Introduction

Comer Industries and Walterscheid Powertrain Group (hereafter *the Company*) consider the information security and preservation of information as fundamental assets for the achievement of business objectives. Therefore, the Company is committed to ensure that the data, information and consequently the processing data systems, especially those having a strategic value for the business, are protected with security systems commensurate with their value and the risks to which they are subjected.

Policy objectives

The Company intends to protect information from any possible threat, internal or external, deliberate or accidental and puts in place strategies, processes, roles and responsibilities in order to ensure the security of the strategic and personal data of all those involved: employees, customers, suppliers and partners. On this perspective, the application of this Policy is part of the broader frame of the corporate strategy and allows the Company to align business and procedures to higher information security standards and all applicable legal requirements.

Policy measures

With the aim of achieving these objectives, the Company voluntarily adopts and constantly evaluate the effectiveness of an Information Security Management System based on ISO/IEC 27001 standards aimed at achieving the following objectives:

- identification of risk areas and adoption of appropriate treatments;
- full compliance with the requirements of Data Protection Regulatory Frameworks of countries where it is operating;
- full compliance with the applicable contractual requirements;
- widespread awareness of the strategic value of security and information protection systems.

In particular, ISO 27002 practices – *Code of Practice for information security* – are used as a reference for the protection of information by applying the security methods deemed most appropriate to ensure the availability, confidentiality, integrity and verifiability of business information and considers adequate protection when the risk of violations is avoided or can be considered acceptable.

The Information Security Management System is based on a set of procedures for the treatment of assets within business processes (logical security) and within the context where such processes take place (physical security).

All employees are responsible for implementing and managing the security system and are informed and periodically updated on the procedures to follow.

The Company undertakes to spread the principles of this Policy by using internal and external communication channels.

Approval of Policy

Name: PRESIDENT AND CEO – Matteo Storchi

Date: October 2022

Signature: