CYBER AND INFORMATION SECURITY POLICY

To support MARITECH® business objectives and its overall strategy, it is essential to protect the confidentiality, integrity, and availability of its technology and information assets, safeguard the solutions it offers, and adhere to industry standards. Every employee of MARITECH® is expected to actively engage in the implementation and observance of the policy; this responsibility chain starts with the Management and General Divisions.

MARITECH® is committed to safeguarding the confidentiality of corporate, client, and customer information through developing and continuous improvement techniques that include technical, organizational, and personnel precautions.

Our objectives

- Design and deliver Security practices that improve our technology and information resilience and reduce risk in alignment with our corporate risk appetite.
- Maintain and embed a corporate culture of awareness around technology and information security.

Policy principles

- **Risk Based:** Ensure technology and information related security decisions, controls and procedures mitigate risk within the defined risk appetite.
- **People Centric:** Develop an effective security culture through ongoing information security and awareness training.
- **Business-aligned:** Ensure technology and information security controls, processes and procedures are fit for purpose, supports a safe environment and return appropriate value to the business.
- **Secure by Design:** Ensure technology investments are selected, implemented, managed and maintained throughout their lifecycle incorporating appropriate security requirements.
- **Defense in depth:** Implement a multi-layered strategy for technology and information security that can flex to identify, detect, protect, respond and recover from threats and risk of compromise.
- **Response and Recovery:** Implement people, processes and systems that enable response to security incidents and ensure recovery in a timely and effective manner.

Actions

MARITECH® initiatives to support this policy include establishing and maintaining:

- Appropriate technology governance.
- Methods that enable technology delivery, information security management, and awareness.
- Leadership involvement and support for a defined program of work that delivers improvement activities targeted to reduce cybersecurity risk across OT and IT systems, assets, and services.
- Compliance with regulatory and legal obligations.

Cyber Security Framework

MARITECH® commits to aligning its Cyber Security Policy and related technology and information standards with the following framework to achieve the objectives and principles.

- International Standards Organization 27001 Information Security Standard (ISO 27001)

**The quality of these measures is controlled by ley performance indicators that are based on testing, audits, penetration tests, security scanning and other methods.*

The present policy

- Is approved by the Company's Sustainability Committee.
- Is developed and revised every three years unless this is required earlier, by the Company's Corporate Governance in cooperation with the Chief Information Officer who is responsible for its implementation.
- Applies to all Business Units of MARITECH®, while its basic principles are also of relevance to its employees, suppliers and business partners, as reflected in the "Suppliers & Business Partners Code of Conduct" of the Company.
- Is available to the Company's Stakeholders.
- The Company is committed to allocating the necessary resources for ensuring the implementation of its Cyber Security Policy, running awareness programs and making any necessary updates towards the continuous modernization and improvement of its performance.

MARITECH GROUP HOLDING LTD

Chen YiJie, Executive BoD member