It is an essential priority for BaseCRM to achieve a level of security in its products and services that ensures adequate protection of information, so that all its customers can use it with the utmost confidence.

Accordingly, BaseCRM Management has defined and implemented an Information Security Management System (ISMS) that enables the company to ensure that its information systems and the information they process and store comply with the following principles:

- Confidentiality: information belonging to BaseCRM must be known exclusively to authorised persons, following identification at the appropriate time and through the means provided.
- Integrity: information belonging to BaseCRM must be complete, accurate and valid, and its content must be that provided by the persons concerned, without any manipulation.
- Availability: information belonging to BaseCRM must be accessible and usable by authorised and identified users at all times, with its continued existence guaranteed against any foreseeable eventuality.
- Traceability: all actions performed on information belonging to BaseCRM are unambiguously associated with an individual or entity.
- Authenticity: BaseCRM guarantees that an entity is who it claims to be or guarantees the source from which the data originate.

The scope of the ISMS covers the information systems supporting the Development, Installation and Maintenance of the BaseCRM Solution.

The Information Security Model implemented at BaseCRM is based on the international standard ISO/IEC 27001:2022 and is set out in the General Information Security Policies Manual. This manual and the set of security policies, procedures, instructions and guidelines established to protect the organisation's information assets against internal or external, deliberate or accidental threats constitute BaseCRM's Internal Information Security Regulatory Framework.

Management assumes responsibility for providing the appropriate material and human resources to establish and implement the organisational, technical and control measures necessary to meet the information security requirements specified in BaseCRM's Internal Information Security Regulatory Framework.

The Security Policies will be maintained, updated and adapted to BaseCRM's purposes and aligned with the organisation's context and risk management strategy, within which the ISMS will be maintained. To this end, a process for analysing and managing information security risks has been established.

Management will promote an appropriate level of technical capability through staff training and awareness, and undertakes to review and continuously improve the ISMS implemented in the company.

Management undertakes to meet the overall information security objectives established annually and to comply with the legal and regulatory requirements affecting BaseCRM. Specifically, the overall security objectives established by the organisation are:

- Carry out appropriate risk assessment, management and treatment, in order to progressively reduce the Risk Criticality Index.
- Maintain and continuously improve the internal information security regulatory framework, incorporating information security policies and processes that are mandatory throughout the organisation, and verify that this framework is applied.
- Maintain an organisational framework and allocation of information security responsibilities that ensures employees and third parties involved know and understand their information security responsibilities and that these responsibilities are appropriate to the functions assigned to them.
- Protect information assets by adopting the controls most effective in preserving their confidentiality, integrity, availability, traceability and authenticity.
- Ensure that information security is an integral part of information systems throughout their life cycle (acquisition, development and maintenance).
- Ensure prompt, effective and appropriate management of information security incidents, events and weaknesses.
- Promote proper compliance with legal, statutory or contractual obligations relating to information security or security requirements.

This Policy will be communicated to everyone concerned within the scope of the ISMS and will be available to interested parties for consultation.

Approved on 1 December 2025. Revision 0.0

Signed: Management