elmeg

# INFORMATION SECURITY POLICY

The primary objective of the Management is to define information security policies, disseminate and share them within the organization, promote and support them externally.

Information security policies are developed in compliance with:

- business requirements
- regulations, standards, legislative requirements
- customer - contractual requirements
- internal prescriptions
- risk assessment in relation to the information managed

**Objectives of the Management:**

- Define the criteria and implement a methodology for assessing information security risks, thus determining the levels of acceptable risk and the intervention protocols, where necessary;
- Monitor and control the processes of the organization in order to evaluate the understanding of the policies, guarantee the adequacy and continuous improvement of the Management System through appropriate indicators and the definition of development objectives and targets;
- Define and assign responsibilities in relation to the tasks and the type of information;
- Define rules for access to networks and network services in relation to the activities performed and the classification of assets;
- Implement reaction plans in case of deviations;
- Periodically review the system and invest in the continuous modernization of the IT structure.

**Operating Policies** :

- **Implementation of policies** : employees, collaborators, suppliers, partners and all other third parties involved in Elmeg's activities fulfill their individual obligations and responsibilities, in order to protect information, assets and resources;
- **Access control:** access to information, assets and resources are controlled and monitored; access is authorized only for the necessary information (need to know); while access is authorized only for information regarding specific previously authorized activities;
- **Physical, environmental and logical security:** access to information, goods and resources is entrusted to authorized, trained and competent personnel. Furthermore, a monitoring system controls the access and authorization process. Inside the establishment, access to public communication channels (e.g. wi-fi) is permitted through a network dedicated to guests ("Guest"). The premises, destined to have computer equipment or archives, are identified and protected from unwanted access.
- **Data security in the design, development and industrialization of the product:** internal and external information is managed by specially trained personnel who are aware of the importance of the information managed.
- **External hosting:** data classified as internal can be archived using Tisax certified external hosting (Level 3 label).
- **Protection from malware:** the security system provides for various levels of filtering, through perimeter firewall and antivirus operating on individual assets;
- **Data protection and saving (backup):** all information is protected from voluntary and involuntary loss, through the implementation of saving procedures. Elmeg has developed a backup system that guarantees timely control, through the reporting of the events of the activities performed;
- **Privacy and protection of personal data:** Elmeg undertakes to implement the provisions of local laws and EU regulations on the matter;
- **Relations with suppliers, service companies:** the Management involves and makes its suppliers and the third parties with whom it collaborates responsible through specific Non Disclosure Agreements (NDA).

**La Direzione**
Gianluca Giordano