency]

- c. 국가재난안전포털 : <https://www.safekorea.go.kr>

The National Disaster and Safety portal

- ② 출장지 위험 여부를 출장 신청서 특기사항에 기록한다.

The hazardous and risk at travel area should be recorded at business travel approval request.

8) 기타 보안조치

Other security measures

- ① 사용자의 모바일 사용에 대하여 명확한 접근통제 조치를 설정하여 모니터링 하여야 한다.

Company should establish and monitor clear access controls for users ' mobile use.

- ② 중요정보를 취급 시 내부 서버에서 외부 인터넷 접속을 제한 등 인터넷 접속 제한 조치가 적용되어야 한다.


Access restrictions should be imposed on internal internet access limits, such as limiting access to external internet connections when handling critical information.

- ③ 로그 기록 보존이 필요한 시스템을 지정하여 시스템 및 장비 별로 로그유형 및 보존기간을 정하여 관리하여야 한다.

Company should specify the system that requires preservation of log records and manage the log type and retention period for each system and equipment.

- ④ 혁신적 보안 기술 및 시스템 도입 시 관련 물리적 조치 및 기술적 보안조치에 대하여 지속적인 모니터링을 이행한다.

Monitoring of physical and technical security measures should be carried out

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 6</p>	<p style="text-align: center;">보안 조치 SECURITY MEASURES</p>	<p>PAGE 8 / 8</p>

continuously when introducing innovative security technologies

6.2 선박 보안 조치

Vessel Security Measures

(1) 드론에 관한 보안

Security for drone

- 1) 선박의 상공에 드론 운용이 필요한 경우 사전에 선박의 보안 책임자와 아래의 사항을 협의 하고 허가를 득하여야 한다.

In case the drone is required to operate over the ship, the following matters should be consulted with the security officer of the ship and permission should be obtained.

① 드론 운용 지역

Drone operation area

② 드론 운용 시간

Drone operation time

③ 드론 운용 목적

Purpose of Operation of drone

④ 드론 운용자 위치

Drone Operator Location

- 2) 사전에 허가 받지 않은 드론의 접근은 제한 하여야 한다.

Unauthorized drone access should be restricted.

- 3) 드론으로 촬영된 선박의 사진 및 영상은 선박의 보안 책임자의 허가 없이 외부로 공개해서는 안된다.


Photographs and images of vessels photographed by drone should not be disclosed to the outside without permission of the ship's security officer.

(2) 그밖의 사항

Others

각 선박의 선박보안계획서에 따름

Refer to the SSP for each ship

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 7</p>	<p style="text-align: center;">보안 기록 및 보안정보 관리 RECORD MAINTENANCE AND MANAGEMENT OF SECURITY INFORMATION</p>	<p>REV. NO. : 0</p> <p>PAGE 1 / 2</p>

7.1 보안기록 관리

Record maintenance

(1) 보안 기록 유지 및 사용 언어

Record to be kept and language of record

- 1) 아래 활동은 선박보안기록부 양식을 사용하여 관련 내용을 작성하여 기록하고, 선내에서 3년 동안 문서화하여 관리/보관하여야 한다.

The following activities shall be recorded in the ship security record book and kept in the vessel for three years.

- 2) 기록은 본선의 공용어 작성되어 관리/보관되어야 한다.

Records shall be recorded in working language.

(2) 기록의 유지 관리

Protection of records

- 1) 본 기록에 대한 유지/관리보관 책임은 회사보안책임자 및 선박보안책임자에게 있다.

The responsibility for maintaining security records is responsible for the company security officer and ship security officer.

- 2) 보안기록은 선박보안계획서상의 규정이 이행되고 있음을 당사국 정부의 인가자가 검증할 수 있도록 제공되어야 한다.


Security records should be provided to the person who authorized by the Flag administration or ROS to verify the implementation of the company and ship security plan.

- 3) 본 기록은 승인되지 않은 접근으로부터 보호되어야 한다. 만약 전자 문서형태로 기록이 유지/관리된다면 이는 암호화하여 저장하여야 한다.

This record shall be protected from unauthorized access. If records are maintained in the form of electronic documentation, it should be encrypted and stored.

- 4) 선박보안책임자는 선박보안기록부를 선박보안계획서와 함께 보관하여야 한다.

The ship security officer shall keep the security records with SSP.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 7</p>	<p style="text-align: center;">보안 기록 및 보안정보 관리 RECORD MAINTENANCE AND MANAGEMENT OF SECURITY INFORMATION</p>	<p>REV. NO. : 0</p> <p>PAGE 2 / 2</p>

7.2 보안정보 관리

Management of security information

(1) 보안정보의 수집

Collection of security information

- 1) 보안정보는 다음 출처를 통해 회사 및 선박에서 수집되어야 하며 보안환경 및 정보 보안 관리체계의 변화에 따른 변경사항을 확인하여야 한다.

Security information should be collected from companies and ships through the following sources and should be review to verify the changes in security environment and security information management systems.

- ① 국제 및 국내 유관 기관

International and national agencies

- ② 지역 해상보안 보고센터

Regional maritime security reporting center

- ③ 기국, 산업계, 현지 대리점

Flag state, industry bodies, local agent

- ④ 국방 보안 관련 정보

Military sources

- ⑤ 보안 업계 지침 및 관련 분야 전문가

Guideline of private security company and Specialist consultants

- ⑥ 선급 유관 지침

Guideline of classification society

2) 보안정보 검토


Review of security related information

- ① 선박보안책임자 또는 회사보안책임자는 수집된 보안정보를 검토하고 육상사무실, 직원 및 선박과 관련 정보에 대하여 중요 안건으로 취급하여 검토하여야 한다.

The company security officer and ship security officer shall review the collected security information and these information should be reviewed as an important items for discussion of the office, shore staff and vessel and related information.

- ② 회사는 혁신적인 보안 기술 및 시스템을 적용하였을 경우 관련 기술에 대한 보안정보를 수집하고 이에 대한 검토를 고려하여야 한다.

The companies should collect and review security information about relevant technologies when applying innovative security technologies and systems

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 8</p>	<p style="text-align: center;">보안 평가 및 보안 심사 SECURITY ASSESSMENT AND SECURITY AUDIT</p>	<p>REV. NO. : 0</p> <p>PAGE 1 / 4</p>

8.1 보안 평가 및 검토

Security assessment and security audit

(1) 일반사항

General

- 1) 회사보안책임자는 회사 및 선박의 보안평가를 수행할 책임이 있으며, 필요시, 평가팀을 구성하여 수행할 수 있다. 보안평가에는 현장보안검사가 포함되어야 하며, 보안평가 결과는 문서화하여 관리하여야 한다.

The CSO is responsible for performing the security assessment of the company and the ship, and if necessary, can organize the assessment team. The SSA shall be included the on scene survey and the result of SSA shall be documented.

- 2) 보안평가 보고서는 승인되지 아니한 접근 또는 유출 등으로부터 보호되어야 한다.

The SSA should be protected from unauthorized access and disclosure.

- 3) 회사 보안 계획서 및 보안 관련 위험성 평가는 회사보안책임자에 의해 매년 정기적으로 검토되어야 하며, 필요 시 개정 및 업데이트되어야 한다. 또한, 회사보안책임자는 하기 선박보안평가에 대해 추가 검토해야 한다.

The company security plans and security-related risk assessments should be reviewed periodically by the company security officer annually and if necessary, it should be amended and updated. Additionally, company security officer shall further review the following ship security assessment.


- 4) 선박보안책임자는 새로운 보안위협이나 수리 및 신조 설계 시 항행구역, 선종 및 사이즈, 승무원 인원 수에 따른 보안 강화 요소에 변경사항을 반영될 수 있도록 1 년마다 정기적으로 선박보안평가를 검토하여야 한다.

The CSO shall review the SSA every year so that new security threat or security enhancement factor according to service area, ship's type/size and number of crew members can be reflected as appropriate.

- 5) 선박보안평가를 수행하는 평가자는 아래 항목에 준하는 자격을 갖추고 있어야 한다.

The person evaluating the security of a ship shall be qualified with the following.

- 6) '보안전문지식'에서 언급한 사항에 대한 교육을 이수한 자

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 8</p>	<p style="text-align: center;">보안 평가 및 보안 심사 SECURITY ASSESSMENT AND SECURITY AUDIT</p>	<p>REV. NO. : 0</p> <p>PAGE 2 / 4</p>

A person who has completed training on the matters referred in the subject 'Security Expertise'.

8.2 보안 심사

Security audit

- (1) 회사보안책임자는 회사 및 선박보안평가 시 보안위협 정보를 수집하고, 현장보안검사를 하여 현재의 보호조치, 절차 등을 확인하고 평가하여야 한다.

During the company/ship security assessment, the CSO shall collect information on security threat and perform the on scene security survey to examine and evaluate existing protective measures, procedures, etc.

1) 내부 보안심사

Internal security audit

- 1) 회사보안책임자는 승인된 선박보안계획서에 따라 회사의 보안활동이 적절히 유지 되도록 보장하기 위하여 회사 및 선박에 대하여 1 년 간격으로 정기적으로 내부보안심사를 계획하고 이행하여야 한다.

The CSO shall, in order to ensure that the company's activities are appropriately maintained in accordance with the approved company/ship security plan, carry out internal security audit for the company and ship at the interval of 1 year.

- 2) 새로운 보안위협에 대한 보안상태 점검 등의 목적으로, 특별히 필요하다고 인정되는 경우에는 임시보안심사를 시행할 수 있다.


If an audit other than the periodic audit is deemed to be required to check the effectiveness of existing security system against the new security threat, an additional audit may be carried out.

- 3) 내부보안심사를 수행하는 보안심사자는 심사대상이 되는 활동과 무관하여야 하며, 적절한 자격을 갖추고 있어야 한다.

The security auditor performing the internal security audit should not be connected to the activities being audited and he/she shall be appropriately qualified.

- 4) 내부 보안심사는 ISM 내부심사와 동시에 시행하거나 또는 별도로 시행할 수 있다.

The internal security audit may be carried out in conjunction with the ISM internal audit or

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 8</p>	<p style="text-align: center;">보안 평가 및 보안 심사 SECURITY ASSESSMENT AND SECURITY AUDIT</p>	<p>REV. NO. : 0</p> <p>PAGE 3 / 4</p>

independently.

(2) 외부 보안심사

Company and ship External security audit

- 1) 회사보안책임자는 선박보안증서를 획득하고 유지하기 위한 책임이 있다. 회사 보안 책임자는 선박보안심사계획을 수립하고, 기국 주관청(또는 주관청이 인정한 보안 심사 대행기관)에 심사를 요청하고 필요한 지원을 하여야 한다.

The CSO has the responsibility to obtain and maintain the International Ship Security Certificate (ISSC). The CSO also has the responsibility to establish the ship security certification audit plan and request the Administration or the RSO to carry out the audit and provide the necessary assistance.

(3) 부적합사항의 보고, 조치 및 관리

Reporting, handling and managing non-conformities

1) 회사 내 부적합 사항

Non-conformities in the company

- ① 회사에서 식별된 보안관련 부적합 사항은 발견된 즉시 처리하여야 하고 회사보안책임자에게 보고하여야 한다.

Any security related non-conformities which are identified in the company should be treated immediately and which shall be reported the CSO.


- ② 식별된 부적합사항은 시정조치 기한을 정하여 시정하여야 하고, 그 기록을 유지하여야 한다.

The identified non-conformities should be corrected within a time limit for corrective action and the result of corrective action shall be recorded.

3) 선박 내 부적합 사항

Non-conformities in the ship

- ① 본선에서 식별된 보안관련 부적합 사항은 발견된 즉시 처리하여야 하고 회사보안 책임자에게 보고하여야 한다. 만일 본선에서 처리할 수 없는 부적합 사항은 회사에 요청하여 빠른 시일 내에 처리하여야 한다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 8</p>	<p style="text-align: center;">보안 평가 및 보안 심사 SECURITY ASSESSMENT AND SECURITY AUDIT</p>	<p>REV. NO. : 0</p> <p>PAGE 4 / 4</p>

Any security related non-conformities which are identified on board the ship should be treated immediately and which shall be reported the CSO. The non-conformities that can not be handled on the ship shall be reported to the company in order to handle them as soon as possible.

- ② 본선에서 식별해야 하는 보안관련 부적합 사항은 다음과 같으며 그러한 사항은 본선에서 시정 및 시정조치를 하여야 하고 필요 시 회사보안책임자에게 적절하게 보고하여 해결방안을 모색하여야 한다.

The security related non-conformities to be identified on board the ship are as follows. The corrective actions against such nonconformities shall be taken on board the ship. Non-conformities shall be reported to the CSO immediately to devise appropriate measures.

- a. 선박보안계획서상의 보안조치가 상충하는 경우

When the security measures in the ship security plan is contradictory.

- b. 안전과 보안조치가 상충하는 사항


When ship safety measures and the security measures are contradictory with each other

- c. 항해나 정박 중 외부로부터 침입 또는 침입시도가 발견된 경우

When the security intrusion or security intrusion attempt has been detected during the voyage or while docked.

