Cyber Security Policy

This policy aims to provide a safe and secure working environment by developing a proactive approach to Cyber Security. To protect the Company's information systems and data from all threats, whether internal or external, deliberate or accidental, to ensure operations continuity, minimize impact of threats and provide resilience against cyber incidents. This policy applies to all Company's locations, vessels, employees/seagoing crew extending also to third party users.

The cyber security policy applied is and should be complementary to the safety and security management practices established by our company.

Samos Steamship will ensure that:

- Information Systems identified as vulnerable to Cyber Security attacks will be protected against loss of: **Confidentiality**, **Integrity** and **Availability**
- Measures to mitigate respond and recover from identified threats are in place.
- Actively promote Cyber Security awareness amongst office and seagoing personnel.
- Provide adequate training to the office and seagoing personnel.
- Aligns with shipping industry guidelines on cybersecurity.

To achieve these objectives:

- Cyber Security Plan has been produced for support. Guidance and procedures include incident handling and reporting, Information systems backup, systems access control, virus protection, network protection, passwords etc. Plan is in accordance with the latest industry guidelines and recommendations • Security procedures are regularly reviewed and updated, taking into account latest industry guidance.
- Assessments and exercises are undertaken to test preparedness.
- Independent specialist support is provided, as appropriate, to respond to identified threats.
- Third-Party vendor assessment and due diligence practices are in place.
- Risk assessment is conducted for all critical assets at our premises and on-board vessels.
- All breaches of information security, actual or suspected, will be reported to, and investigated by the Cyber Security Officer (Cyso).
- Innovative security technology is tested, evaluated and implemented as appropriate.
- Top management should set clear policies and provide relevant resources to support Information, Communication and other computer dependent systems.
- The company will provide comprehensive training to personnel, according to their responsibilities.
- All Departments managers are directly responsible for implementing Cyber Security Policy within their departments.
- All employees (shore based or sea going) are required to adhere to the Cyber Security Policy.
- Technical and other controls are in place to support cyber security management.
- Disaster recovery (DR) plan is in place and a location in different geographical area is selected.
- Backup procedures are in place and regularly tested. Backup logs are daily reviewed.

Specific Cyber Security control methods have been adopted, implemented, and maintained for achieving the set objectives and targets, taking into account the unique design characteristics and operating requirements of each office system and ship type, its cyber-enabled systems, its cyber-physical (control) systems, and their failure potential effects both onboard and ashore.