 Bruschi	TISAX Management System
	TISAX BRUSCHI POLICY

The **Company Policy** requires that, in line with the company mission, the managing of all company processes is set up with the rules of the application of the TISAX Management System, developed taking into consideration also the ISO/IEC 27001 standard and the therein expected controls.

PURPOSE AND OBJECTIVES

The management of Bruschi SpA has defined, disseminated, and is committed to keeping this information security management policy active at all levels of its organization.

The purpose of this policy is to ensure **maximum customer satisfaction** in the use of our services and the **protection from all threats, internal or external, intentional or accidental, of information in the context of our activities** in accordance with the indications provided by the TISAX standard.

FIELD OF APPLICATION


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

The implementation of this policy is mandatory for all personnel, and it must be included in the regulation of agreements with any external subject who, for whatever reason, may be involved with the processing of information that falls within the scope of application of the TISAX Management System.

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

It is necessary to ensure the following:

- The **confidentiality** of information: that is, the information must be accessible only by authorized people.
- Information integrity: that is, protecting the accuracy and completeness of the information and the methods for processing it.

 Bruschi	TISAX Management System
	TISAX BRUSCHI POLICY

- The **availability** of information: that is, authorized users can effectively access the information and related assets when 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 damages of an economic and financial nature.

An adequate level of security is also essential for sharing information.

The company identifies all security needs through the analysis of the risks looming over its corporate assets, which allows it to acquire suitable awareness of the level of exposure to threats. The risk assessment makes it possible to evaluate the potential consequences and damages that may derive from the failure to apply 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 suitable security measures.

The principles of information security management embrace the following aspects:

1- ALWAYS UPDATED ASSET INVENTORY - Guarantee a constantly updated catalog of company assets relevant to information management purposes, and assign a manager for each. The information must be classified according to its level of criticality so as to be managed with consistent and appropriate levels of confidentiality and integrity.

2- UPDATED INFORMATION RISK ASSESSMENT - The information risk assessment is updated at least once a year upon management review or in case of adverse events or in case there is an adjustment of the asset inventory.

3- SECURE SYSTEM ACCESS - To ensure information security, every access to the systems must undergo an identification and authentication procedure. Information access authorizations must be differentiated according to the roles and tasks individuals cover so that each user can access only the information he needs and must be periodically reviewed.

 Bruschi	TISAX Management System
	TISAX BRUSCHI POLICY

4- SAFE USE OF COMPANY ASSETS - Procedures must be defined for the safe use of company assets and information and their management systems.

5- CONTINUING PERSONNEL TRAINING - Full awareness of information security issues must be encouraged in all personnel (employees and collaborators) starting from the moment of selection and for the entire duration of the employment relationship.

6- TIMELY HANDLING OF ADVERSE EVENTS - To handle incidents in a timely manner, everyone must report any safety-related issues. Each incident must be managed as indicated in the procedures.

7- ADEQUATE PHYSICAL PROTECTION OF THE COMPANY OFFICES - It is necessary to prevent unauthorized access to the offices and individual company premises where the information is managed, and the safety of the equipment must be guaranteed.


8- MANAGEMENT OF CONTRACTUAL COMPLIANCE WITH THIRD PARTIES - Compliance with legal requirements and information security principles in contracts with third parties must be ensured.

9- BUSINESS CONTINUITY PLAN SIMULATIONS - A continuity plan must be prepared which allows the company to deal effectively with an unforeseen event, guaranteeing the restoration of critical services in time and in ways that limit the negative consequences on the company mission.

10- IT SECURITY BY DESIGN - The security aspects must be included in all phases of design, development, operation, maintenance, assistance, and decommissioning of IT systems and services.

11- CONTINUOUS LEGISLATIVE UPDATE - Compliance with the provisions of the law, statutes, regulations, or contractual obligations and with any requirement concerning information security must be guaranteed, minimizing the risk of legal or administrative sanctions, significant losses, or damage to the reputation.

12- PERIODICAL PENETRATION TESTS - Periodic penetration tests must be performed on the infrastructures and applications to assess the resilience of the systems to external attacks and to identify any vulnerabilities and allow for their subsequent fixing.

 Bruschi	TISAX Management System
	TISAX BRUSCHI POLICY

RESPONSIBILITY FOR COMPLIANCE AND IMPLEMENTATION

Compliance with and implementation of the policies are the responsibility of:

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

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


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

The Management System Manager, through appropriate rules and procedures, must:

- conduct risk analysis with proper methodologies and adopt all risk management measures
- establish all the rules necessary for the safe conduct of all company activities
- verify security breaches and take necessary countermeasures and control the company's exposure to key threats and risks
- organize training and promote staff awareness of everything related to information security
- periodically check the effectiveness and efficiency of the Management System.

Whoever, 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 offices and in full compliance with the legal and contractual obligations.

REVIEW

 Bruschi	TISAX Management System
	TISAX BRUSCHI POLICY

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

The Management System Manager is responsible for reviewing the policy.

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

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

The result of the review shall include all decisions and actions relating to the improvement of the company's approach to information quality and security management.

MANAGEMENT COMMITMENT


Management actively supports information security in the company through clear direction, clear commitment, explicit assignments, and acknowledgment of responsibilities related to information security.

The management's commitment is implemented through a structure whose tasks are:

ensure that all information security objectives are identified and meet business requirements;

establish corporate roles and responsibilities for developing and maintaining the TISAX Management System;

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

 Bruschi	TISAX Management System
	TISAX BRUSCHI POLICY

check that the TISAX Management System is integrated into all company processes and that procedures and controls are effectively developed;

approve and support all initiatives aimed at improving the quality and security of information;

activate programs for the dissemination of information security awareness and culture.

Milan, **20/03/2023**

CEO

Paul Rastelli