선박보안책임자는 상기의 보안사건이 발견된 경우 즉시 회사보안책임자 및 당사국 정부에 보고하여야 하고 수신자의 접수 사실여부를 확인하여야 한다.

The SSO shall report the above non-conformities or security incidents to the CSO and the Contracting Governments upon discovery and confirm the receipt of such reporting.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
Ch. 9	<p style="text-align: center;">보안 위반에 대한 징계 DISCIPLINARY ACTION AGAINST SECURITY VIOLATION</p>	<p>REV. NO. : 0</p> <p>PAGE 1 / 3</p>

9.1 회사 보안 위반

Company security violation

- (1) 회사 보안관리와 관련한 위반자는 회사 인사위원회에 회부하여 징계 조치하고, 민/형사상 법률에 의거하여 제소할 수 있다.

The employees who violate the company security management may be referred to the company personnel committee for disciplinary action and may sue them under civil/criminal law.

(2) 징계 절차

Disciplinary action procedure

- 1) 회사보안책임자는 별도의 지침에 정하는 바에 따라, ‘보안 징계위원회’를 설치 운영하여야 한다.

The CSO shall establish and manage the security disciplinary action committee according to the separate guidelines.

2) 구성

Composition

① 위원장

Chairman

: 회사보안책임자

Company Security Officer

② 위원

Member

: 보안관련업무자

Personnel who is responsible for security

3) 소집, 운용


Convocation, Management

: 회사보안책임자가 소집하고 주관하여 운용한다.

The CSO shall convene, supervise and manage the committee.

4) 징계 사항

Disciplinary action

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
<p>Ch. 9</p>	<p style="text-align: center;">보안 위반에 대한 징계 DISCIPLINARY ACTION AGAINST SECURITY VIOLATION</p>	<p>REV. NO. : 0</p> <p>PAGE 2 / 3</p>

① 출입 허가 시스템의 오용

Misuse of access authorization system

② 보안 사건의 관련자

Person who involved in security incidents

③ 보안침해와 관련하여 고의적인 과실이 있는 자

Any person who has intentional negligence in relation to security violation

5) 징계의 종류 및 범위

Type and scope of disciplinary action

① 견책

Reprimand

② 감봉

Pay cut

③ 정직

Suspension

④ 해고

Dismissal

6) 회사보안책임자는 징계심의 및 결과를 기록으로 유지하여야 한다.

CSO shall keep records of deliberation for disciplinary action and the result

9.2 선박 보안 위반

Vessel security violation


(1) 선박 보안 위반

Ship security violation

1) 선박 보안 위반

Ship security violation

- ① 선박 보안관리와 관련한 위반자는 선내인사위원회에 회부하여 징계 조치하고, 민/형 사상 법률에 의거하여 제소할 수 있다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p>
Ch. 9	<p style="text-align: center;">보안 위반에 대한 징계 DISCIPLINARY ACTION AGAINST SECURITY VIOLATION</p>	<p>REV. NO. : 0</p> <p>PAGE 3 / 3</p>

The crew who violate the ship security management may be referred to the ship personnel committee for disciplinary action and may sue them under civil/criminal law.

2) 징계 절차

Procedure

① 선박보안책임자는 별도의 지침에 정하는 바에 따라 ‘보안 징계위원회’를 구성하고,

의결된 사항을 회사에 통보한다.

The SSO shall organize the security disciplinary action committee according to the separate guidelines and notify the result to the company after the disciplinary action is confirmed.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 1 / 13</p>

10.1 적용 Apply

(1) 회사보안책임자 및 선박보안책임자는 회사 및 선박의 보안에 위협을 주는 다음과 같은 비상상황이 발생하였을 경우에는 본 지침에 따라 이행하도록 하여야 한다.

The Company Security Officer and the Ship Security Officer should ensure that the following emergency situations occur that threaten the security of the Company and the ship.

- 1) 좀도둑질
Petty theft
- 2) 기물파손
Vandalism
- 3) 밀항자
Stowaway
- 4) 화물 절도
Cargo theft
- 5) 사이버 위협
Cyber Threat
- 6) 불충분한 항만 보안
Inadequate port security
- 7) 무기 또는 마약 밀수, 인신매매
Smuggling of arms or drugs, trafficking of people
- 8) 해적행위 및 무장공격
Piracy and armed attacks
- 9) 파괴행위 및 방화
Sabotage and arson
- 10) 선박에 대한 폭탄 위협
Bomb threats against ships
- 11) 테러 및 그 테러의 후속영향
Terrorism and its subsequent effects
- 12) 선박 및 선원의 대피
Evacuation of ships and crew
- 13) 입거 중 또는 장기간 수리시의 보안절차
Security procedures during docking or long- term repair

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 2 / 13</p>

- (2) 만일 회사보안계획서 또는 선박보안계획서에서 식별되지 아니한 비상상황이 발생한 경우, 회사 보안 책임자 및 선박보안책임자는 선박과 선원 및 여객(해당되는 경우)의 안전을 고려하여 필요하다고 판단되는 조치를 하여야 한다.

In the event of an emergency not identified in the company security plan or the ship security plan, the company security officer and the master (ship security officer) should take the necessary measures in consideration of the safety of the ship, crew and passenger.

10.2 해적행위 및 무장공격 Piracy and armed attacks

- (1) 해적행위 대비한 일반적인 주의 사항

General cautions against piracy

- 1) 대부분의 해적공격은 정박 중에는 항만에서, 해상에서는 대부분 선박이 육지를 가깝게 항해 할 경우 및 조종성능에 제약을 받는 협수로를 통과 시에 공격을 받기 쉬우므로, 이러한 경우 특히 주의하여야 하며, 선박보안책임자는 다음과 같은 지침을 이행하여야 한다.

Particular care should be taken in this case, as most pirate attacks are likely to be attacked in harbors during berths, when most ships sail close to land, and when they pass through barges restricted by maneuvering capabilities. Master (Ship Security Officer) should implement the following guidelines.

- ① 해적 또는 무장 강도의 공격 위험 및 대응 계획을 승무원에게 사전 교육
Pre-train the crews to plan attacks and counter-attack of pirates or armed robbers
- ② 선교, 기관실, 타기실, 사관 침실, 승무원 거주구역의 봉쇄
Blocking bridge, engine room, steering gear room, cabin, crew accommodation
- ③ 가능하면 위험이 높은 지역과 병목지역의 항해를 회피
Avoid high-risk areas and bottlenecks areas if possible
- ④ 만약 항구에서 해적에 대한 높은 위험이 존재하고, 항구가 연이은 선박의 취약성의 최소화에 대한 즉각적인 가능성이 없을 경우 선박의 입항에 대한 연기를 고려

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 3 / 13</p>

If there is a high risk of piracy in the port, consider the postponement of the vessel's entry into port if there is no immediate possibility about minimizing of risk

- 2) 해적은 선박이 소지한 고가의 물품 또는 선박 자체를 탈취할 수 있다. 어떤 값비싼 물건 또는 심지어 선박 그 자체를 훔칠 수 있다. 따라서 대량의 화폐를 소지하고 항해하는 것은 가능한 기피해야 하며 불가피한 경우 그러한 사실이 외부에 알려지지 않도록 하여야 한다.

Pirates may seize the expensive goods owned by the ship or the ship itself and they can steal any expensive things or even ship itself. Therefore, it should be avoided sailing with a large amount of money, and if it is unavoidable, such fact should not be known to the outside.

- 3) 해적은 조난선을 가장하여 선박에 접근하는 위장술을 사용할 수 있다. 만약, 선박보안 책임자가 조난자를 선박에 승선시키도록 결정하였다면, 한번에 한명씩 옮겨 타도록 하며, 각 승선자의 신분 탐색에 대하여 각별한 주의를 기울여야 한다.

Pirates can use camouflage to approach the ship by pretending to be a distress. If the master decides to permit embarkation on the ship, he should move one person at a time and pay special attention to the identification of the identity of each boarder.

(2) 항만에서의 해적보안조치

Piracy security measures in the port

선박보안책임자는 항만에서 아래의 지침이 준수되도록 하여야 한다.

The Ship Security Officer should ensure that the following guidelines are adhered to in the port.

- 1) 가급적 통제된 단일통로 또는 선측의 승강계단을 이용하게 하여 접근통로를 최소화
Minimize the access path by using a single controlled passage or side elevator stairs

- 2) 비상 사다리를 해면에서 일정 높이로 올려놓는 상태를 유지하고 도선사용 사다리는 사용 후 반드시 격납

Keep the emergency ladder up to a certain height from the sea surface and pilot ladder must be stored after use

- 3) 만약 위협 발생 가능성이 높으면 접근 출입지점에 보안감시자 배정

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 4 / 13</p>

If the threat is likely to occur, assign a security supervisor to the access point

- 4) 근접한 위치에 있는 소형선을 지속적인 감시대상으로 유지

Keep small ships adjacent to our ship under constant surveillance

(3) 항해 중 보안조치

Security measures during sailing

- 1) 선박보안책임자는 위험이 높은 지역을 항해할 경우 아래의 지침이 준수되도록 하여야 한다.

The master (Ship Security Officer) should ensure that the following guidelines are adhered to when sailing in a high-risk areas.

- ① 선박 근처를 모니터링할 경우, 본선과 같은 속도 또는 본선과 평행하게 항해중인 소형선에 대하여 추가 감시 실시
When monitoring near the ship, small ships sailing at the same speed with our ship or parallel to our course line need further monitoring
- ② 항해지역의 관계 당국 또는 적절한 육상조직과의 무선 통신을 유지
Maintain wireless communications with the relevant authorities of the sailing area or appropriate land-based organizations

- 2) 만약, 항해 중 의심스러운 선박이 위협적인 태도로 접근한다면, 아래의 지침에 따라 행동한다.

If suspicious vessels approach the vessel in a threatening manner, act in accordance with the following guidelines


- ① 필요 시 레이더 맹목구간에 견시자를 배치한다.
If necessary, position the watcher in the radar blind section
- ② 선속을 높이며 가능시 침로를 변경한다.
Increase the speed and change the course if possible
- ③ 선박이 본선에 계선하려 접근하는 것을 허용하지 않는다.

Do not allow the ship to approach our ship for mooring

- a. 위협선의 무선, 불빛, 또는 큰소리로 부르는 반응을 보이지 않는다

Do not respond to the action of threatening ships call our ship wirelessly or use light, or loud shouting.

- ④ 위협선을 상세하게 기록한다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 5 / 13</p>

Record the threatening ship in detail.

a. 가능하면 비디오 또는 사진을 찍는다

If possible, take a video or photo

⑤ 야간에 노천갑판 조명을 끈다.

Turn off outdoor's deck light at night

⑥ 접근하는 선박에게 탐조등을 비춘다.

Use a search light on the approaching ship

⑦ 노천갑판의 사람을 철수시킨다.

Evacuate the people on the outdoor's deck

(4) 선박이 납치된 경우

When a ship is hijacked

만약에 선박이 불가피하게 납치된 경우에는, 납치된 후 사고 없이, 장시간이 지날수록 더 유리하다는 점을 참고하여 다음과 같이 행동하도록 한다.

If a ship is inevitably hijacked, it should be noted that it is more advantageous the longer the time goes without incident and act as follows

1) 침착함을 유지하고, 생명에 위협을 가하는 상황이 아니라고 판단되면, 무장한 해적에게 저항하지 않는다.

If you think it is not a life threatening situation, stay calm and do not resist armed pirates

2) 해상 연습에 따라 선박과 사람들의 안전을 확보

Ensure the safety of ships and people according to drills and training

3) 가능 시 조난 신호를 송신

Send distress signal if possible

4) 납치자와 우호적인 관계가 유지되도록 노력

Efforts to maintain friendly relations with hijackers

5) 납치자의 인원, 조직 규모를 파악

Identify the number of hijackers and size of organization

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 6 / 13</p>

- 6) 선박보안책임자와 승무원은 관계당국의 지시가 없다면 납치자와 협상을 시도해서는 안된다.

Master and crew should not attempt to negotiate with the hijackers unless directed by the authorities concerned

10.3 선박 사이버 보안 위협 Shipboard cyber threat

(1) 사이버 보안 위협의 유형

Type of cyber threat

선박 내 발생 가능한 사이버 보안 위협 유형은 일반적으로 아래와 같이 구분할 수 있고 기술의 발전에 따라 계속 진화될 수 있음을 고려하여야 한다.

The type of shipboard cyber threats are classified as follows and should be considered that it is evolving by technology development.

- 1) 비정상적으로 많은 네트워크 트래픽의 감지

Excessive network traffic.

- 2) 시스템 장애 또는 예기치 못한 종료

System malfunction or unexpected close of system

- 3) 바이러스 등 악성코드, 랜섬웨어 감염 또는 IDS 알람

Infection of malware and ransomware or Indication of IDS(Intrusion Detection System) Alarm

- 4) 비인가자에 의한 접근

Access by un-authorized person

(2) 사이버 보안 위협에 대한 대응 절차

Response procedure

선박 내 사이버 보안 위협을 인지하였을 시 다음과 같이 대응한다.

