## 2.8 CYBER SECURITY & IT POLICY

**§ 1 Who policy applies to**

Regulations apply to all employees in companies managed by Olympic including subsidiaries (hereinafter called Company), hired staff and others granted access to company information, in or outside the company's office locations and vessels. The policy is also valid for using private equipment when this is linked to the company's IT systems.

Cyber Security should be considered at all levels of the Company, from Senior Management ashore to onboard personnel, as an inherent part of the safety and security culture necessary for the safe and efficient operation of the vessel.

Olympic shall put in place necessary procedures and action to maintain the security of Cyber systems onboard our vessels and shore premises and implement best practices to safeguard from current and emerging cyber threats and vulnerabilities.

**§ 2 General**

The Company's IT systems is intended for preparation, processing, and storage of business-related information. All use and storage of private information shall be limited.
Private use must not charge bandwidth, storage, and processing capacity unnecessary. Use of the company's IT resources must not conflict with current ethical guidelines. The use of resources should not be in competition with the Company's business, or otherwise create negative reputation or publicity for the company.
Treatment and / or storage of business-related information on IT resources that are not owned and / or controlled by the Company shall not be made without prior written approval from the Company. The computer system may only be used for operating purposes. All data stored in the system, including documents and e-mails are considered basically as the company's property, according to applicable legislation.
Limited personal use of the computer system (surfing the web, writing private letters and e-mail) is permitted provided that the use does not compromise the employee's duties or safety and functionality of the computer system. Private files in small amounts can be stored in a private folder in a way that the document owner is identified.

**§ 3 Use of internet services**

Use of internet services should only occur with software approved by the company. When internet services are used, electronic tracks are generated. It is not allowed to search or browse the pages, or sites with services which may lead to the prosecution of a provider or user. One shall avoid web sites with increased risk of virus exposure, such as webpages with warnings. This applies both for company's and private equipment connected to the network.

**§ 4 General Hardware and Software**

Installation of hardware and software shall be done by authorized personnel with administrative rights.

**§ 5 The security software**

The company's hardware is equipped with software that is essential for the company's IT-security. Only authorized personnel can, modify, replace, discontinue, or modify the company's security solutions. Deviations must be reported immediately to superior officer. It is not allowed to test the security of systems and networks by attempting to breach the company's security mechanisms.

**§ 6 Access**

Access to the company's IT resources should be protected by use of password on startup. Access password on the particular machine should not be stored electronically using the "memo function", unless it is made special exceptions for this.
Password must at all times be treated in a proper manner and must not be communicated to anyone other than authorized IT personnel after specific request. Password should not normally be given by telephone request. All company computers should be set-up with password protected log out or screensaver with 15 minutes limit. For Captain and Chief officer users the limit time shall be 3 minutes. All Company computers should be regularly re-started at least weekly, to ensure installation of critical updates.
Individual computers should be without Admin rights, this should be covered by IT Department.

**§ 7 Handling of Data Files**

All business-related data files should be stored on company's servers and not on the local hard drive, USB's, or similar. If temporary storage is needed on local devices, the files should later be transferred to the server and then deleted locally.
It is not allowed to copy any business-related files, documentation, or e-mails to private storage medias without company approval.

**§ 8 Old Hardware**
Old hardware that will be discarded should first be reviewed by authorized personnel. Users are not permitted to carry out disposal of hardware. Destruction of hardware and storage media must be performed by authorized personnel in accordance with instructions. Contact Purchase/IT Department for information.

**§ 9 Use of mobile devices**
Storage of business-related information shall not be made on mobile phones, handheld devices and similar without approval. If such information is stored, the content must be protected by password or access code. The use of USB's or other external storage devices must be made with caution.

During watch keeping, personal use of smartphones, tablets or other IT devices is considered as unacceptable

**§ 10 Wireless networks**
Wireless networks shall not be connected to Company network resources without approval from IT department at the main office. All wireless networks on the vessel shall be password protected administrated by senior management of the location.

**§ 11 Disclosure**
Company's administration and personnel authorized by company's management, has the right to access all information stored on corporate IT resources without regard to storage location or labeling. This also applies in cases that require access to employee e-mail and personal data areas, according to applicable legislation. All company's network traffic may be reviewed with respect to illegal content.

**§ 12 Use of social medias**
It is not allowed to use Olympics IT or network resources to publish in any external media detailed information of vessel operation/ movement, colleagues, or express any opinion of negative competitive/reputational significance for the company. Social medias like Facebook, web discussion forum etc. are considered as external communication channels.
Updating of personal information, general geographic location, etc. is within acceptable use.
Ref 2.10 Social Media Policy

**§ 13 Consequences of breach**
Violation of this policy may endanger the company's business. Violations of the policy can be regarded as gross misconduct and made the subject of disciplinary action in accordance with applicable laws and treaties, including dismissal.

Fosnavåg 21.06.2024

Stig Remøy
CEO