Elaboration and Verification	Approval and Issuance
System Administrator Aron Marinescu	CEO Matteo Saltarello
Signature ----------	Signature ----------
Date 20 12 2022	Date 14 04 2025

Rev	Reason	Description of Changes
01	Emission	First emission
02	Revision	Document classification according to the Document Classification Procedure rev.3
03	Revision	Eng Translation

The Management of Touch & Contact, aware of the importance and necessity of implementing an internationally recognized Information Security Management System (ISMS), to ensure the quality of the services provided and to pursue customer satisfaction, considers it appropriate to make its Information Security Management System compliant with the ISO/IEC 27001:2022 standard.
The primary objectives of this corporate information security policy are as follows:

- Provide all necessary resources to meet applicable regulatory requirements and ensure continued legal compliance over time.
- Commit to the continuous improvement of the ISO/IEC 27001:2022 management system.
- Monitor factors emerging from risk assessment and initiate all possible actions to eliminate or reduce risks.
- Seize opportunities offered by technological evolution, consistent with the company's financial needs, to achieve continuous improvement of the management system.
- Effectively identify all potential threats and vulnerabilities to eliminate or reduce incidents deriving from them.
-
- Monitor cloud services on which the company's business continuity depends.
- Simulate information security incidents to verify response capability in terms of timeliness and effectiveness.

- Implement all possible actions to preserve the integrity, availability, and confidentiality of any asset belonging to Touch & Contact.
- In order to pursue these primary objectives, the following are some examples of initiatives promoted within the company:
- Assign responsibility for the control of corporate assets to personnel, ensuring that everyone, in ways pertinent to their role and function, is involved and participates in protecting Touch & Contact's information assets.
- Establish control methods for the external transfer of corporate assets.
- Ensure that the disposal of any corporate asset does not result in a loss of confidentiality of any information it may contain.
- Control access for visitors to corporate offices and all access to any corporate information by personnel or third parties in any capacity.
- Ensure that all workstations have password-protected access, with passwords regularly updated.
- Define and periodically test effective backup procedures.
- Establish mutual responsibilities for information security management with clients and suppliers.
- Periodically verify the effectiveness of the business continuity and disaster recovery plan.

All personnel, collaborators, suppliers, and visitors must operate in compliance with company rules and procedures established to ensure business management in accordance with the aforementioned principles.

The Management hopes to achieve, at all levels, maximum collaboration in respecting and systematically applying these general guidelines.