New Guidance for Cyber Resilience of Ships and Systems

■ Summary of Major Amendments

Related Rules/Guidance	Effective date
Guidance for Cyber Resilience of Ships and Systems	- ships contracted for construction on or after 1 July 2024

■ Major Amendments

○ Reason for Amendments

1. Technological evolution of vessels, ports, container terminals. etc and increased reliance upon Operation Technology(OT) and Information Technology(IT) has created an increased possibility of cyber-attacks
2. The aim is to provide requirements for Cyber Resilience of ships, on-board systems, equipment and components with the purpose of providing technical means to safeguard ships and shipping in general from current and emerging threats
3. Reflection of IACS UR E26 and E27(Rev.1)

○ Amendments

1. Ships complying with the Guidance will be assigned the notations **Cyber Resilience** or **Cyber Resilience(Managed)**
2. Providing the technical and survey requirements of ships based on the requirements of IACS UR E26 (Rev.1)
3. Providing the type approval test requirements of on-board systems, equipment and components based on the requirements of IACS UR E26 (Rev.1)

○ Impact Analysis

✓ Indication of any impact on and/or contribution to safety, security or environmental protection

: Enhancing ship's safety and security by the new cyber resilience guidance.

✓ Indication of any impact on net and gross scantlings

: N/A