Capital Ship Management Corp.

Cyber Security Policy

CAPITAL SHIP MANAGEMENT CORP. is committed to ensure Cyber Security, by establishing and maintaining the required office and vessel Cyber Security protection measures to safeguard the confidentiality, integrity and availability of Information, Information Systems and IT / OT equipment, in order to promote the Safety and Security of persons and property onboard within the company, both onboard and ashore.

The objective of this Policy is to protect the company's information assets (note 1) from all threats, whether internal or external, deliberate or accidental, to ensure operations continuity, minimize damage and maximize return on investments and relevant industry opportunities.

To fulfil these objectives, the management is committed to the following approach:

1. It is the Policy of **CAPITAL SHIP MANAGEMENT CORP.** to ensure that:
   - Information and Systems identified as vulnerable to Cyber-attacks will be protected from a loss of confidentiality (note 2), integrity (note 3) and availability (note 4).
   - Regulatory and legislative requirements are to be met.
   - Cyber Security Contingency Plans have been produced for support (note 5).
   - Cyber Security training is available to all staff.
   - All breaches of information security, actual or suspected, will be reported and investigated.

2. Guidance and procedures have been produced to support this policy. These include incident handling, information backup, system access, virus controls, passwords and encryption.

3. The role and responsibility of the Information Technology Manager is to manage information security and to provide advice and guidance on implementation of the Cyber Security Policy.

4. All managers are directly responsible for implementing this Policy within their departments.

5. It is the responsibility of each employee/crew member to adhere to the Cyber Security Policy.

6. The management is committed to provide all necessary resources onboard and ashore to support company's Cyber Security Objectives.

NOTES
1. Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or by using electronic means, stored on tape or video, or spoken in conversation.
2. Confidentiality: ensuring that information is accessible only to authorized individuals.
3. Integrity: safeguarding the accuracy and completeness of information and processing methods.
4. Availability: ensuring that authorized users have access to relevant information when required.
5. This will ensure that information and vital services are available to users whenever they need them.

Managing Director **Date: 02/01/2023**