



## Cyber Security and Information Protection Policy

The purpose of this policy is to protect the Information Technology (IT) and Operational Technology (OT) systems of Queensway Navigation Co. Ltd. from cyber threats, whether internal or external, deliberate or accidental, and to ensure their ongoing:

- 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 continuous and secure access to relevant information

This policy is implemented in accordance with IMO Resolution MSC.428(98) on Maritime Cyber Risk Management in Safety Management Systems.

This policy applies to both Information Technology (IT) and Operational Technology (OT) systems, including navigation, cargo, engine control, and communication systems.

To protect its digital assets and ensure business continuity, the Company shall:

- Continuously monitor relevant international and national regulatory and legislative requirements to ensure this policy remains compliant and up to date
- Maintain a Cyber Security Manual that includes procedures, guidance, and contingency plans to prevent unauthorized, deliberate, or accidental breaches and disruptions
- Implement layered cyber risk management measures, including incident response protocols, damage control measures, and business continuity and disaster recovery planning
- Ensure that access to IT and OT systems is restricted based on role-specific authorizations, and that network activity is continuously monitored for signs of malicious activity
- Promote cyber security awareness across all shipboard and shore-based personnel and contractors, including responsible use of email, internet, workstations, passwords, social media, and portable devices
- Provide structured and updated cyber security training, including onboard/offboard campaigns, circulars, Computer-Based Training (CBT), and awareness material
- Ensure that all cyber security incidents, breaches, or suspected data losses are reported immediately to the Information Technology Coordinator (ITC) or Cyber Security Officer (CySO) and investigated promptly
- Define the responsibility of the ITC/CySO, which includes managing the security of IT and OT systems, providing advice and guidance, and ensuring proper implementation of this policy across all Company operations
- Require all employees and crew members to understand and comply with the Cyber Security and Information Protection Policy as part of their operational responsibilities





- Ensure that cyber security controls and response plans are tested periodically through drills or simulations, and that this policy is reviewed regularly to reflect evolving threats and requirements

Cyber security is an essential component of the Company's risk management and operational resilience strategy. All personnel are expected to remain vigilant and to actively support the prevention and mitigation of cyber threats at all times.

