NLNG SHIPPING & MARINE SERVICES LIMITED

INFORMATION SECURITY POLICY

POLICY OBJECTIVE

The objective of the Information Security Policy is to ensure:

- Confidentiality: Ensuring that information and systems are accessible only to authorized users.
- Integrity: Safeguarding the accuracy and completeness of information and processing methods.
- Availability: Ensuring that authorized users have access to information and systems when required.
- Increased resilience of the Company to Cyber Security threats
- Proactive management and prompt response to the continuously evolving security threats both internal and external
- Optimization of costs associated with information security
- The entire company is protected from technology-based risks and other, more common threats, such as poorly informed staff or ineffective procedures.

SCOPE

The scope of this Information Security Policy shall include the following:

- All information systems (including computer equipment, network equipment and telecommunications equipment) owned or operated by the Company or connected to the Company network by third parties.
- All software (including operating systems, network services and application software) installed on applicable information systems.
- All information stored on digital media, paper-based, intellectual property, company secrets, data on-devices and in the Cloud, hard copies, corporate and personal; and applicable information systems.
- All external parties that provide services to NSML whether in respect of information processing facilities and other services where NSML information asset is involved.

POLICY STATEMENTS

NSML shall ensure that:

Information assets and information processing facilities are protected against unauthorized access.

Information is protected from unauthorized disclosure.

Information is made available to business users and any other approved parties on a "need to have" basis in line with documented business approval.

Statutory, expressed and implied legal obligations are met.

IT Disaster Recovery Plans are regularly reviewed to ensure minimum business impact in case of disaster or loss Unauthorized use of information assets and information processing facilities is prohibited.

Information Security training and awareness are conducted for all employees.

All breaches of information security, actual or suspected, are reported and investigated.

Adequate controls (administrative, technical/logical and physical) are implemented to protect NSML information asset and processing facilities as commensurate with the NSML risk appetite.

Controls are put in place to minimize the business impact of information/cyber security incidents

IMPLEMENTATION/RESPONSIBILITIES

The Information Security, Risks and Controls Unit in IMT department of NLNG and NSML IT department shall establish the framework for managing Information security within NSML. Information owners within NSML shall be responsible for the identification, implementation and maintenance of controls that are commensurate with the value of the information assets they own and the risks to which they are exposed.

It is the responsibility of all employees to adhere to this Information Security Policy.

Non-compliance with the Information Security Policy by any employee shall be subject to the Expectation and Compliance process.

The Executive Management of NSML shall be accountable for ensuring that appropriate information security controls are identified, implemented and maintained by information owners.

External service providers shall comply with Company's information security needs and requirements.

Executive Management shall support the continuous review, improvement and approval of the Company Information Security Policy and Information Security management framework.

ABDULKADIR K. AHMED
MD/CEO
January, 2024.