***Subject*: CYBERSECURITY POLICY AND OBJECTIVES - NIS2 Directive (EU 2022/2555)**

Turboden designs and builds plants in the field of renewable energy and heat recovery. Within the scope of its activities, the company safeguards the security of its own information and that of all stakeholders - guaranteeing its confidentiality, integrity and availability - and ensures the continuity, effectiveness and efficiency of communication systems (Cybersecurity), as far as this is within its direct control. Turboden also implements constant monitoring of cybersecurity events, promptly taking appropriate and effective remedial action.

To pursue these objectives, Turboden undertakes to:

• **Define, maintain, disseminate, improve and monitor a Cybersecurity System** based on a structured risk management process, aimed at ensuring full compliance with the requirements of Directive (EU) 2022/2555 "NIS2" transposed in Italy with Legislative Decree 138/2024, as well as with the guidelines of the National Cybersecurity Agency (ACN), through the implementation of appropriate mitigation measures.

• **Ensuring the continuous involvement of management,** promoting a cybersecurity culture at all levels of the company, communicating policy and objectives, guaranteeing the necessary resources and holding each function accountable.

• **Appointing, training and empowering** the figures foreseen by the NIS2 Directive for the definition, application, dissemination and monitoring of the effectiveness of the Cybersecurity System.

• **Encouraging the active and conscious participation of workers**, involving them in the implementation of the System and continuous improvement.

• **Integrate sustainability requirements** into the Cyber risk management process, where applicable.

Cybersecurity objectives

- **To increase the overall level of Cybersecurity**, spreading the culture of cybersecurity and ensuring that staff are adequately competent.
- **Identify, assess, classify and correct vulnerabilities**, ensuring the availability of adequate information and infrastructure assets (hardware, software, network systems) for all staff.
- **Monitor the Cybersecurity System** through appropriate audit plans, taking into account applicable regulatory and legal requirements.
- **Preserve data security**, ensuring confidentiality, integrity and availability.
- **Safeguard the physical security of tangible and intangible** assets by ensuring they are properly maintained and decommissioned.
- **Ensure the monitoring of information security events**, providing timely and appropriate responses to restore data and communication infrastructures.
- **Effectively manage crises**, maintaining business continuity and restoring the functionality of information and communication assets in the event of a disaster.
- **Review product design, planning, implementation and maintenance**, including Cyber risk assessment according to the Cybersecurity System.
- **Review and implement communication requirements requested by stakeholders**, ensuring that they do not conflict with the risk mitigation measures taken.
- **Reduce the environmental impact of communication systems**, contributing to the decarbonisation process.
- **Ensure the availability of suppliers, contractors and outsourcers that comply with Cybersecurity Management System criteria**, ensuring secure communications with company resources.

This Policy is communicated to all personnel and made available through official company channels. The Policy is subject to annual review, as well as in the event of changes in the cyber security regulatory environment, significant incidents, organisational changes or changes in exposure to threats and related risks. Any updates are approved by the governing and management bodies and communicated to all personnel in a timely manner.

Dr. Paolo Bertuzzi
Managing Director, CEO and DdL
(Legislative Decree 81/08)

Ing. Roberto Bini
Managing Director

Ing. Giorgio Fagnani
Procurator & QHSE Manager

This document contains proprietary information of Turboden S.p.A.
Duplication or disclosure to a third party of the information contained herein is expressly forbidden without the written consent of Turboden S.p.A.

MOVE THE WORLD FORWARD MITSUBISHI HEAVY INDUSTRIES GROUP