Recognized cyber threat shall be treated as follows,

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 7 / 13</p>

- 1) 사이버 보안 위협을 인지한 경우 위협 대응책을 마련하기 위하여 신속한 원인 식별이 이루어져야 한다.

Identify causes of cyber threats are required for prepare measures.

- 2) 선박보안책임자는 발생한 사이버 보안 위협의 원인을 파악하고 피해를 최소화하기 위한 대응조치를 취하여야 한다.

Ship cyber security officer should take measures to mitigate losses.

- 3) 선박보안책임자는 관련 위협이 회사 및 선박의 운영에 중대한 손실을 발생시킬 것으로 판단될 경우 회사보안책임자 및 적합한 관계당국에 관련사실을 통보하고 해결방안을 강구하여야 한다.

Ship cyber security office should be take measures after forwarded cyber incident report to company cyber security officer and concerned authority in case of significant harms to expected.

(3) 사이버 보안 위협에 대한 사후 관리

Management of cyber threat incident

선박 내 사이버 보안 위협 종료 시 관련 정보는 회사 및 선박 관계자에게 분석 및 공유되어야 한다.

Shipboard cyber threats shall be analyzed and distributed to concerned department after close incident.

- 1) 사이버 보안 위협이 종료 되었을 경우 선박보안책임자는 발생 원인 및 조치결과에 대하여 관련 조직간에 공유하도록 한다.

Ship cyber security officer shall be distributed causes and result of cyber threat to concerned department after close incident.

- 2) 선박보안책임자는 분석된 결과에 따라 필요시 정책, 절차, 조직 등 사이버 사고 위협 대응 체계에 대한 변경을 수행하여야 한다.

Ship cyber security officer shall be modified cyber security response plan in accordance with analyzed cyber threat incident.

- 3) 회사는 매년 정기적으로 사이버 보안 위협 및 사고 관련 대응에서 얻은 교훈을 바탕으로 대응 계획을 개선하여 업데이트하여야 한다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 8 / 13</p>

Cyber security response plan shall be revised annually in accordance with analysis result of cyber threat incident.

- 4) 회사는 사이버 사고 대응계획에 포함된 내용과 시나리오를 바탕으로 주기적인 모의훈련을 실시하고 이에 대한 이력을 관리하여야 한다.

Cyber security drill shall be conducted regulatory and maintained drill record in accordance with cyber security response plan.

(4) 사이버 보안 위협에 대한 복구관리

Recovery plan against cyber threat

선박 내 사이버 보안 위협 후 발생한 피해에 대하여 적절한 복구 체계를 구축하고 관리하여야 한다.

Recovery plan shall be established and managed to recover cyber threat incident.

- 1) 선박보안책임자는 사이버 보안 위협의 유형을 식별하고 이에 따른 업무 영향 분석을 수행하여 피해규모를 예상할 수 있는 체계를 구축하여야 한다.

Ship cyber security officer shall be established damage prediction system by identify type of cyber threat and risk assessment.

- 2) 선박보안책임자는 IT 및 OT 시스템 복구 목표 시간, 복구 시점을 정의하고 적절한 복구 전략 및 대책을 수립하여야 한다.


Ship cyber security office shall be established recovery plan by define target time of IT and OT system

- 3) 선박보안책임자는 IT 및 OT 시스템 복구 전략 및 대책에 따른 복구가 실제로 가능한 지를 수행하는 시험 계획을 수립하여야 한다.

Ship cyber security officer shall be established test plan for IT and OT system recovery plan.

- 4) 선박보안책임자는 시험결과에 따라 IT 및 OT 환경변화, 법규 등에 따른 변화를 반영하여 복구 전략 및 대책을 보완하여야 한다.

Ship cyber security officer shall be supplemented recovery plan in accordance with test result including modification of concerned regulation and IT and OT system

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 9 / 13</p>

10.4 선박에 대한 폭탄 위협 Bomb threat to ship

(1) 폭탄 위협에 대한 대응

Response to bomb threats

선박에 폭탄이 설치되었다는 위협이 있을 시 다음과 같이 대응한다.

If there is a threat that a bomb has been installed on the ship, it should be dealt with as follows.

- 1) 폭탄 위협을 받은 사람은 선박보안책임자 또는 당직 사관에게 즉시 연락하여야 한다.

Any person who is threatened by the bomb must contact the master (Ship Security Officer) or the duty officer immediately.

- 2) 선박보안책임자는 회사보안책임자 및 적합한 관계 당국에 관련 사실을 통보해야 한다.

The Ship Security Officer should notify the company security officer and appropriate authorities concerned of the relevant facts.

(2) 전화를 이용한 폭탄 위협에 대한 대응 절차

Response procedures for phone-based bomb threat

전화 연락을 통해 선박에 폭발물이 설치되어 있다는 위협을 받았을 경우 다음과 같이 대응한다.

If you are threatened with an explosive on board by telephone, you may:

- 1) 가능 시, 폭발물 설치에 대한 위협 전화의 음성을 한명 이상이 듣도록 한다.

If possible, make sure that one or more people are listening to the threatening telephone call.

- 2) 전화를 건 사람에게 통화내용을 반복하도록 요청하고, 모든 통화내용을 기록 한다.

Ask the person who called the phone to repeat the conversation and record all conversations.

- 3) 반복되는 단어 또는 용어에 주의한다.

Pay attention to repeated words or terms

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 10 / 13</p>

- 4) 전화를 건 사람의 신분이나 장소를 알아내는데 도움을 줄 수 있는 주위 소음 등을 구별한다.

Identify ambient noise that can help identify the identity or location of the person making the call.

- 5) 가능하면 통화를 녹음한다.

Record the call, if possible.

- 6) 선박보안책임자에게 즉시 알린다. 가능하면 폭탄의 위치와 위협한 폭발시각을 함께 전달한다.

Notify the Ship Security Officer immediately. If possible, combine the location of the bomb and the time of the threatening explosion.

(3) 폭탄 탐색 지침

Bomb search instructions

- 1) 폭발물 탐색은 폭발물 수색 경험이 많은 사람에 의해 수행되는 것이 바람직하다. 폭발물 탐색을 수행하는 경우 새로운 사항이나 통상적이지 않은 것에 주의하여야 한다. 의심스러운 징후 포착 시 즉시 선박보안책임자에게 보고하여야 한다.

Explosive exploration is preferably performed by a person with extensive explosive search experience. When exploring explosives, care should be taken not to be new or unusual. The ship security officer should immediately report any suspicious signs.

- 2) 탐색요령은 다음과 같다.

The exploration tips are as follows.

- ① 각 선박의 특정 수색 계획에 바탕을 둔 수색팀이 편성되어야 한다.

A search team based on each vessel's specific search plan should be organized.

- ② 수색을 하는 사람들은 수색지역에 익숙하여 그 지역에서 새로운 또는 이상한 항목들을 식별할 수 있어야 한다.

Searchers should be familiar with the search area and be able to identify new or strange items in the area.

- ③ 수색이 끝난 장소는 적절한 표시로 식별되어야 한다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 11 / 13</p>

The place where the search is completed should be identified with an appropriate mark

- ④ 만약 폭탄을 발견하였다면 수색자는 또 다른 폭탄의 존재를 파악하기 위하여 수색을 계속 하여야 한다.

If a bomb is found, the searcher must continue to search for another bomb.

- 3) 만일, 의심스러운 물건이 발견된 경우 다음과 같이 행동한다.

If a suspicious object is found, act as follows.

- ① 절대 만지거나, 뚜껑을 열거나, 운반하지 아니한다.

Never touch it, open the lid, or carry it.

- ② 폭발할 경우를 대비하여, 매트리스나, 모래주머니 등을 이용하여 폭발효과를 최소화하도록 한다.

Be prepared for explosion, use mattress or sand bag to minimize explosion effect

- ③ 선박이 항만에 있는 경우에는 항만시설보안책임자에게 연락하여 폭발물처리 전문가가 방선하여 처리할 수 있도록 조치한다.

If the ship is in the port, contact the Port Facility Security Officer and arrange for the explosive treatment specialist to dispose of it.

- ④ 항해 중에 발생한 경우에는, 회사보안책임자에게 연락하여 회사의 지시에 따르도록 한다.

If it occurs during the voyage, contact the company security officer and follow the company's instructions

10.5 선박의 대피 Evacuation of a vessel

- (1) 선박보안책임자는 다음과 같은 경우 선박의 안전을 위하여 선박을 대피하도록 하여야 한다.

The master should ensure that the ship is evacuated for the safety of the ship when;

- 1) 주관청 및 당사국의 지침이 있는 경우

If the Administration and the state party are instructed

- 2) 보안 위협 또는 보안 위반 발생시 선박보안책임자의 전문적인 판단으로 선박의 대피가 필요하다고 판단되는 경우

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 12 / 13</p>

In the event of a security threat or security violation, the ship's evacuation is deemed necessary by the master's professional judgment

(2) 대피 절차

Evacuation procedure

- 1) 선박의 대피가 필요하다고 판단되는 경우, 즉시 회사보안 책임자에게 알린다.

If it is deemed necessary to evacuate a ship, immediately notify the company security officer.

- 2) 승무원의 인원 점검 및 선박의 대피를 위한 Stand-by 를 발령한다.

Stand-by should be issued to do roll-call and to evacuate the ship.

- 3) 선박보안책임자는 당사국 정부 및 회사의 권고를 참조하여 피난지를 결정하여 이동한다.

The master decides to evacuate by referring to the recommendation of the government of the Party and the company.

- 4) 선박보안책임자는 모든 인원의 대피가 완료된 후 당사국정부 및 회사에 보고한다.

The master should report to the government of Parties and the Company after the evacuation of all personnel has been completed.

- 5) 선박보안책임자는 당사국정부 및 회사보안책임자와 향후 보안 관련 조치 사항을 지속적으로 관리/통제한다.

The master should continue to manage and control future security measures with the Government of the Party and the company security officer.

10.6 선원의 대피 Evacuation of a crew

- (1) 선박보안책임자는 아래 경우에 해당시 선원의 안전을 위하여 선원이 대피하도록 하여야 한다.

The master should cause the crew to evacuate for the safety of the crew in case of the following cases.

- 1) 주관청 및 당사국의 지침이 있는 경우

If there is instruction from the Administration and the Party

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>Ch. 10</p>	<p style="text-align: center;">비상 대응 지침 EMERGENCY RESPONSE GUIDELINE</p>	<p>PAGE 13 / 13</p>

- 2) 보안 위협 또는 보안 위반 발생 시 선박보안책임자의 전문적인 판단으로 선원의 대피가 필요하다고 판단되는 경우. 선박 항해 현황에 따라 대피 장소는 다음과 같다

In the event of a security threat or security violation, if it is deemed necessary to evacuate a crew in the professional judgment of the Master, the place of evacuation is as follows

- ① 항해 중 Sailing
: 구명정 또는 비상 대피처 Lifeboat or Citadel
- ② 접안 중 Berthing
: 접안 측 현문 사다리 Shore-side gang-way

10.7 입거 중 또는 장기간 수리 시 보안 절차 Security procedure dry docking or long-term repairs

- (1) 선박보안책임자는 입거 중 또는 장기간 수리 시 선박보안을 위하여 다음과 같은 사항이 유지되도록 하여야 한다.

The master should ensure that the following items are maintained for ship security during dry docking or long-term repairs.

- 1) 선박보안책임자의 보안 브리핑 교육 시행
Master's security briefing education enforcement
- 2) 최소 당직 인원에 대한 보안조직 구성
Organization of security organization for minimum number of personnel

- (2) 입거 또는 장기 수리가 종료된 경우, 선박의 보안 취약성이 발생하지 않도록 다음과 같은 사항이 수행되어야 한다.

In the event that the dry docking or long-term repair is terminated, the following should be carried out in order to avoid the occurrence of security vulnerabilities of the ship.

- 1) 선박의 보안 관리 상태 평가
Evaluation of security management status of ship
- 2) 보안 위반 또는 부적합 사항 발생시 조치
Action in case of security violation or non- conformity

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.1</p>	<p style="text-align: center;">사이버 보안 지침 CYBER SECURITY INSTRUCTION</p>	<p>PAGE 1 / 2</p>

1.1 일반 General

(1) 목적

Purpose

① 본 절차의 목적은 회사 및 선박의 사이버 보안 위협 요소를 식별 및 차단하여 회사 및 선박의 전자 자료 및 정보를 보호함에 있다.

The purpose of this procedure is to protect company and ship's electronic data and information by identifying and blocking company and ship's cyber security threats.

② 사이버 안전 및 사이버 보안 위험 관리에 대한 필수 지침을 제공하는 것을 목표로한다.

And also aims to provide essential guidelines for cyber safety and cyber security risk management.

