UNICREW
MANAGEMENT

INFORMATION SECURITY POLICY

Unicrew Management's Information Security Policy underlines our commitment to protecting the confidentiality, integrity, and availability of company information assets. By adhering to this policy, we fortify our digital infrastructure and contribute to the long-term success and resilience of the organization. This policy and its parts apply in parallel with other policies and rules in this domain, including those of the shipowner, flag state and port state authorities, as well as regulatory agencies.

Objective: This policy is meant to ensure the confidentiality, integrity, and availability of information assets.

Scope: This policy covers all information, regardless of format or medium, that is generated, processed, stored, or transmitted within the company's facilities. It applies to all employees, contractors, third-party vendors, and any other entities with access to the company's information assets.

Classification: Data is classified into levels of sensitivity and urgency to ensure appropriate security measures are tailored to the value and sensitivity of information.

Data Handling: Procedures for secure handling, storage, and disposal of information are outlined to prevent unauthorized access or loss. Encryption, secure file sharing, and data retention guidelines ensure the integrity and confidentiality of information throughout its lifecycle. Only authorized individuals have access to specific data. User access is regularly reviewed and updated to prevent unauthorized use or exposure.

Systems Security: Comprehensive network security measures are implemented to fortify the company's digital infrastructure. Firewalls, intrusion detection systems, and vulnerability tests are conducted to identify and mitigate potential cyber threats.

Incidence and Reporting: A robust incident response plan is in place to address and mitigate security breaches promptly. Employees are sensitized to recognize and report suspicious activities, ensuring a swift and coordinated response to any potential threats.

Training and Awareness: Awareness and education programs are conducted regularly to keep employees informed about information security best practices.

Compliance and Continuous Improvement: This policy mandates compliance with relevant laws, regulations, and industry standards pertaining to information security. Regular audits and assessments are carried out to ensure the effectiveness of security measures and to identify opportunities for continuous improvement.

Jason M. Firth,
Managing Director