

# THE SECURITY POLICY

1. To maintain a high standard of security system in compliance with the SOLAS convention and the ISPS Code and guarantee confidence against a security threat.

SOLAS 협약 및 ISPS 법규를 준수하여 높은 수준의 보안 시스템을 유지하고 보안 위협에 대한 신뢰성을 보장.

2. Seeks to implement, and improvement high standards of the security system including Cyber Security  
사이버 보안을 포함한 높은 수준의 보안시스템, 이행 및 개선

3. For fully realized this policy;

이 방침을 완전히 실현하기 위하여;

- 1) The company established [COMPLY WITH SECURITY MEASURE] as its basic policy in order to ensure that all organizations in the company and all parts of the company's activities, including ship's crew and shore-based staff, conform to the company's security procedures.

회사는 회사 내 모든 조직과, 선박 및 직원을 포함한 회사 활동의 모든 부분이 회사의 보안 절차에 부합하도록 하기 위하여, [보안 활동의 생활화]를 기본 방침으로 수립한다.

- 2) All employees prevent information security accidents in advance, minimizing threats or losses that could result from loss, theft, or destruction of the information system.

모든 직원은 정보 보안 사고를 사전에 예방하여, 정보 시스템의 손실, 절도, 파괴 등으로 발생할 수 있는 회사 또는 선박에 미칠 수 있는 위협이나 손실을 최소화한다.

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

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

- 4) 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.

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

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

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



2025.01.01.

President : O-GIL, KWON