(2) 책임 및 권한

Responsibility and authority

1) 선장

Master

① 하드 웨어/ 소프트웨어/전산관련도서를 종합적으로 관리할 책임과 의무가 있으며 회사의 지시, 권고 사항 이행

Master has the responsibility and obligation to manage systematically the hardware, software, publications of computation system, and perform the Company's instructions and recommendations

② 시스템 오류 발생시 전산팀 및 선박관리팀에 시스템 점검 요청

In case of having system errors the System check requisition should be dispatched to IT and MM

③ 통신용 컴퓨터 관리

Management of communication computer

④ 중요 시스템의 패스워드 및 권한 관리 총 책임자

Overall responsible for management of important system onboard.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
APP.1	<p style="text-align: center;">사이버 보안 지침 CYBER SECURITY INSTRUCTION</p>	<p>PAGE 2 / 2</p>

2) 일등 항해사

Chief officer

① 화물 및 갑판 기기 관련 하드웨어 및 소프트웨어 관리

Manage the hardware and software related with cargo and deck machinery.

: 상태 점검, 펌웨어 최신화, 자료 백업 및 복구를 포함한다.

Include, condition check, update of firmware, data back-up and recovery.

② 공용 컴퓨터 및 네트워크 관리

Manage the common computer and network

3) 이항사

2nd officer

① 항해 통신 장비 관련 하드웨어 및 소프트웨어 관리

Manage the hardware and software related with navigation/communication equipment.

: 상태 점검, 펌웨어 최신화, 자료 백업 및 복구를 포함한다.

Include, condition check, update of firmware, data back-up and recovery.

4) 기관장

Chief Engineer

① 기관실 장비 관련 하드웨어 및 소프트웨어 관리

Manage the hardware and software related with machinery in engine room.

: 상태 점검, 펌웨어 최신화, 자료 백업 및 복구를 포함한다.

Include, condition check, update of firmware, data back-up and recovery.

② PMS 프로그램 관리

Management of PMS program

	보안 절차서 SECURITY PROCEDURE	DOC NO. : PR - 19 REV. NO. : 0
APP.2	위험 요소 식별 IDENTIFY THREATS	PAGE 1 / 7

2.1 제기 된 위협과 회사 및 그들이 운영하는 선박에 대한 잠재적 인 결과

The threat posed and the potential consequences for companies and the ships they operate:

그룹 Group	동기 Motivation	목적 Objective
행동주의자 Activists * 불만을 가진 직원을 모두 포함한다. Including disgruntled employee	<ul style="list-style-type: none"> • 명예 훼손 Reputational damage • 서비스 운영 중단 Disruption of operations 	<ul style="list-style-type: none"> • 데이터 파괴 위협 Destruction of data • 중요 데이터의 게시 Publication of sensitive data • 언론의 관심 Media attention • 서비스 또는 시스템에 대한 액세스 거부 Denial of access to the service or system targeted
범죄자 Criminals	<ul style="list-style-type: none"> • 재정적 이득 Financial gain • 상업 스파이 Commercial espionage • 산업 스파이 Industrial espionage 	<ul style="list-style-type: none"> • 도난당한 데이터 판매 Selling stolen data • 도난당한 데이터 랜싱 Ransoming stolen data • 랜싱 시스템의 조작성 Ransoming system operability • 화물의 사기성 운송 배치 Arranging fraudulent transportation of cargo • 보다 정교한 범죄, 정확한 화물 위치, 선박 운송 및 취급 계획 해제 등을 위한 정보 수집 Gathering intelligence for more sophisticated crime, exact cargo location, off vessel transportation and handling plans etc
기회주의자 Opportunists	<ul style="list-style-type: none"> • 도전 The challenge 	<ul style="list-style-type: none"> • 사이버 보안 방어 수단을 통한 접근 Getting through cyber security defences • 재무적인 이익 Financial gain
정부단체 및 테러 리스트 States organisations and Terrorists	<ul style="list-style-type: none"> • 정책적 이익 Political gain • 스파이 활동 Espionage 	<ul style="list-style-type: none"> • 지식 확보 Gaining knowledge • 경제 및 주요 국가 인프라에 대한 혼란 Disruption to economies and critical national infrastructure

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.2</p>	<p style="text-align: center;">위험 요소 식별 IDENTIFY THREATS</p>	<p>PAGE 2 / 7</p>

- 1) 위의 그룹은 활동적이며 선박의 안전과 보안을 위협하는 기술과 자원 및 회사의 사업 수행 능력을 갖추고 있다.

The above groups are active and have the skills and resources to threaten the safety and security of ships, and a company's ability to conduct its business.

- 2) 또한 회사 내부의 개인이나 선박에 탑승 한 사람들이 사이버 시스템과 데이터를 무의식적으로 손상시킬 가능성이 항상 있다.

In addition, there is always the potential for individuals inside a company or onboard a ship to compromise cyber systems and data unknowingly.

2.2 사이버 공격 유형 Types of cyber attack

- 1) 회사 또는 선박의 시스템 및 데이터가 많은 잠재적 목표 중 하나 인 비 표적 공격.

Untargeted attacks, where a company or a ship's systems and data are one of many potential targets; or

① 악성 코드

Malware

- a. 악의적인 소프트웨어로 소유자의 지식없이 컴퓨터에 액세스하거나 컴퓨터를 손상시킴. 트로이 목마, 랜섬 웨어, 스파이 웨어, 바이러스 및 웜을 비롯한 다양한 유형의 악성 코드가 있다.

Malicious software which is designed to access or damage a computer without the knowledge of the owner. There are various types of malware including trojans, ransomware, spyware, viruses, and worms.

- b. 랜섬웨어는 값이 지불 될 때까지 시스템의 데이터를 암호화 함.

Ransomware encrypts data on systems until a ransom has been paid.

- c. 악성 코드는 구식 / 패치되지 않은 업무 소프트웨어의 알려진 결함 및 문제점도 악용 할 수 있다.

Malware may also exploit known deficiencies and problems in outdated/unpatched business software.

② 소셜 엔지니어링

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.2</p>	<p style="text-align: center;">위험 요소 식별 IDENTIFY THREATS</p>	<p>PAGE 3 / 7</p>

Social engineering

: 사회적 매체를 통한 상호 작용을 통해 내부적으로 보안을 침해하는 비기술적 기법

Non-technical techniques that interfere with security internally through interactions through social media.

③ 피싱

Phishing

a. 민감한 또는 기밀 정보의 특정 부분을 요구하는 다수의 잠재적 인 대상에게 전자 메일을 발송

Sending emails to a large number of potential targets asking for particular pieces of sensitive or confidential information.

b. 이러한 전자 메일은 전자 메일에 포함 된 하이퍼 링크를 사용하여 가짜 웹 사이트를 방문하도록 요청할 수도 있음

Such an email may also request that a person visits a fake website using a hyperlink included in the email.

④ 워터 홀링

Water holing

: 가짜 웹사이트를 개설하여 방문객을 착취하는 유형.

Establishing a fake website or compromising a genuine website to exploit visitors.

⑤ 스캐닝

Scanning

: 인터넷의 상당부분을 무작위로 추출한다.

Attacking large portions of the internet at random.

2) 대상 공격, 회사 또는 선박의 시스템과 데이터가 의도 된 대상.

Targetted attacks, where a company or a ship's systems and data are the intended target.

① 무작위 대입

Brute force

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.2</p>	<p style="text-align: center;">위험 요소 식별 IDENTIFY THREATS</p>	<p>PAGE 4 / 7</p>

- a. 궁극적으로 정확하게 추측 할 수 있도록 많은 암호를 사용하여 공격.

An attack trying many passwords with the hope of eventually guessing correctly.

- b. 공격자는 올바른 암호가 발견 될 때까지 가능한 모든 암호를 체계적으로 검사.

The attacker systematically checks all possible passwords until the correct one is found.

② 서비스 거부 (DoS)

Denial of service (DoS)

- a. 합법적이고 권한이 부여 된 사용자가 일반적으로 네트워크에 데이터를 넘겨 정보에 액세스하는 것을 막음.

prevents legitimate and authorized users from accessing information, usually by flooding a network with data.

- b. 분산 서비스 거부 (DDoS) 공격은 여러 컴퓨터 및 / 또는 서버를 제어하여 DoS 공격을 구현.

A distributed denial of service (DDoS) attack takes control of multiple computers and/or servers to implement a DoS attack.

③ 스피어 피싱.

Spear-phishing.

- : 피싱과 유사하지만 개인 전자 메일을 대상으로 악성 소프트웨어 또는 악성 소프트웨어를 자동으로 다운로드 하는 링크가 포함되어있는 경우가 많음.

Similar to phishing but the individuals are targeted with personal emails, often containing malicious software or links that automatically download malicious software.

④ 공급망 전복

Subverting the supply chain.

- : 회사 혹은 선박에 전달되는 장비 또는 소프트웨어를 침해하여 회사 나 선박을 공격하는 행위

Attacking a company or ship by compromising equipment or software being delivered to the company or ship.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.2</p>	<p style="text-align: center;">위험 요소 식별 IDENTIFY THREATS</p>	<p>PAGE 5 / 7</p>

2.3 사이버 공격 단계 Stages of a cyber attack

사이버 공격을 준비하는 데 소요되는 시간은 공격자의 동기와 목표에 의해 결정되며, 배에 탑재된 기술을 포함하여 회사가 구현한 기술적 및 절차적 사이버 보안 통제의 회복이다. 공격의 네 가지 단계는 다음과 같다.

The length of time taken to prepare a cyber attack can be determined by the motivations and objectives of the attacker, and the resilience of technical and procedural cyber security controls implemented by the company, including those onboard its ships. The four stages of an attack are:

1) 조사/정찰

Survey/reconnaissance

① 오픈 소스는 사이버 공격을 준비하기 위해 사용될 수 있는 회사, 선박 또는 선원에 대한 정보를 얻기 위해 사용되었다.

Open/public sources used to gain information about a company, ship or seafarer, which can be used to prepare for a cyber attack.

② 웹 사이트, 문서, 문서 및 간행물의 소셜 미디어, 기술 포럼 및 숨겨진 속성은 기술적, 절차적, 물리적 취약성을 식별하는 데 사용될 수 있다.

Social media, technical forums and hidden properties in websites, documents and publications may be used to identify technical, procedural and physical vulnerabilities.

③ 오픈 소스를 사용하는 소스의 사용은 회사 또는 선박에서 유입되는 실제 데이터를 모니터링(분석 - 스니핑) 하여 보완할 수 있다.

The use of open/public sources may be complemented by monitoring (analyzing – sniffing) the actual data flowing into and from a company or a ship.

2) 전달

Delivery

① 공격자는 회사와 시스템 및 데이터에 액세스 하려고 시도할 수 있다.

Attackers may attempt to access company and ship systems and data.

② 이것은 회사 내에서 또는 인터넷과의 연결을 통해 원격으로 수행할 수 있다.

This may be done from either within the company or ship or remotely through connectivity with the internet.

③ 액세스를 얻는 데 사용되는 방법의 예

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.2</p>	<p style="text-align: center;">위험 요소 식별 IDENTIFY THREATS</p>	<p>PAGE 6 / 7</p>

Examples of methods used to obtain access include:

- a. 화물 또는 위탁 추적 시스템을 포함하는 회사 온라인 서비스
company online services, including cargo or consignment tracking systems
- b. 악의적 인 파일 또는 악성 웹 사이트 링크가 포함 된 전자 메일을 직원에게 보냄
sending emails containing malicious files or links to malicious websites to personnel
- c. 예를 들어 선박 시스템에 대한 소프트웨어 업데이트의 일부로 감염된 이동식 미디어 제공
providing infected removable media, for example as part of a software update to an onboard system
- d. 직원이 사용자 계정 정보를 공개하도록 권장하는 허위 또는 오도 된 웹 사이트를 생성하는 행위.
creating false or misleading websites which encourage the disclosure of user account information by personnel.

3) 침해

Breach

① 공격자가 회사 또는 선박 시스템을 침입할 수 있는 범위는 공격자가 발견한 취약점의 중요도와 공격을 전달하기 위해 선택한 방법에 달려 있다.

The extent to which an attacker can breach a company or ship system will depend on the significance of the vulnerability found by an attacker and the method chosen to deliver an attack.

② 장비의 상태에 대한 명백한 변화가 발생하지 않을 수 있다는 점에 유의해야 한다.

It should be noted that a breach might not result in any obvious changes to the status of the equipment

③ 침입의 목적에 따라 침입자는 다음을 수행 할 수 있다.

Depending on the significance of the breach, an attacker may be able to:

- a. 시스템 작동에 영향을 주는 변경, 예를 들면 항해 장비가 사용하는 정보를 방해하거나 조작하는 것
make changes that affect the system's operation, for example interrupt or manipulate information used by navigation equipment
- b. 화물 적하 목록 및 / 또는 승무원 및 승객 명부와 같이 상업적으로 민감한 데이터에 접근

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.2</p>	<p style="text-align: center;">위험 요소 식별 IDENTIFY THREATS</p>	<p>PAGE 7 / 7</p>

Gain access to commercially sensitive data such as cargo manifests and/or crew and passenger lists;

- c. 기계 관리 시스템과 같은 시스템을 완벽하게 제어

Achieve full control of a system, for example a machinery management system.

