INFORMATION SECURITY POLICY

The Company is committed to ensure Information Security, by establishing and maintaining the required Office, Vessel & Cloud Information Security measures to safeguard the Confidentiality, Integrity and Availability of Information and Information Systems in order to accomplish the Company's objectives.
The Company expects all its Employees to comply with the requirements relating to Information Security Risk Management as these are described in Information Security ISO/IEC 27001: 2022 Standard and ISM Code Objectives & Functional Requirements also considering MSC.428 (98) - Maritime Cyber Risk Management in Safety Management Systems (SMS) as well as TMSA3 – Element 13 and relevant Industry Guidelines. All employees and 3rd Parties are expected to be familiar with their relevant Information Security duties and responsibilities and follow the measures required to protect the Organization from any loss of Confidentiality, Integrity, and Availability of Information.

OBJECTIVE:

The Company's principal objectives are to:

- Ensure there is executive level sponsorship / support for Information Security.
- Establish regulatory compliance & best practice guidance.
- Ensure Information Security roles & responsibilities are defined.
- Target Continuous improvement through evaluation & mitigation of Information Security Risks.
- Develop and maintain a set of Information Security Policies, Procedures and Practices.
- Deliver regular Information Security Awareness Training & Education to Office & Vessel staff.
- Collect and analyze information related to Information Security Threats.
- Implement consistent technological safeguard / control measures.

These objectives will be achieved by:

- Developing & Implementing an Information Security Management System (ISMS) as part of Company's Integrated Management System (IMS).
- Defining ISMS Boundaries by compiling a Statement of Applicability (SoA) documenting & justifying controls adopted, their implementation status as well as any exclusions.
- Monitoring and Implementing regulatory requirements, Industry, and Information Security Best Practices.
- Ensuring the appropriate protection and usage of Company's information assets, including ICT Systems and telecommunication networks as well as Operation Technology (OT) equipment.
- Controlling users' behavior with ICT and OT systems through implemented procedures.
- Maintaining Company's Business Continuity through backup and restore capabilities.
- Assigning responsible personnel – both ashore and onboard – to execute relevant tasks.
- Actively promoting Information Security Awareness by arranging comprehensive training of all Company Personnel in Office and Onboard.
- Providing familiarization and promoting adherence of all 3rd Parties towards Company's Information Security Policies, Procedures and Practices.
- Collecting, processing, and analyzing information related to Information Security threats, from selected sources, which can be internal and external.
- Conducting regular documented Reviews and Internal Audits of ISMS Policies, Processes & Procedures, Awareness as well as ICT and OT assets and continuously improve.

The Company is committed to provide all necessary resources onboard and ashore to support the Company's Information Security Objectives. The Master has the **Ultimate Authority** and responsibility to take decisions regarding Information Security incidents or threats in order to preserve the Information Security onboard. In case of conflict between Safety and Information Security requirements, Safety will prevail.

Signed by COO: 

George A. Kouleris

Issue Date: 30/11/2021 Last Review : 04/05/2023