

COMPANY POLICY

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 immaginable 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:

J
☐ 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

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.

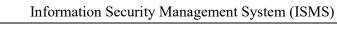
The results of this assessment determine the actions necessary to manage the identified risks and the most appropriate security measures.

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



COMPANY POLICY





COMPANY POLICY

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:

111	The communent 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;													
	establis	h con	npan	y roles and r	esponsibi	lities for the	e dev	elopment a	and n	nainte	enance	of the	ISMS;

provide sufficient resources for the planning, implementation, organization, control, review, management and continuous improvement of the ISMS;

 \Box 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;

 $\hfill \square$ activate programs for the dissemination of awareness and culture of information security.

Feletto (TO)-Italy, 15th January 2021

General Manager