4) 영향

Affect

① 침입자의 동기와 목적은 회사 또는 선박 시스템 및 데이터에 어떤 영향을 주는지 결정한다. 공격자는 시스템을 탐색하고 액세스를 확장하거나 시스템으로 돌아갈 수 있는지 확인하여 다음 작업을 수행 할 수 있다.

The motivation and objectives of the attacker will determine what affect they have on the company or ship system and data. An attacker may explore systems, expand access and/or ensure that they are able to return to the system in order to:

- a. 접근 할 수 없는 화물, 승무원 및 승객에 대한 상업적으로 민감하거나 기밀인 데이터에 접근.

Access commercially sensitive or confidential data about cargo, crew and passengers to which they would otherwise not have access;

- b. 승무원 또는 여객 명부 또는 화물 적하 목록을 조작. 이것은 불법 화물의 사기 수송을 허용하기 위해 사용될 수 있다.

Manipulate crew or passenger lists, or cargo manifests. This may be used to allow the fraudulent transport of illegal cargo; and

- c. 비즈니스 시스템에서 서비스 거부가 발생합니다.

cause complete denial of service on business systems

- d. 다른 유형의 범죄 (예 : 불법 복제, 절도 및 사기) 사용

enable other forms of crime for example piracy, theft and fraud

- e. 중요한 사전 도착 정보를 삭제하거나 회사 시스템을 과부하 하는 등 회사 및 선박 시스템의 정상 작동을 방해.

Disrupt normal operation of the company and ship systems, for example by deleting critical pre-arrival information or overloading company systems.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
APP.3	<p style="text-align: center;">사이버 보안 관련 시스템 SYSTEM RELATED WITH CYBER SECURITY</p>	<p>PAGE 1 / 7</p>

3.1 화물 관리 시스템

Cargo management systems:

1) 특징 및 주요 취약 점

Characteristics and vulnerable

: 위험 화물을 포함한 화물의 관리 및 제어에 사용되는 디지털 시스템은 여러 가지 시스템과 연계 될 수 있다.

Digital systems used for the management and control of cargo, including hazardous cargo, may interface with a variety of systems ashore.

2) 화물 관리 시스템은 다음을 포함한다.

Cargo management systems include;

① 화물 통제실 및 장비

Cargo Control Room (CCR) and its equipment

② 액위/온도/압력 감시 시스템

Level/Temp./Press. monitoring system

③ 원격 밸브 제어 시스템

valve remote control system

④ 평형수 시스템

ballast water systems

⑤ 화물 운용 기기 제어 시스템

Cargo operation equipment control system

3.2 선교 시스템

Bridge systems

1) 특징 및 주요 취약 점

Characteristics and vulnerable

① 다른 네트워크에 연결되지 않은 선교 시스템은 이동식 미디어가 다른 시스템에서 제어되거나 제어되지 않는 네트워크에서 시스템을 업데이트하는 데 종종 사용되기 때문에 똑같이 취약 할 수 있다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.3</p>	<p style="text-align: center;">사이버 보안 관련 시스템 SYSTEM RELATED WITH CYBER SECURITY</p>	<p>PAGE 2 / 7</p>

Bridge systems that are not connected to other networks may be equally vulnerable, as removable media are often used to update such systems from other controlled or uncontrolled networks.

② 사이버 사건은 서비스 거부 또는 조작으로 확대 될 수 있으므로 ECDIS, GNSS, AIS, VDR 및 Radar / ARPA를 비롯한 탐색과 관련된 모든 시스템에 영향을 줄 수 있다.

A cyber incident can extend to service denial or manipulation, and therefore may affect all systems associated with navigation, including ECDIS, GNSS, AIS, VDR and Radar/ARPA.

2) 선교 시스템은 다음을 포함한다.

Bridge system include;

- ① 통합 항해 시스템
integrated navigation system
- ② 위치 시스템
positioning systems (GPS, etc.)
- ③ 전자해도 표시 정보 시스템
Electronic Chart Display Information System (ECDIS)
- ④ 전자해도와 연결된 시스템 및 추진/선박 조종 시스템
systems that interface with electronic navigation systems and propulsion/maneuvering systems
- ⑤ 자동 식별 시스템
Automatic Identification System (AIS)
- ⑥ 국제 해상 조난 및 안전 시스템
Global Maritime Distress and Safety System (GMDSS)
- ⑦ 레이더 장비
radar equipment
- ⑧ 항해 데이터 기록기
Voyage Data Recorders (VDRs)
- ⑨ 기타 모니터링 및 데이터 수집 시스템
other monitoring and data collection systems.

3.3 추진 및 기계 관리 및 전력 제어 시스템 :

Propulsion and machinery management and power control systems:

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.3</p>	<p style="text-align: center;">사이버 보안 관련 시스템 SYSTEM RELATED WITH CYBER SECURITY</p>	<p>PAGE 3 / 7</p>

1) 특징 및 주요 취약 점

Characteristics and vulnerable

① 선내 기계, 추진 및 조향을 모니터링하고 제어하기 위한 디지털 시스템의 사용은 그러한 시스템을 사이버 공격에 취약하게 만든다.

The use of digital systems to monitor and control onboard machinery, propulsion and steering make such systems vulnerable to cyber attacks.

② 이러한 시스템의 취약성은 원격 상태 기반 모니터링과 함께 사용되거나 통합 선교 시스템을 사용하는 선박의 항해 및 통신 장비와 통합 될 때 증가 할 수 있다.

The vulnerability of these systems can increase when they are used in conjunction with remote condition-based monitoring and/or are integrated with navigation and communications equipment on ships using integrated bridge systems.

2) 추진 및 기계 관리 및 전력 제어 시스템은 다음을 포함한다.

Propulsion and machinery management and power control systems include;

① 전자 제어 엔진

ME engine

② 전력 관리

power management

③ 통합 제어 시스템

integrated control system

④ 알람 감시 시스템

alarm monitoring system

⑤ 비상 대응 시스템

emergency response system.

3.4 출입 통제 시스템

Access control systems

1) 특징 및 주요 취약 점

Characteristics and vulnerable

: 감시, 선상 보안 경보 및 전자 "승선인원"시스템을 포함하여 배 및 화물의 물리적 보안 및 안전을 보장하기 위해 출입 통제를 지원하는 데 사용되는 디지털 시스템.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.3</p>	<p style="text-align: center;">사이버 보안 관련 시스템 SYSTEM RELATED WITH CYBER SECURITY</p>	<p>PAGE 4 / 7</p>

Digital systems used to support access control to ensure physical security and safety of a ship and its cargo, including surveillance, shipboard security alarm, and electronic “personnel-on-board” systems.

2) 출입 통제 시스템은 다음을 포함한다.

Access control systems include;

- ① CCTV 네트워크와 같은 감시 시스템
surveillance systems such as CCTV network
- ② 선교 항해당직 경보 시스템 (BNWAS)
Bridge Navigational Watch Alarm System (BNWAS)
- ③ 선내 보안 경보 시스템
Shipboard Security Alarm Systems (SSAS)

3.5 행정 및 승무원 복지 시스템

Administrative and crew welfare systems:

1) 특징 및 주요 취약 점

Characteristics and vulnerable

- ① 선박 운영 또는 승무원 복지에 사용되는 선내 컴퓨터 네트워크는 인터넷 액세스 및 전자 메일을 제공 할 때 특히 취약하다.

Onboard computer networks used for administration of the ship or the welfare of the crew are particularly vulnerable when they provide internet access and email.

- ② 이러한 시스템은 제어되지 않는 것으로 간주되어야 하며 선상 안전 관련 중요 시스템에 연결되어서는 안된다.

These systems should be considered uncontrolled and should not be connected to any safety critical system on board.

- ③ 선박 관리 회사 또는 소유자가 제공하는 소프트웨어도 이 범주에 포함됩니다.

Software provided by ship management companies or owners is also included in this category.

2) 행정 및 승무원 복지 시스템은 다음을 포함한다.

Administrative and crew welfare systems: include;

- ① 행정 시스템

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.3</p>	<p style="text-align: center;">사이버 보안 관련 시스템 SYSTEM RELATED WITH CYBER SECURITY</p>	<p>PAGE 5 / 7</p>

administrative systems

- ② 승무원 Wi-Fi 또는 LAN 인터넷 액세스. 예를 들어 선상 직원 자신의 장치.

crew Wi-Fi or LAN internet access, for example where onboard personnel can connect their own devices.

3.6 통신 시스템

Communication systems

1) 특징 및 주요 취약 점

Characteristics and vulnerable

- ① 위성 및 / 또는 기타 무선 통신을 통한 인터넷 연결성은 선박의 취약성을 증가시킬 수 있다.

Availability of internet connectivity via satellite and/or other wireless communication can increase the vulnerability of ships.

- ② 서비스 제공 업체가 구현 한 사이버 방어 메커니즘은 신중하게 고려되어야 하지만 모든 선상 시스템과 데이터를 보호하기 위해 전적으로 의존해서는 안된다.

The cyber defense mechanisms implemented by the service provider should be carefully considered but should not be solely relied upon to secure every shipboard systems and data.

2) 통신 시스템은 다음을 포함한다.

Communication systems include;

- ① 통합 통신 시스템

integrated communication systems

- ② 위성 통신 장치

satellite communication equipment

- ③ VOIP (Voice over Internet Protocols) 장비

Voice Over Internet Protocols (VOIP) equipment

- ④ 무선 네트워크

wireless networks

- ⑤ 공공 주소 및 일반 경보 시스템

public address and general alarm systems.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.3</p>	<p style="text-align: center;">사이버 보안 관련 시스템 SYSTEM RELATED WITH CYBER SECURITY</p>	<p>PAGE 6 / 7</p>

3.7 육해상 인터페이스

Ship to shore interface

- 1) 육상측 작업과의 통합이 점점 더 복잡해지고 있다. 디지털 커뮤니케이션이 비즈니스 수행, 운영 관리 및 본사와의 연락을 위해 사용되고 있기 때문이다. 또한 탐색, 전력 및 화물 관리의 안전에 필수적인 중요한 선박 시스템은 점점 더 디지털화되어 인터넷과 연결되어 다음과 같은 다양한 합법적 기능을 수행한다.

Ships are becoming more and more integrated with shore side operations because digital communication is being used to conduct business, manage operations, and stay in touch with head office. Further, critical ship systems essential to the safety of navigation, power and cargo management have been increasingly digitalized and connected to the internet to perform a wide variety of legitimate functions such as:

- ① 엔진 성능 모니터링
engine performance monitoring
- ② 유지 보수 및 예비 부품 관리
maintenance and spare parts management
- ③ 화물, 크레인 및 펌프 관리
cargo, crane and pump management
- ④ 항해 성능 모니터링.
voyage performance monitoring.

3.8 공통 취약점

Common vulnerabilities

- 1) 특징 및 주요 취약 점

Characteristics and vulnerable

- ① 사용되지 않는 운영 체제 및 지원되지 않는 운영 체제
obsolete and unsupported operating systems
- ② 오래된 바이러스 백신 소프트웨어 및 맬웨어 방지
outdated or missing antivirus software and protection from malware
- ③ 비효율적 인 네트워크 관리와 기본 관리자 계정 및 암호 사용, 최소 권한 원칙을 기반으로 하지 않는 비효율적 인 네트워크 관리를 포함하여 부적절한 보안 구성 및 모범 사례

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>APP.3</p>	<p style="text-align: center;">사이버 보안 관련 시스템 SYSTEM RELATED WITH CYBER SECURITY</p>	<p>PAGE 7 / 7</p>

inadequate security configurations and best practices, including ineffective network management and the use of default administrator accounts and passwords, and ineffective network management which is not based on the principle of least privilege

- ④ 보호 수단 부족하고 네트워크 분리가 없는 선내 컴퓨터 네트워크

shipboard computer networks, which lack boundary protection measures and segmentation of networks

- ⑤ 육상과 상시 연결된 안전에 중요한 장비 또는 시스템

safety critical equipment or systems always connected with the shore side

- ⑥ 계약자 및 서비스 제공 업체를 포함한 제 3 자에 대한 부적절한 접근 제어.

inadequate access controls for third parties including contractors and service providers

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.4</p>	<p style="text-align: center;">위험 노출 평가 ASSESS RISK EXPOSURE</p>	<p>PAGE 1 / 4</p>

4.1 회사의 위험 평가

Risk assessment made by the company

1) 평가 시기

Interval of assessment

① 최소 년 1회

At least once a year

② 사이버 보안의 위협을 감지 하였을 시

When treated cyber security

2) 평가자

Assessor

: 회사 보안 책임자

Company Security officer

3) 위험 평가 프로세스는 선박의 시스템을 평가하여 현재의 사이버 위협 수준을 처리하기 위한 견고성을 매핑한다.

The risk assessment process starts by assessing the systems on board, in order to map their robustness to handle the current level of cyber threats

① 육해상 IT 시스템을 보호하기 위한 기존 기술 및 절차의 식별.

Identification of existing technical and procedural controls to protect the shore and shipboard IT systems

② 인적 요인을 포함한 특정 취약성 및 이러한 시스템의 사용을 통제하는 정책 및 절차를 포함한 취약한 IT 시스템을 식별.

