	Information Security Management System (ISMS)
	<b>COMPANY POLICY</b>

The **COMPANY POLICY** requires that, according to the company mission, the management of all business processes is set with the rules of the application of the Management System according to ISO/IEC 27001.

**PURPOSE AND OBJECTIVES**

Stamet's direction has defined, disclosed and undertakes to maintain this Information Security Management policy at all levels of its organization.

The purpose of this policy is:

to ensure the protection from imaginable threats, internal or external, intentional or accidental, of the information in the context of its activities in accordance with the indications provided by the ISO/IEC 27001 standard and the guidelines contained in the ISO/IEC 27002 standard in their latest versions.

**SCOPE OF APPLICATION**

This policy applies without distinction to all processes and at all levels of the Company.

The implementation of this policy is mandatory for all personnel and must be included in the regulation of agreements with any external entity that, for any reason, may be involved with the processing of information that falls within the scope of the Management System (ISMS).

The company allows the communication and dissemination of information to the outside only for the correct performance of business activities that must take place in compliance with the rules and mandatory regulations.

**INFORMATION SECURITY POLICY**

The information assets to be protected consist of all the information managed through the services provided and located in all company locations.

It is necessary to ensure:

- the confidentiality of information: i.e. information must only be accessible by those who are authorised.
- the integrity of information: i.e. protect the accuracy and completezza of information and the methods for its processing.
- the availability of information: i.e. that authorised users can effectively access the information and related goods at the time they request it.


The lack of adequate levels of security can lead to damage to the corporate image, lack of customer satisfaction, the risk of incurring penalties related to the violation of current regulations as well as economic and financial damage.

An adequate level of security is also essential for the sharing of information. The company identifies all security needs through risk analysis that allows you to become aware of the level of exposure to threats of your information system. The risk assessment makes it possible to assess the potential consequences and damage that may result from the non-application of security measures to the information system and what is the realistic probability of implementation of the identified threats.

The results of this assessment determine the actions necessary to manage the identified risks and the most appropriate security measures.

The general principles of information security management cover several aspects:

- There must be a constantly updated catalog of company assets relevant to the management of information and for each one a manager must be identified. Information must be classified

	Information Security Management System (ISMS)
	<b>COMPANY POLICY</b>

according to its level of criticality, so as to be managed with consistent and appropriate levels of confidentiality and integrity.

To ensure the security of information, all access to systems must be subject to an identification and authentication procedure. The authorizations of access to information must be differentiated according to the role and tasks held by individuals, so that each user can access only the information he needs, and must be periodically reviewed.

Procedures must be defined for the safe use of company assets and information and their management systems.

Full awareness of information security issues in all staff (employees and collaborators) must be encouraged from the moment of selection and for the entire duration of the employment relationship.

In order to be able to manage incidents in a timely manner, everyone must notify any safety-related issues. Each incident must be handled as indicated in the procedures.

Unauthorized access to the premises and individual company premises where the information is managed must be prevented and the security of the equipment must be ensured.

Compliance with legal requirements and principles related to information security in contracts with third parties must be ensured.

A continuity plan must be prepared that allows the company to effectively deal with an unforeseen event, ensuring the restoration of critical services in a time and manner that limits the negative consequences on the company mission.

Security aspects must be included in all phases of design, development, operation, maintenance, servicing and decommissioning of IT systems and services.

Compliance with the provisions of law, statutes, regulations or contractual obligations and any requirements concerning the security of information must be ensured, minimizing the risk of legal or administrative sanctions, significant losses or damage to reputation.

### **RESPONSIBILITY FOR COMPLIANCE AND IMPLEMENTATION**

Compliance with and implementation of policies is the responsibility of:

1- All personnel who, for any reason, collaborate with the company and are in some way involved with the processing of data and information that fall within the scope of the Management System.

All staff are also responsible for reporting all anomalies and violations of which they become aware.

2- All external subjects who maintain relationships and collaborate with the company. Must ensure compliance with the requirements contained in this policy.

The Manager of the Management System who, within the Management System and through appropriate rules and procedures, must:


conduct risk analysis with the appropriate methodologies and take all measures for risk management

establish all the rules necessary for the safe conduct of all business activities

verify security breaches and take the necessary countermeasures and control the company's exposure to the main threats and risks

organise formation and promote staff awareness of all matters relating to information security.

periodically verify the effectiveness and efficiency of the Management System.

	Information Security Management System (ISMS)
	<b>COMPANY POLICY</b>

Anyone, employees, consultants and / or external collaborators of the Company, intentionally or negligently, disregards the established safety rules and in this way causes damage to the company, may be prosecuted in the appropriate locations and in full compliance with legal and contractual obligations.

**REVIEW**

The Management will periodically and regularly or in conjunction with significant changes verify the effectiveness and efficiency of the Management System, in order to ensure adequate support for the introduction of all the necessary improvements and in order to encourage the activation of a continuous process, with which control and adaptation of the policy is maintained in response to changes in the business environment, of the business, of the legal conditions.

The Management System Manager is responsible for reviewing the policy.

The review will have to verify the status of preventive and corrective actions and adherence to the policy.

It will have to take into account all changes that may affect the company's approach to information security management, including organizational changes, the technical environment, the availability of resources, legal, regulatory or contractual conditions and the results of previous reviews.

The outcome of the review should include all decisions and actions related to improving the company's approach to information security management.

**MANAGEMENT COMMITMENT**

Management actively supports the security of information in the company through a clear address, an evident commitment, explicit assignments and the recognition of responsibilities related to information security.

The commitment of the management is implemented through a structure whose tasks are:

- ensure that all information security objectives are identified and that these meet business requirements;
- establish company roles and responsibilities for the development and maintenance of the ISMS;
- provide sufficient resources for the planning, implementation, organization, control, review, management and continuous improvement of the ISMS;
- check that the ISMS is integrated into all business processes and that procedures and controls are effectively developed;
- approve and support all initiatives aimed at improving information security;
- activate programs for the dissemination of awareness and culture of information security.

Feletto (TO)-Italy, **15<sup>th</sup> January 2021**

**General Manager**

