Maersk Offshore Wind
QMS-QMC-POL-0084
Revision 00 / 21/10/2024

MAERSK OFFSHORE WIND

Cyber Security & Information Classification Policy

1. PURPOSE

The Company aims to ensure compliance with all laws and obligations relating to privacy, confidentiality and cyber security, hereunder:

- Keeping all our information confidential (where it is legally permitted to do so) if its disclosure will be disadvantageous to the company.
- Create, identify, maintain and store information in a safe and secure way which facilitates appropriate access to it by those inside and outside the company who need to know it.

This policy provides guidelines for the organisation to improve the governance and practices relating to information and cyber security which are aligned to the company Information and Cyber Security Policies, Guidelines and Required Practices.

2. APPLICATION

This Policy applies to all our employees, contractors, suppliers and third-party personnel who is employed or engaged or works in any capacity on board our vessel(s), offices and workplaces ashore.

Information systems refer to computers, communication systems, data processing systems and servers that are directly managed by the IT department. Information systems also incl. mobile phones, scanners and printers.

3. POLICY STATEMENT

All applicable laws and regulations regarding the creation, retention, sharing, and destruction of information must be strictly followed:

- Effective information security measures must be implemented and maintained.
- Regular education and training on information and cyber security should be provided to all employees who handle relevant data.
- Information should be classified based on its significance, the risk of unauthorised disclosure, and the potential negative impact on the business from such disclosure.
- Information must only be utilised for its intended business purposes.
- Careful consideration must be given when sharing information with third parties to minimise the risk of loss; sensitive information should only be shared with authorised individuals.
- Highly sensitive information must be encrypted prior to transmission.
- Information owners are responsible for ensuring their data is adequately protected.
- Regular reviews of information security and cyber security risks, along with appropriate mitigation strategies, should be conducted.
- All sensitive information must be disposed of properly to prevent any possibility of reconstruction. This applies to all types of materials and storage devices, including paper, computers, audio and video tapes, disks, magnetic tapes, drives, USBs, and photographs.
- Access to facilities by employees and visitors should be regulated to reduce the risk of unauthorised access to or removal of sensitive information.

- Sensitive information should only be transmitted through corporate-approved email systems.
- Mobile devices that contain sensitive information or have access to corporate networks must be secured to prevent unauthorised data leaks.
- Computers and other IT equipment must be safeguarded against unauthorised access.
- Adequate controls must be established to protect personal data, ensuring its security and privacy while complying with all relevant laws and regulations.

Michael Reimer Mortensen

Chief Executive Officer

Maersk Offshore Wind