Identification of IT systems that are vulnerable, the specific vulnerabilities identified, including human factors, and the policies and procedures governing the use of these systems

③ 사이버 공격에 취약한 주요 육상/선박 시스템 운영의 식별 및 평가

Identification and evaluation of key shore and ship board operations that are vulnerable to cyber attacks

④ 잠재적인 사이버 사건과 주요 선박 운항에 미치는 영향, 그리고 발생 시 보호대책을 수립하고, 우선순위를 확립할 가능성.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>APP.4</p>	<p style="text-align: center;">위험 노출 평가 ASSESS RISK EXPOSURE</p>	<p>PAGE 2 / 4</p>

Identification of possible cyber incidents and their impact on key ship board operations, and the likelihood of their occurrence to establish and priorities protection measures.

4.2 선박 평가

Ship assessment

1) 평가 시기

Interval of assessment

① 최소 년 1회

At least once a year

② 사이버 보안의 위협을 감지 하였을 시

When treated cyber security

2) 평가자

Assessor

: 선박 보안 책임자

Ship Security officer

3) 선박 네트워크와 시스템 및 장치의 평가의 목적은 손상되거나 무결성 상실 또는 장비, 시스템, 네트워크 또는 심지어 선박의 작동 손실을 초래할 수 있는 취약성을 식별한다.

The goal of the assessment of a ship's network and its systems and devices is to identify any vulnerabilities that could compromise or result in either loss of confidentiality, loss of integrity or result in a loss of operation of the equipment, system, network, or even the ship.

① 소프트웨어 결함이나 오래되거나 패치 없는 시스템과 같은 기술

Technical such as software defects or outdated or un-patched systems

② 액세스 관리, 비관리 네트워크 상호연결 등의 설계

Design such as access management, unmanaged network interconnections

③ 잘못 구성된 방화벽에 대한 구현 오류

Implementation errors for example misconfigured firewalls

④ 절차 또는 기타 사용자 오류

Procedural or other user errors.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.4</p>	<p style="text-align: center;">위험 노출 평가 ASSESS RISK EXPOSURE</p>	<p>PAGE 3 / 4</p>

5) 작성된 기록은 회사 보안 책임자에게 전달한다.

The recording is to be sent to company security officer

4.3 제 3자의 위험 평가

Third-party risk assessments

자가 평가는 좋은 출발이 될 수 있으나, 제3자의 위험 평가를 통해 더 심층적으로 보완할 수 있으며, 자체 평가 동안에 발견되지 않을 위험과 격차를 식별할 수 있다

Self-assessments can serve as a good start, but may be complemented by third- party risk assessments to drill deeper, and identify the risks and the gaps that may not be found during the self-assessment.

4.4 취약점에 대한 검토

Review of vulnerability

- 1) 평가자는 평가 후에, 각각의 식별된 취약성은 잠재적인 영향과 그것의 악용 가능성에 대한 평가를 평가해야 한다.

Following the assessment, each identified vulnerability should be evaluated for its potential impact and the probability of its exploitation by assessor.

① 실행 요약

Executive summary

: 평가 된 환경, 시설 또는 선박의 결과, 권고 사항 그리고 전반적인 보안 개요 요약
a high-level summary of results, recommendations and the overall security profile of the assessed environment, facility or ship

② 기술적인 발견

Technical findings

: 발견 된 취약점, 악용 가능성, 결과로 인한 영향 및 기술 수정 및 완화 조언에 대한 자세한 표 형식의 분석

a detailed, tabular breakdown of discovered vulnerabilities, their probability of exploitation, the resulting impact, and technical fix and mitigation advice

③ 우선 순위 행동 리스트

Prioritized list of actions

: 할당 된 우선순위는 측정의 효과성, 비용, 적용 가능성 등을 반영해야 하며, 이 목록은 사용 가능한 옵션의 전체 목록이 아닌 타사 위험 목록을 나타내는 서비스 및 제품 목록을 나타낸다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.4</p>	<p style="text-align: center;">위험 노출 평가 ASSESS RISK EXPOSURE</p>	<p>PAGE 4 / 4</p>

The priorities allocated should reflect the effectiveness of the measure, the cost, the applicability, etc. It is important that this list does not represent a list of services and products the third-party risk assessor would like to sell, instead of being a complete list of options available.

④ 보충 자료

Supplementary data

: 모든 주요 조서 결과에 대한 기술적 세부사항과 중대한 결함에 대한 포괄적인 분석을 포함하는 부록. 중요하거나 위험성 높은 취약성의 침투 시험 동안 복구된 샘플 데이터도 포함되어야 한다.

a supplement containing the technical details of all key findings and comprehensive analysis of critical flaws. This section should also include sample data recovered during the penetration testing of critical or high-risk vulnerabilities

4.5 시스템 관리자에게 보고

Report to system administrator

: 시스템 개선이 필요한 경우 평가 결과를 시스템 관리자에게 전달하여 시스템 개선을 요청한다.

If system improvement is required, the result of assessment is sent to the system administrator to request improvement of the system.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 1 / 12</p>

5.1 기술적 보호 조치

Technical protection measures

1) 네트워크 포트, 프로토콜 및 서비스의 제한 및 제어

Limitation to and control of network ports, protocols and services

① 네트워크 시스템에 대한 액세스 목록을 사용하여 회사의 보안 정책을 이행할 수 있다. 따라서 해당 제어 정책에 따라 제어되는 네트워크 또는 서브넷을 통한 트래픽만 허용됩니다.

Access lists to network systems can be used to implement the company's security policy. This ensures that only traffic will be allowed via a controlled network or subnet, based on the control policy of that network or subnet.

② 라우터가 공격으로부터 보호되고, 시스템 또는 데이터에 대한 무단 액세스를 방지하기 위해 사용하지 않는 포트를 닫아야 합니다.

It should be a requirement that routers are secured against attacks and unused ports should be closed to prevent unauthorised access to systems or data.

2) 방화벽, 라우터 및 스위치와 같은 네트워크 장치 구성

Configuration of network devices such as firewalls, routers and switches

① 통제되지 않은 네트워크는 데이터 트래픽 제어 부족으로 인해 위험을 초래할 수 있으며, 이는 직접적인 인터넷 연결이 멀웨어에 의해 침투하기 쉽기 때문에 통제된 네트워크로부터 격리되어야 한다.

Uncontrolled networks may pose risks due to lack of data traffic control and they should be isolated from controlled networks, as direct internet connection makes them highly prone to infiltration by malware

3) 물리적 보안

Physical security

① 보안 및 안전 중요도 부품 및 케이블 구동 장비는 무단 접근으로부터 보호되어야 한다.

Security and safety critical equipment and cable runs should be protected from unauthorised access.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 2 / 12</p>

4) 탐지, 차단 및 알림

Detection, blocking and alerts

① 침입과 감염을 파악하는 것은 통제력의 중요한 부분이다. 사이버 사고 경보 임계값을 설정할 수 있도록 사용자 및 시스템에 대한 네트워크 운영 및 예상 데이터 흐름을 설정하고 관리해야 한다.

Identifying intrusions and infections is a vital part of the controls. A baseline of network operations and expected data flows for users and systems should be established and managed so that cyber incident alert thresholds can be established.

5) 위성 및 무선 통신

Satellite and radio communication

① 무선 및 위성 연결의 사이버 보안은 서비스 제공 업체와의 협력으로 고려되어야 한다. 또한, 선상 네트워크 보호에 대한 요구 사항을 정립할 때 위성 네트워크의 사양을 고려해야 한다.

Cyber security of the radio and satellite connection should be considered in collaboration with the service provider. In this connection, the specification of the satellite link should be considered when establishing the requirements for onboard network protection.

② 육상 기반 서비스 제공자에게 선박의 운항 및 제어 시스템에 대한 연결을 구축할 때, 부적절한 연결 장치가 선상시스템에 접속하는 것을 방지하는 방법에 대한 고려해야 한다.

When establishing an uplink connection for ships' navigation and control systems to shore-based service providers, consideration should be given in how to prevent illegitimate connections gaining access to the onboard systems.

③ 네트워크에 연결된 서버와 컴퓨터 앞에 있는 방화벽을 배치해야 한다

You need to deploy a firewall in front of the computer and servers connected to the network

④ 웹 기반 사용자 인터페이스의 보호 또한 고려해야 한다.

Protection of the Web-based user interface should also be considered.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 3 / 12</p>

6) 무선 접속 제어

Wireless access control

① 선박의 네트워크에 대한 무선 접속이 승인 된 장치로 제한되고 정기적으로 변경되는 강력한 암호화 키를 사용하여 보안을 유지해야 한다

It should be ensured that wireless access to networks on the ship is limited to authorised devices and secured using a strong encryption key, which is changed regularly.

7) 멀웨어 탐지

Malware detection

① 선상 컴퓨터는 육상 컴퓨터와 동일한 수준으로 보호되어야 한다.

As a general guideline, onboard computers should be protected to the same level as office computers ashore.

② 안티 바이러스 및 멀웨어 방지 소프트웨어는 설치된 모든 개인 관련 컴퓨터에 설치, 유지 보수 및 업데이트되어야 한다.

Anti-virus and anti-malware software should be installed, maintained and updated on all personal work-related computers onboard.

8) 하드웨어 및 소프트웨어에 대한 보안

Secure configuration for hardware and software

① 일반 사용자 프로필의 설정 및 비활성화를 제어할 수 있도록 관리자가 관리자 프로필을 제공해야 합니다.

Only senior officers should be given administrator profiles so that they can control the set up and disabling of normal user profiles.

② 사용자 프로필은 시스템, 워크 스테이션 또는 서버가 필요한 목적으로 사용될 수 있도록 제한해야 한다.

User profiles should be restricted to only allow the computers, workstations or servers to be used for the purposes for which they are required.

③ 사용자 프로파일은 사용자가 시스템을 변경하거나 새 프로그램을 설치하거나 실행할 수 없도록 해야 한다

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 4 / 12</p>

User profiles should not allow the user to alter the systems or install and execute new programs.

9) 이메일 및 웹 브라우저 보호

Email and web browser protection

① 선박과 육상 간의 이메일 통신은 선박 운항의 필수적인 부분인 만큼, 보안 또한 확실해야 한다

Email communication between ship and shore is a vital part of a ship's operation.
Appropriate email and web browser protection serves to:

② 전자메일이나 음성을 통해 중요한 정보를 안전하게 교환하여 데이터의 기밀성과 무결성을 확인한다. 예를 들어 암호화를 통해 보호한다.

Ensure that the exchange of sensitive information via email or by voice is appropriately protected to ensure confidentiality and integrity of data, for example protecting by encryption

③ 악의적인 스크립트의 실행으로부터 웹 브라우저와 메일 클라이언트를 보호한다.

Prevent web browsers and email clients from executing malicious scripts.

④ zip 또는 암호화 된 파일로 전자 메일을 보내고 전자 메일 시스템에서 하이퍼 링크를 사용하지 않도록 설정하고 일반 전자 메일 주소를 사용하지 않고 시스템에서 사용자 계정을 구성했는지 확인한다.

Email as zip or encrypted file when necessary, disable hyperlinks on email system, and avoid using generic email addresses and ensure the system has configured user accounts.

10) 데이터 복구 기능

Data recovery capability

① 데이터 복구 기능은 안전한 사본 또는 이미지에서 시스템 및 / 또는 데이터를 복원하여 깨끗한 시스템의 복원을 가능하게 하는 기능이다.

Data recovery capability is the ability to restore a system and/or data from a secure copy or image thereby allowing the restoration of a clean system.

② 중요한 정보와 소프트웨어는 백업 기능을 사용하여 사이버 사건 후에 복구 할 수 있어야 한다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 5 / 12</p>

Essential information and software could be backup facilities should be available to ensure it can be recovered following a cyber incident.

- ③ 데이터 가용성 요구 사항이 높은 시스템은 복원력이 있어야 한다..

Systems that have high data availability requirements should be made resilient.

- ④ OT 시스템은 선박의 안전한 항해 및 운영에 필수적이며, 사이버 사건 발생 후 항해 및 운항 능력을 신속하고 안전하게 회복 할 수 있는 백업 시스템을 갖추고 있어야 한다.

OT systems, which are vital to the safe navigation and operation of the ship, should have backup systems to enable the ship to quickly and safely regain navigational and operational capabilities after a cyber incident.

11) 응용 소프트웨어 보안 (패치 관리)

Application software security (patch management)

- ① 중요한 안전 및 보안 업데이트는 선상 시스템에 제공되어야 한다.

Critical safety and security updates should be provided to onboard systems.

- ② 이러한 업데이트 또는 패치는 시스템의 결함이 사이버 공격에 의해 악용되기 전에 해결 될 수 있도록 시기 적절하게 정확하게 적용되어야 한다.

These updates or patches should be applied correctly and in a timely manner to ensure that any flaws in a system are addressed before they are exploited by a cyber attack.

5.2 절차상 보호 조치

Procedural protection measures

1) 교육 및 인식

Training and awareness

- ① 교육은 사이버 안전 및 보안에 대한 효과적인 접근법에 대한 핵심적인 지원 요소이다.

