2.8 IT & CYBER SECURITY POLICY

1. PURPOSE

The purpose of this policy is to ensure safe, secure and reliable operations by protecting Olympic's information, systems and vessel operations from cyber threats. Cyber security is an integral part of operational safety and business resilience and is managed in line with other operational risks.
This policy supports compliance with applicable maritime and regulatory requirements, including International Maritime Organization requirements to address cyber risks within the Safety Management System (SMS), and other relevant cyber security and data protection requirements, like IACS UR E26/E27.

2. SCOPE

This policy applies to:

- All Olympic-managed companies and operations
- All persons with access to Olympic information or systems, including employees, crew, temporary staff, contractors and third parties
- All information technology (IT) and operational technology (OT) environments

3. STATEMENTS, PRINCIPLES & COMMITMENTS

Olympic manages cyber security risks in a systematic and risk-based manner, aligned with maritime safety requirements, applicable regulations and recognised standards.

Leadership and responsibility
Cyber security is a shared responsibility. Olympic defines clear roles and responsibilities across ship and shore, and management is responsible for ensuring effective cyber risk management.

Cyber risk management

- Cyber risks shall be identified, assessed and managed as an integral part of Olympic's safety management system (SMS) and enterprise risk management processes.
- The company follows internationally recognised principles for cyber security, including identity, protect, detect, respond and recover.

Protection of IT and OT systems

- Olympic shall protect both information technology (IT) systems and operational technology (OT) onboard vessels.
- Appropriate technical and organisational measures shall be implemented to prevent unauthorised access, disruption or misuse.

Access control and data protection

- Access to systems and data shall be restricted based on business needs and the principle of least privilege.
- Personal data shall be processed in accordance with applicable data protection laws and protected against unauthorised access, loss or disclosure.

Secure operations and monitoring

- Systems shall be monitored, maintained and updated to manage vulnerabilities and emerging threats.
- Backup and recovery solutions shall be in place to ensure operational continuity.

Incident management

- Cyber incidents and suspected weaknesses shall be reported without delay.
- The company shall maintain procedures for incident response, business continuity and recovery.

Supply chain and third-party security

- Cyber security risks related to suppliers, contractors and service providers shall be assessed and managed as part of procurement and contract management processes.

Fosnavåg 22.05.2026

Stig Remøy
CEO