

## INFORMATION TECHNOLOGY & CYBER SECURITY POLICY

The Company's management information environment is comprised largely of proprietary computer hardware and software systems, complemented by tailor-made software solutions, which address the Company's particular operating requirements.

The Company Management recognizes the fundamental risks to the safe ship operation through cybercrime and the need for regulation and those for the expansion of the own ISM management objectives

It is the Company's policy that all information should be treated as being of the highest confidentiality and available only to the Company's employees. Particular emphasis is placed on the confidentiality of Client information. Accordingly, access to the Company's information data base is strictly controlled.

The Company aims to safeguard assets, guide personnel and their actions, and allow freedom of action and of decision making within the boundaries of the system, avowing interference from both internal and external influences through the application of Cyber security methods.

In order to achieve these aims, The Company has put in place security and back-up systems, which demonstrate the Company's commitment to the preservation of its information technology systems and data.

The Management also ensure that the systems in use are designed, architected, engineered, built and operated with appropriate due care and due diligence to ensure the Cyber security.

Company Identify the Cyber Security hazards, the critical systems and ensure protection, detection , response and restore measures are in place.

The Company ensures that all employees are familiarized and understand the ICT & Cyber Security measures and other controls in order to use and protect systems, data, and asset functions.