CYBER SECURITY POLICY

The purpose and objective of this Cyber Security Policy is to protect the company's information assets 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.

POLICY

1. Top Management has approved the Cyber Security Policy.
2. It is the Policy of the **SHIPS SURVEYS AND SERVICE** to ensure that:
   a. Information and Systems identified as vulnerable to Cyber-attacks will be protected from a loss of: confidentiality (note 2), integrity (note 3), and availability (note 4).
   b. Regulatory and legislative requirements are to be met.
   c. Cyber Security Contingency Plans have been produced for support (note 5).
   d. Cyber Security training will be available to all staff.
   e. All breaches of information security, actual or suspected, will be reported to, and investigated by, the Information Security Manager.
   f. Cooperating Third Parties (service providers, producers etc.) to be reviewed regarding their Cyber Security Policy and performance
3. Guidance and procedures have been produced to support this policy. These include incident handling, information backup, system access, virus controls, passwords and encryption.
4. The role and responsibility of the designated Information Security Manager (note 6) is to manage information security and to provide advice and guidance on implementation of the Cyber Security Policy.
5. The designated owner of the Cyber Security Policy has direct responsibility for maintaining and reviewing the Policy.
6. All managers are directly responsible for implementing the Cyber Security Policy within their departments.
7. It is the responsibility of each employee/crew member to adhere to the Cyber Security Policy.

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: ensuring that information is accessible only to authorized individuals.
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. This will ensure that information and vital services are available to users whenever they need them.
6. Depending on the size and nature of the business this may be a part or full-time role for the nominated person.

Approved by

Naples, Rev.0 – 30/09/2019

Ships Surveys and Service Srl
Sole Administrator