



## Cyber Security Policy Statement

The main purpose and target of this Policy is to protect the Informational and Operational Technology Systems of Queensway Navigation Co. Ltd from cyber threats whether internal or external, deliberate or accidental and to ensure their

- Confidentiality (ensuring that information is accessible only to authorized individuals)
- Integrity (safeguarding the accuracy and completeness of information and processing methods)
- Availability (ensuring that authorized users have direct and uninterrupted access to relevant information)

In order to protect its assets and business operations and secure the fulfillment of these objectives, company will ensure at all times that:

- The regulatory and legislative requirements are continuously monitored in order for this Policy to be in compliance and updated.
- Guidance, Procedures and Cyber Security Contingency Plans have been produced in order to prevent from deliberate, unauthorized, unintentional or accidental breaches and to ensure secure and seamless IT operations. These include deployment of Cyber Security preventive countermeasures, response, damage control, business continuity and disaster recovery plans.
- Cyber Security awareness is promoted to all ashore/on board personnel and contractors in order to encourage responsible IT operational behavior such as safe e-mail and browsing practices, locking of unattended work stations, safeguarding/frequent change of passwords, responsible use of social media, portable device usage control etc.
- Cyber Security training is available to all ashore/on board personnel through continuous upgrade of training material (via e-mails/CDs etc.) and Computer Based Training.
- All Cyber Security breaches/loss of data, actual or suspected, will be reported to Information Communication Technology Officer (ICT) Officer and investigated promptly.
- The role and responsibility of the ICT Officer is to manage security of all IT systems and processing data, provide advice, guidance and overall implementation of the Cyber Security Policy.
- It is the responsibility of each employee and crew member to comply with the Cyber Security Policy.

The Managing Director, DPA, Heads of Departments and ships' Masters are responsible for ensuring that the standards set forth by this policy are communicated to ship and shore staff and that their own conduct sets a good lead by example in all respect.

