Information Security Policy

Costruzioni Elettro Meccaniche Ing. Buzzi & C. – CEMB S.p.A (CEMB S.p.A) management with this document sets out the Information Security Policy specifying the objectives and commitments arising from it.
The general objectives for the Information Security Management System are as follows:

- to create and implement an Information Security Management System in compliance with all mandatory regulations, laws and decrees in force, and with the maturity standards to which the company has decided to adhere or to which Customers require adherence;
- to create a continuously improving market image and guarantee Customers "business continuity" without the risk of interruption caused by potential information security incidents;
- to reduce the damage caused by potential incidents.

These objectives are in line with the company's objectives, strategy and business plans.
The aim is to perfect procedures ensuring that the organisation operates more efficiently, improves the control and safety of its activities and achieves increasingly challenging objectives.
CEMB S.p.A provides machines (Balancing Machines and devices for vibration analysis) that manage data/information. The use of information resources shall be consistent with good working practices and procedures, as well as legal, regulatory and contractual requirements, and shall ensure the confidentiality, integrity and availability of all information resources of CEMB S.p.A and its Customers.
Information is an extremely important asset of CEMB S.p.A and enables it to fulfil its commercial functions and obligations towards its counterparties.
CEMB S.p.A Information Security Management System ensures that it meets the legal, regulatory and contractual requirements for information security, including those provided for by the personal data protection legislation (EU Reg 2016/679, Legislative Decree 101/18 and Legislative Decree 196/03) and the Italian Data Protection Authority.
In terms of Information Security, in detail:

- the approach will be risk-based in accordance with UNI CEI EN ISO/IEC 27001:2022 and best practice;
- the procedures will establish risk assessment criteria aligned with CEMB S.p.A current approved strategic business risk management policies.

It is the Management's precise intention and task to consolidate internal awareness towards the increasingly challenging objectives of information security, to strengthen the company's image and seriousness, above all through the search for transparency towards its Customers, the professionalism that is acknowledged to the company and an increasingly personalised and exclusive style.
It is therefore CEMB S.p.A firm intention to implement and follow this Information Security Policy so that it is permeated and implemented at all company levels. The Company undertakes to train its collaborators in this sense.
This Policy represents the commitment on which the Information Security Management System is based.
All business processes (primary and support) are affected by the guidelines and directions defined in this document.
All stakeholders must take appropriate security measures in line with the principles set out in this policy.
Failure to comply with or violation of the principles set out in this policy may result in disciplinary action against employees under the National Collective Bargaining Agreement, as well as taking all permitted civil and criminal legal actions, and for external stakeholders in the review of the contractual relationship between the parties up to and including termination of the contract.
In particular, the Management confers on the Information Security Management System Manager (ISMSM) the responsibility for ensuring the application of the provisions and establishments of the Information Security System and for keeping the Management informed of the results of periodic audits.
CEMB S.p.A Management will periodically review the company's current practices, policies and guidelines during the Management Review to recommend any changes or improvements to ensure that appropriate security measures are in place.
This Policy is a controlled document and is available to employees on the server on a read-only basis and to all stakeholders on the website. The Information Security Management System Manager (ISMSM) must ensure that all changes are disseminated and obsolete copies are removed and/or archived.
Together with this policy CEMB S.p.A has drawn up specific policies to regulate the following topics: incident management, business continuity management, password management, change management, Regulation on the correct Use of Company Assets, management of information backup and recovery.

Mandello del Lario 31/03/2023

On behalf of the Management of
CEMB S.p.A

Ing. Buzzi Carlo