MARITIME & CYBER SECURITY POLICY

Maritime Security:

TMS Cardiff Gas Ltd. is involved in the shipping and transportation of Liquefied Gas by sea, and recognizes the threat and potential impact that the ever changing geo-political situation may have on its operations and is therefore committed to the protection of its ships and all personnel from all forms terrorism, piracy and criminal activity which are within its sphere of operation.

TMS Cardiff Gas Ltd. is committed to comply with the **International Ship and Port Facility Security (ISPS) Code** requirements and has implemented the current requirements of the Code and supporting SOLAS regulations and will apply any subsequent amendments when they arise.

TMS Cardiff Gas Ltd. is committed to complying with all local, national and international rules and regulations and legal obligations, including industry recommendations, guidelines and codes of practice as setting the standards for security within the company premises and on board its ships.

TMS Cardiff Gas Ltd. is committed to providing secure documented procedures for each security level that shall be fully implemented on board its ships which shall be periodically reviewed to ensure they meet the needs of responding to any future changes in the geo-political situation.

TMS Cardiff Gas Ltd. requires all ships to operate at **Security Level 1** at all times unless the security level has been raised by Flag or Port State Authorities in response to a specific threat or perceived threat to the security of the ship and its crew.

TMS Cardiff Gas Ltd. recognizes the importance of monitoring changes in legislation, equipment and practices which impact on ship security in order to continually improve the security of the ship and all persons on board, both at sea and in port.

TMS Cardiff Gas Ltd. is committed to providing all necessary resources to enable its ships and on board personnel to perform their duties safely and securely and to ensure that this policy is fully complied with at all times and by all persons involved with its implementation.

TMS Cardiff Gas Ltd. shall ensure that all third parties involved with its office and shipboard activities shall conform to the company policy when providing their services to the company and its ships during the course of their business activities.

TMS Cardiff Gas Ltd. is committed to ensuring that the implementation of specified security procedures on board its ships shall not give rise to a conflict between the safety and security of the ship and its crew and in this respect the Master has the ultimate authority for ensuring no such conflict arises.

Cyber Security:

The purpose and objective of this Policy is to protect the company's information assets (note 1) 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 fulfill these objectives, the management is committed to the following approach:

1) It is the Policy of the Company to ensure that:

- Information and Systems identified as vulnerable to Cyber-attacks will be protected against unauthorized access
- Confidentiality of information is assured (note 2)
- Integrity (note 3) of information is maintained
- Company's requirements for availability will be met (note 4).
- Regulatory and legislative requirements will be met.
- Cyber Security Contingency Plans have been produced for support.
- Cyber Security training will be available to all staff.
- All breaches of information security, actual or suspected, will be reported and investigated.

2) It is the responsibility of each crew member/employee to adhere to the Cyber Security Policy.

3) The role and responsibility (note 5) of the designated Information Security personnel is to manage information security and to provide advice and guidance on implementation of the Cyber Security Policy.

4) All managers are directly responsible for implementing this Policy within their business areas.

NOTES

1) Information takes many forms and includes data printed or written on paper, stored electronically, transmitted by post or using electronic means, stored on tape or video, spoken in conversation.

2) Confidentiality: The protection of information from unauthorized disclosure or intelligible interruption.

3) Integrity: safeguarding the accuracy and completeness of information and processing methods.

4) Availability: ensuring that authorized users have access to relevant information when required.

5) Nominated member of IT Department

.....

GEORGE KOURELIS
GENERAL MANAGER

THE ORIGINAL POLICY DOCUMENT IS SIGNED BY THE GENERAL MANAGER AND IS HELD BY THE QUALITY ASSURANCE DEPARTMENT