INFORMATION TECHNOLOGY (IT) POLICY

This policy relates to all IT facilities provided by **Marlow Offshore Germany GmbH & Co. KG**. All staff (ashore and onboard) are expected to adhere to it. Deliberate and serious breach of the policy will lead to disciplinary measures.

Marlow Offshore Germany GmbH & CO. KG top management is committed to treating information security management issues with the same responsibility and importance which address the entire business operations in the ship management market. We strongly believe that in this way we maximize the benefit from the operation of the business, for our customers, our employees and our shareholders.

We are committed to support the implementation of information security management processes promising to conserve the following objectives:

- To protect the company's business information and any customer or partner information within our custody by safeguarding its confidentiality, integrity and availability.
- To establish measures to protect the company's 's information resources from theft, abuse, misuse and any damage.
- To establish responsibility and accountability for Information Security in the company.
- To encourage management and staff to maintain an appropriate level of awareness, knowledge and skills to allow them to minimise the occurrence and severity of Information Security incidents.
- To ensure that the company is able to continue its business activities in the event of significant Information Security incidents.
- To ensure any stakeholder that the company comply with normative and legislative requirements.

We intend to realize our commitment to following the principles of prevention and protection in accordance with legislative and regulatory requirements arising from the wider framework developed by the company's risk management and strategic importance, and through the publication of our actions and continuous improvement of our performance in the areas of Information Security.

This continuous effort made by the monitoring and implementation of high technologies and international practices, defining objectives and criteria which shall be continuous assessment of the risk level, the implementation of treatment programs and information, education and participation of workers in information security management system.

Seeking ways to improve the methods implemented information security management, will help us to protect constantly getting information more effectively managed. We will always keep all our interested parties such as customers, employees and shareholders informed for the improvement of our actions.

Top Management gives its full support and maximum priority in Information Security Management System, which will be reviewed systematically so that it is always aligned with the standards set.

All Marlow Offshore Germany's IT facilities and information resources remain the property of Marlow Offshore Germany and not of any Master, crew member or departments. By following this policy, we will help to ensure IT facilities are used legally, securely, and effectively and that software licensing and copyright agreements are being respected. Please be informed that copying software is illegal and may result in criminal charges.

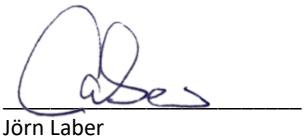
For security reasons strictly adhere to the following guidelines:

- Do not attempt to gain unauthorised access to information or facilities
- Do not disclose personal system passwords or other security details to anyone
- If you leave your PC unattended without logging off, you are responsible for any misuse of it, while you are away
- ALWAYS check storage media like flash drives, sticks, disks etc. for viruses with a company approved anti-virus software before use
- Do not make unauthorized changes to the system or to the software

Kindly take some general points on email use into account:

- Never open emails or email attachments from senders you do not know nor follow any sent links to confirm passwords etc.
- Installing Software: Get permission from Marlow Offshore Germany before you install any software (including public domain software) on equipment owned and/or operated by Marlow Offshore Germany.
- Handle all devices with care, as it would be your own equipment
- Do not re-arrange how equipment is plugged in (computers, power supplies, network cabling, modems etc.) without first contacting your department head.
- Do not take food or drinks into rooms which contain sensitive equipment like servers. Access to such rooms is limited to authorised staff only.

Hamburg, 05th December 2022



Jörn Laber
MD

Rev. 04