Training and awareness is the key supporting element to an effective approach to cyber safety and security as described in these guidelines

- ② 내부의 사이버 위협은 상당하며 과소 평가되어서는 안됩니다. 인사는 IT 및 OT 시스템을 보호하는 데 핵심적인 역할을 하지만 부주의 할 수도 있다.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 6 / 12</p>

The internal cyber threat is considerable and should not be underestimated. Personnel have a key role in protecting IT and OT systems but can also be careless,

2) 교육 및 인식 프로그램 포함 내용(전승무원)

Education and awareness programs include(All crew)

① 이메일과 관련된 위험 및 안전한 방식으로 행동하는 방법
risks related to emails and how to behave in a safe manner

② 소셜 미디어, 채팅 포럼 및 데이터 이동이 덜 통제되고 모니터링 되는 클라우드 기반 파일 스토리지를 포함하여 인터넷 사용과 관련된 위험
risks related to internet usage, including social media, chat forums and cloud-based file storage where data movement is less controlled and monitored

③ 개인 장치 사용과 관련된 위험
Risks related to the use of own devices

④ 감염된 하드웨어 (이동식 미디어) 또는 소프트웨어 (감염된 패키지)를 사용하여 회사 하드웨어에 소프트웨어를 설치 및 유지 관리하는 것과 관련된 위험
risks related to installing and maintaining software on company hardware using infected hardware (removable media) or software (infected package)

⑤ 안티 바이러스 검사 또는 인증이 확인되지 않은 소프트웨어 및 데이터 보안 관행의 취약성과 관련된 위험
risks related to poor software and data security practices where no anti-virus checks or authenticity verifications are performed

⑥ 사용자 정보, 암호 및 디지털 인증서 보호
safeguarding user information, passwords and digital certificates

⑦ 의심스러운 활동이나 장치를 탐지하고 가능한 사이버 사건이 진행 중일 때보고 하는 방법
detecting suspicious activity or devices and how to report if a possible cyber incident is in progress

⑧ 사이버 사건이 선박의 안전 및 운항에 미칠 영향 또는 영향에 대한 인식

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 7 / 12</p>

awareness of the consequences or impact of cyber incidents to the safety and operations of the ship

⑨ 안티 바이러스 및 멀웨어 방지, 패치, 백업, 사고 대응 계획 및 테스트와 같은 예방적 유지 관리 루틴을 구현하는 방법 이해

understanding how to implement preventative maintenance routines such as anti-virus and anti-malware, patching, backups, and incident-response planning and testing

⑩ 선박 시스템에 연결하기 전에 서비스 제공 업체의 이동식 매체로 인한 위험으로부터 보호하기 위한 절차.

procedures for protection against risks from service providers' removable media before connecting to the ship's systems.

3) 항해 사관/ 기관 사관은 컴퓨터가 손상된 경우 해당 징후를 알아야 한다.

Officers /engineer should know the signs when a computer has been compromised.

여기에는 다음이 포함될 수 있습니다.

This may include the following:

① 반응이 없거나 반응이 느린 시스템

an unresponsive or slow to respond system

② 올바르게 실행되지 않거나 예기치 않게 실행되는 프로그램을 포함한 프로그램의 예상치 못한 오류

unexpected errors in programs, including failure to run correctly or programs running unexpectedly

③ 메모리의 갑작스러운 변경 혹은 예상치 못한 디스크 용량 변화

unexpected or sudden changes in available disk space or memory

④ 예상치 못한 메일의 반환

emails being returned unexpectedly

⑤ 빈번한 시스템 충돌

frequent system crashes

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 8 / 12</p>

⑥ 예기치 않은 네트워크 변경 문제

unexpected network connectivity difficulties

⑦ 비정상적인 하드 드라이브 혹은 프로세서 작동

abnormal hard drive or processor activity

⑧ 브라우저, 소프트웨어 또는 사용자 설정 및 권한의 예기치 못한 변화

unexpected changes to browser, software or user settings, including permissions.

4) 방문자를 위한 조치

Access for visitors

① 방문자가 네트워크에 접속할 수 있고 허용되는 경우에는 사용자 권한 측면에서 제한을 받아야 합니다.

If visitors are allowed and allowed to access the network, they should be limited in terms of user rights.

② 당국, 기술자, 대리인, 항구 관리 및 선주 대표와 같은 방문객은 선내에 있는 동안 컴퓨터 액세스와 관련하여 제한되어야 한다.

Visitors such as authorities, technicians, agents, port officials, and owner representatives should be restricted with regard to computer access whilst on board.

③ 민감한 OT 네트워크 컴퓨터에 대한 무단 액세스는 명확하게 표시된 물리적 장벽을 통해 금지되어야 한다.

Unauthorized access to sensitive OT network computers should be prohibited through clearly marked physical barriers.

④ 방문자가 네트워크에 액세스 할 필요가 있을 시

If access to a network by a visitor is required

-. 책임 사관의 허가를 득하고 사용자 권한 측면으로 제한된다.

Obtain permission by senior officer and it should be restricted in terms of user privileges.

⑤ 방문객이 컴퓨터 및 프린터 액세스를 요구하는 경우 모든 제어 된 네트워크에서 에어 갭이 있는 독립적 인 컴퓨터를 사용해야 한다

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 9 / 12</p>

If a visitor requires computer and printer access, an independent computer, which is air-gapped from all controlled networks, should be used.

⑥ 무단 액세스를 방지하려면 물리적으로 액세스 가능한 다른 모든 컴퓨터 및 네트워크 포트에서 이동식 미디어 차단기를 사용해야 한다.

To avoid unauthorized access, removable media blockers should be used on all other physically accessible computers and network ports.

5) 소프트웨어 유지 관리

Software maintenance

① 하드웨어 또는 소프트웨어 개발자가 더 이상 지원하지 않는 하드웨어 또는 소프트웨어는 잠재적인 취약성을 해결하기 위한 업데이트를 받지 못 합니다. 이러한 이유로, 더 이상 지원되지 않는 하드웨어와 소프트웨어의 사용은 사이버 위험 평가의 일환으로 회사에 의해 세심하게 평가되어야 한다.

Hardware or software that is no longer supported by its producer or software developer will not receive updates to address potential vulnerabilities. For this reason, the use of hardware and software, which is no longer supported, should be carefully evaluated by the company as part of the cyber risk assessment.

② 충분한 보안 수준을 유지하려면 보드에 관련된 하드웨어 및 소프트웨어 설치를 업데이트해야 합니다.

Relevant hardware and software installations on board should be updated to maintain a sufficient security level.

6) 안티 바이러스 및 맬웨어 방지 툴 업데이트

Anti-virus and anti-malware tool updates

① 소프트웨어 도구를 검색하여 맬웨어를 탐지하고 처리하려면 먼저 업데이트해야 합니다. 절차적인 요구 사항을 적시에 선박에 배포하고 모든 관련 컴퓨터가 업데이트되도록 하기 위해 절차적 요건을 수립해야 한다.

In order for scanning software tools to detect and deal with malware, they need to be updated. Procedural requirements should be established to ensure updates are distributed to ships on a timely basis and that all relevant computers on board are updated.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 10 / 12</p>

7) 원격 액세스

Remote access

① IT 또는 OT 시스템이 중단 된 경우 검토를 위해 모든 원격 액세스 발생을 기록해야 한다.

All remote access occurrences should be recorded for review in case of a disruption to an IT or OT system.

② 원격 액세스가 필요한 시스템은 정기적으로 명확하게 정의, 모니터링 및 검토해야 한다.

Systems, which require remote access, should be clearly defined, monitored and reviewed periodically.

8) 관리자 권한 사용

Use of administrator privileges

① 정보에 관한 전산팀에게만 허용되어야 한다.

Access to information should only be allowed to IT team.

② 관리자 권한은 시스템 구성 설정 및 모든 데이터에 대한 완전한 액세스 권한을 허용합니다. 관리자 권한이 있는 시스템에 로그인하면 기존 취약성이 더 쉽게 악용될 수 있습니다. 관리자 권한은 이러한 권한을 사용하여 시스템에 로그인하는 데 필요한 인력 진의 역할을 수행하는 적절한 교육을 받은 직원에게만 제공되어야 합니다.

Administrator privileges allow full access to system configuration settings and all data. Users logging into systems with administrator privileges may enable existing vulnerabilities to be more easily exploited. Administrator privileges should only be given to appropriately trained personnel who have a need, as part of their role in the company or on board, to log into systems using these privileges

③ 해당 사용자가 더 이상 선상에 있지 않을 경우 사용자 권한을 제거해야 합니다.

User privileges should be removed when the people concerned are no longer on board.

9) 물리적 및 이동식 미디어 컨트롤

Physical and removable media controls

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 11 / 12</p>

① 이동식 미디어 장치를 사용하는 것이 불가피한 상황 (예: 소프트웨어 유지 관리 중)의 경우, 멀웨어에 대한 이동식 미디어를 검사하거나 디지털 서명 및 워터 마크를 통해 소프트웨어를 확인 하여야 한다.

There are situations where it is unavoidable to use these media devices, for example during software maintenance. In such cases, it is required to check the removable media for malware and/or validating legitimate software by digital signatures and watermarks.

② 이동식 미디어의 사용과 관련된 정책 및 절차는 해당 선박의 통제된 네트워크에 연결되지 않은 컴퓨터의 모든 이동식 미디어 장치를 검사해야 한다

Policies and procedures relating to the use of

10) 물리적 및 이동식 미디어 컨트롤

Physical and removable media controls

① 통제되지 않은 시스템에서 통제 된 시스템으로 데이터를 전송하는 것은 멀웨어 유입 될 위험이 크다는 것을 나타낸다.

Transferring data from uncontrolled systems to controlled systems represents a major risk of introducing malware.

② 이동식 미디어는 방어 층을 우회하는 데 사용할 수 있으며 인터넷에 연결되어 있지 않은 시스템을 공격하는 데 사용될 수 있다.

Removable media can be used to bypass layers of defences and can be used to attack systems that are otherwise not connected to the internet.

③ 통제되지 않은 시스템과 통제 된 시스템간에 정보를 전송하는 데 미디어 장치가 일반적으로 사용되지 않도록 확인해야 한다.

It must ensure that media devices are not normally used to transfer information between un-controlled and controlled systems.

④ 미디어 장치를 사용하는 것이 불가피한 상황 일 시

Situations where it is unavoidable to use these media devices,

a. 디지털 서명 및 워터 마크를 사용하여 이동식 미디어에서 멀웨어 및 / 또는 합법적 인 소프트웨어의 유효성을 검사한다.

Check the removable media for malware and/or validating legitimate software by digital signatures and watermarks.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19 REV. NO. : 0</p>
<p>APP.5</p>	<p style="text-align: center;">사이버 보안 조치 CYBER SECURITY MEASURES</p>	<p>PAGE 12 / 12</p>

b. 선박의 제어 된 네트워크에 연결되지 않은 컴퓨터에서 이동식 미디어 사용시
이동식 미디어 장치를 검사해야 한다

Removable media devices must be inspected when using removable media on
computers that are not connected to the ship's controlled network

⑤ 회사는 파일을 선박 시스템에 업로드 하기 전에 이동식 미디어를 스캔 해야 한다는
요구 사항에 대해 포트 및 터미널에 알려야 한다. 이 스캔은 다음 파일 형식을 전송할 때
수행해야 한다.

Companies should notify ports and terminals about the requirement to scan removable
media prior to permitting the uploading of files onto a ship's system. This scanning should be
carried out when transferring the following file types:

- a. 화물 파일 및 적재 계획
cargo files and loading plans
- b. 국가, 세관 및 항만 당국 양식
national, customs, and port authority forms
- c. 벙커링 및 윤활유 형태
bunkering and lubrication oil forms
- d. 선용품 및 부식 목록
ship's stores and provisions lists
- e. 엔지니어링 유지 보수 파일.7
engineering maintenance files.

이 목록은 예제를 나타내며 철저한 것으로 간주되어서는 안된다.

This list represents examples and should not be seen as exhaustive.

12) 데이터 폐기를 포함한 장비 폐기

Equipment disposal, including data destruction

① 폐기 된 장비는 상업적으로 민감하거나 기밀 인 데이터를 포함 할 수 있다.

Obsolete equipment can contain data which is commercially sensitive or confidential.

② 장비를 폐기하기 전에 폐기 된 장비에 보관 된 데이터가 제대로 폐기되었는지
확인하여 중요한 정보를 검색 할 수 없어야 한다.

The data held in obsolete equipment is destroyed prior to disposing of the equipment,
ensuring that vital information cannot be retrieved

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.6</p>	<p style="text-align: center;">사이버 보안 대응 사건 대응 RESPONSE TO CYBER SECURITY INCIDENT</p>	<p>PAGE 1 / 3</p>

6.1 초기 평가

Initial assessment

1) 적절한 대응을 확보하기 위해 대응팀이 알아야 할 사항

To ensure an appropriate response, essential items that the response team find out:

- ① 사건 발생 경위
how the incident occurred
- ② 영향을 받는 IT 및 / 또는 OT 시스템과 정도
which IT and/or OT systems were affected and how
- ③ 상업 및 / 또는 운영 데이터가 영향을 받는 정도
the extent to which the commercial and/or operational data is affected
- ④ 남겨진 IT 및 OT에 대한 위협의 범위
to what extent any threat to IT and OT remains.

