CYBER SECURITY POLICY

The purpose and objective of this Policy is to protect the Company's information assets, including data printed or written on paper, stored electronically, transmitted by post or electronic means, stored on tape or video, or spoken in conversation, 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 must ensure that:

- *Information and Systems identified as vulnerable to Cyber Security Incidents will be protected from a loss of confidentiality (ensuring that information is accessible only to authorized individuals), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to relevant information when required).*
- *Regulatory and legislative requirements are to be met.*
- *Cyber Security Contingency Plans have been produced for support.*
- *Cyber Security Training will be available to all staff.*
- *All breaches, actual or suspected, will be reported and investigated.*
- *Guidance and procedures to manage the cyber risk are in place. These include incident handling, information backup, system access, virus controls, passwords and encryption.*
- *The role and responsibility of the shore and shipboard personnel are addressed. All Managers are directly responsible for implementing this Policy within their Departments.*

This Policy abides all personnel employed ashore and/or onboard, contractors, visitors, vendors agents and any person using Company’s network systems.