6.2 시스템 및 데이터 복구

Recover systems and data

1) IT 및 OT 시스템 및 데이터는 사이버 사건의 초기 평가 후 가능한 한 시스템의 위협을 제거하고 소프트웨어를 복원하여 작동 상태로 정리, 복구 및 복원 한다.

Following an initial assessment of the cyber incident, IT and OT systems and data should be cleaned, recovered and restored, so far as is possible, to an operational condition by removing threats from the system and restoring software.

- ① 해당 기기의 사용을 중지한다.
The device's operation should be suspended.
- ② 해당 기기와 다른 장치의 접촉을 제한한다. (네트워크 제거, USB 삽입 등)
The device should be prohibited to contact other devices. (Disconnecting network, Use of USB, etc.)
- ③ 회사에 필요한 지원을 요청한다. (수리, 교체, 프로그램 제공, 엔지니어 파견 등)
Request assistance to company. (Repair, replace, supply new program, service engineer, etc)

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
<p>APP.6</p>	<p style="text-align: center;">사이버 보안 대응 사건 대응 RESPONSE TO CYBER SECURITY INCIDENT</p>	<p>PAGE 2 / 3</p>

- 2) 사이버 사건이 복잡한 경우, 예를 들어 IT 및 / 또는 OT 시스템을 정상 작동 상태로 되돌릴 수 없는 경우, 선상의 비상 계획과 함께 복구 계획을 시작해야 할 수 있다. 이 경우 대응 팀은 다음과 같은 경우에 해당 선박에 조언을 제공 할 수 있어야 한다.

When a cyber incident is complex, for example if IT and/or OT systems cannot be returned to normal operation, it may be necessary to initiate the recovery plan alongside onboard contingency plans. When this is the case, the response team should be able to provide advice to the ship on:

- ① 데이터를 보호하기 위해 IT 또는 OT 시스템을 종료하거나 계속 실행해야 하는지 여부

whether IT or OT systems should be shut down or kept running to protect data

- ② 육상과의 특정 선박 통신 연결이 종료 되어야 하는지 여부

whether certain ship communication links with the shore should be shut down

- ③ 사전 설치된 보안 소프트웨어에 제공된 고급 도구를 적절한 사용

the appropriate use of any advanced tools provided in pre-installed security software

- ④ 사고가 IT 또는 OT 시스템에서 기존 복구 계획의 기능 이상으로 손상된 정도.

the extent to which the incident has compromised IT or OT systems beyond the capabilities of existing recovery plans.

6.3 사이버 사고 조사

Investigating cyber incidents

- 1) 가능한 경우 회사는 선박의 IT 및 OT에 영향을 미치는 사이버 사건을 조사해야 한다.

Companies should, wherever possible, investigate cyber incidents affecting IT and OT on board.

- 2) 사이버 사건의 원인과 결과를 이해하려면 필요한 경우 경우 외부 전문가의 지원을 받아 조사를 수행해야 한다.

To understand the causes and consequences of a cyber incident, an investigation should be undertaken by the company, with support from an external expert, if necessary.

- 3) 조사의 정보는 선박 및 육상의 기술 및 절차상의 보호 조치를 개선하는 데 사용될 수 있다.

The information from an investigation can be used to improve the technical and procedural protection measures on board and ashore.

	<p style="text-align: center;">보안 절차서 SECURITY PROCEDURE</p>	<p>DOC NO. : PR - 19</p> <p>REV. NO. : 0</p>
APP.6	<p style="text-align: center;">사이버 보안 대응 사건 대응 RESPONSE TO CYBER SECURITY INCIDENT</p>	<p>PAGE 3 / 3</p>

4) 모든 조사가 다음의 결과를 가져 온다.:

Any investigation should result in:

① 선내 및 육상에서 해양 산업이 직면 할 수 있는 잠재적 인 사이버 위험에 대한 더 나은 이해

a better understanding of the potential cyber risks facing the maritime industry both on board and ashore

② 인식 향상을 위한 교육 개선을 포함하여 학습 교훈의 확인

identification of lessons learned, including improvements in training to increase awareness

③ 재발 방지를 위한 기술적 및 절차 적 보호 조치에 대한 업데이트.

updates to technical and procedural protection measures to prevent a recurrence.

6.4 재발 방지

Prevent a re-occurrence

1) 위에서 언급한 조사 결과를 고려할 때 시정 조치 이행 관련 회사 절차에 따라 기술 및 절차 보호 조치에 대한 부적절한 조치를 고려해야 한다.

Considering the outcome of the investigation mentioned above, actions to address any inadequacies in technical and/or procedural protection measures should be considered, in accordance with the company procedures for implementation of corrective action.

평가서 번호 Sheet No.	KS-2018-003	대 분류 : Main Category : Security procedure			1차 분류 : 1st Category : Cyber security		2차 분류 : 2nd Category : Protection				
검토구간 Review section	실제적 잠재적 위험 Actual and Potential Hazards				현재안전조치 Present Safety Measurement	위험등급 Risk Grade					관리대상 Management Target
	공정변수 Process parameter	이탈 Deviation	원인 Cause	결과 Result		관리수준 Management Level	노출 Exposure Frequency	가능성 Probability Grade	위험성심각도 Seriousness grade	위험등급 Risk Rating	
Access Control	Confidential information	Access to confidential information	Unauthorized access	Leak / Loss of confidential information	Access rights assigned to roles; approval system in place for access rights requests.	2	2	2	D	1	No
Access Control	Critical system and data	Theft	Physical attack	Leak / Loss of information	Access rights need to be authorized and approved before access is granted.	2	1	2	D	1	No
Awareness	Training	Lack of awareness	No security awareness training for staff or contractors	Leak / Loss of personnel & company information	In-house training and external training	2	2	2	D	1	No
Data Security	Protection	Hacking or Intrusion	No protection system	Theft, Leak of secret, Loss of data or asset	Password / Authorize of network / System back-up	2	1	2	D	1	No
Data Security	System	Saturation of data processing resources due to legacy systems	Old system	Theft, Leak of secret, Loss of data or asset	Upgrade system and software	2	2	2	D	1	No
Data Security	Disposal	Unintentionally through	Incorrect disposal	Theft, Leak of secret, Loss of data or asset	Destroy of disposal data	2	1	2	D	1	No
Maintenance	Maintenance	Cyber attack	Poor maintenance	Paralysis of work, Loss of data or asset by hacking	Regular checks carried out by line management.	2	1	2	D	1	No
Protective Technology	Internal/external threats	Business critical systems disrupt	Vulnerabilities in operating systems	Paralysis of work, Loss of data or asset by hacking	Check information about vulnerabilities of business critical operating systems / Test and review when change system	2	1	2	D	1	No

평가서 번호 Sheet No.	KS-2018-001	대 분류 : Main Category : Risk assessment			1차 분류 : 1st Category : Management of change		2차 분류 : 2nd Category : Delivery of second hand ship				
검토구간 Review section	실제적 잠재적 위험 Actual and Potential Hazards				현재안전조치 Present Safety Measurement	위험등급 Risk Grade					관리대상 Management Target
	공정변수 Process parameter	이탈 Deviation	원인 Cause	결과 Result		관리수준 Management Level	노출빈도 Exposure Frequency	급성 Probability Grade	위험성심각도 Seriousness grade	위험등급 Risk Rating	
Protective Technology	Historical activities	Unable to track security event or incident.	Unauthorized access	Theft, Leak of secret, Loss of data or asset	Access by only authorized staff	2	1	2	D	1	No
Security Continuous Monitoring	Monitoring	Threats to the organization would not be caught	Insufficient monitoring procedures	Leak and loss by malware and hacking	Monitoring system in place to monitor traffic on network.	2	2	2	D	1	No
Detection Processes	Malfunction	Malfunction by Malware and hacking	Lack of protection	Leak and loss / Paralysis of work	Install anti-virus program and update / training for staff against cyber security	2	2	2	D	1	No

1) 관리수준 Management level

평 가 항 목 Assessment item	점수 Point
<p>시스템 : 발생방지를 위한 절차 및 발생 시 대응을 위한 절차가 있으며, 절차에 따라 잘 이행하고 있다. System : Has the procedure which enables to prevent the occurrence and/or to treat the situation occurred, and it is perfectly maintained and implemented.</p> <p>하드웨어 : 발생방지를 위한 안전장치, 설비가 있으며, 모두 정상적으로 작동하고 있다. Hard wear : Safety device and equipments for prevent the occurrence are provided and operated in normal condition.</p> <p>인력 : 관리자가 충분한 지식과 경험을 가지고 있으며 적절한 교육을 받았다. Manpower : Management has enough knowledge and receive appropriate education.</p>	1
시스템, 하드웨어 및 Manpower 중 1 가지가 미흡하다. Lack of one thing among system, hard ware and manpower.	2
시스템, 하드웨어 및 Manpower 중 2 가지가 미흡하다. Lack of two things among system, hard ware and manpower.	3
시스템, 하드웨어 및 Manpower 중 3 가지가 모두 미흡하다. Lack of three things among system, hard ware and manpower.	4

2) 노출빈도 Exposure frequency

노 출 빈 도 Exposure frequency	점수 Point
<p>년 1회 또는 그 이하의 빈도로 해당 작업에 노출된다. Exposed frequency of the relevant job is once in a year or less.</p>	Yearly 1
<p>년 2회 정도의 빈도로 해당 작업에 노출된다. Exposed frequency of the relevant job is twice in a year.</p>	Half yearly 2
<p>년 3 ~ 4회 정도의 빈도로 해당 작업에 노출된다. Exposed frequency of the relevant job is 3 ~ 4 times in a year.</p>	Quarterly 3
<p>년 5 ~ 12회 정도의 빈도로 해당 작업에 노출된다. Exposed frequency of the relevant job is 5 ~ 12 times in a year.</p>	Monthly 4
<p>년 13회 또는 그 이상의 빈도로 해당 작업에 노출된다. Exposed frequency of the relevant job is 13 times in a year or more.</p>	Weekly 5

3) 발생 가능성 등급 산출 방법 How to calculate probability grade

노출 빈도 Exposure frequency 관리수준 Management level	5	4	3	2	1
4	4	4	4	4	4
3	3	3	3	2	2
2	3	2	2	2	2
1	1	1	1	1	1

4) 위험 심각도 Seriousness grade for risk

등 급 Seriousness grade	구 분 Specification of accident	구 분 기 준 Description
A	치명적 Fatal	인적 Human 사망, 실종, 다수부상 또는 질병. 1 인 부상 또는 질병 : 급성중독, 생명단축 질병(암, 등), 시력상실, 절단(신체부위절단), 큰 골절 기타 심각한 부상 또는 질병 Death, Missing, Numerous Injury or Disease. Personal Injury or Disease : Toxication, Shortening of life, Loss of eyesight or Hearing, Cut of body, Fracture of bone, Another serious disease or Injury.
		물적 Property 설비파손 또는 물적 피해 100 만 USD 이상, 운항 정지 기간 7 일 이상 Property damage more than 100 thousand USD Ship operation delay more than 7 days.
B	중대함 Critical	인적 Human 1 인부상 또는 질병 : 화상, 작은 골절, 청각장애, 시력장애, 열상, 피부염, 일반질병, 시력장애, 기타 4 주 이상의 치료를 요하는 부상/질병 Personal injury or disease including burn, slight fracture of bone, obstacle of eyesight and hearing and other injury or disease necessary for medical treatment more than 4 weeks.
		물적 Property 설비파손 또는 물적 피해 50 만 ~ 100 만 USD. 운항 정지 기간 3 일 이상 7 일미만 Property damage more than 50~ 100 thousand USD. Ship operation delay more than 3 days but less than 7 days.
C	보통 Ordinary	인적 Human 1 인부상 또는 질병 : 4 일 이상, 4 주미만의 치료를 요하는 부상/질병 Personal injury or disease necessary for medical treatment 4 days ~ 4 weeks.
		물적 Property 설비파손 또는 물적 피해 50 만 USD 미만. 운항 정지 기간 3 일 미만 Property damage less than 50 thousand USD. Ship operation delay less than 3 days.
D	경미 Slight	인적 Human 1 인부상 및 질병 : 4 일 미만의 치료를 요하는 부상/질병 Personal injury or disease necessary for medical treatment less than 4 days.
		물적 Property 설비파손 또는 물적 피해 1만 USD 이하. 운항 정지 기간 1일미만 Property damage less than 10 thousand USD. Ship operation delay less than 1 day.

5) 위험등급 판정 기준표 Risk rating matrix

발생가능성 등급 Probability grade		4	3	2	1
심각도 Seriousness grade					
치명적 Fatal (A)		5	4	3	2
중대함 Critical (B)		4	3	3	2
보통 Ordinary (C)		3	3	2	1
경미 Slight (D)		2	2	1	1