INFORMATION SECURITY POLICY

PUBLIC VERSION

Security Governance represents a key point for the growth of GM Software's business, and its positioning on the market, considering its influence on:

- preserve company assets;
- support the strengthening of the GM Software's role within the reference market;
- achieve business results by increasing levels of effectiveness and efficiency while optimizing resources;
- increase customer trust.

Therefore, defining an Information Security Management Policy is a strategic point to support and ensure the objectives that can be achieved.

GM Software is committed to implementing an Information Security strategy, based on protecting the confidentiality, integrity, and availability of all physical and logical information assets of the company, in order to ensure compliance with regulatory, operational, and contractual requirements.

In particular, the main objectives of Information Security to be addressed are:

- **Confidentiality:** ensure that information is accessible only to those authorized to access it;
- **Integrity:** safeguarding the accuracy and completeness of information and processing methods;
- **Availability:** ensure that authorized users have access to information when needed.

The general objectives of Information Security include the following:

- Ensure compliance with current national laws, regulations and related guidelines,
- Ensure a level of security of the network and information systems appropriate to the existing risk, taking into account of the following elements:
    a) risk assessment and information systems security policies;
    b) security of systems and plants;
    c) information security event and incident management;
    d) business continuity management;
    e) supply chain security;
    f) security of the acquisition, development and maintenance of information and network systems;
    g) strategies and procedures for evaluating the effectiveness of cybersecurity risk management measures;
    h) information security training and awareness campaigns to support the objective’s achievement
    i) human resources security, access control strategies, and asset management.
- Be aligned with the internal policies of GM Software concerning organizational and technical protection of technological infrastructure
- Establish controls to protect the GM Software's information systems and information from theft, misuse, and other forms of damage and loss;
- Motivate all employees to improve their security awareness in order to protect and safeguard GM Software data;
- Ensure that GM Software is able to provide continuity of its services, even if major security incidents occur
- Ensure the availability and reliability of the network infrastructure and the continuity of the essential services provided and managed by GM Software

- Comply with the methodologies of international standards for Information Security, particularly those of the ISO/IEC 27001 standard;
- Ensure flexibility and an adequate level of security for access to information systems.
- Ensure a continual improvement process aimed to evaluate opportunities to increase effectiveness of the information security management system.

GM Software's security vision is based on protecting information assets, managing security risks, and effectively and efficiently implementing business strategies, supported by operational leadership and embraced by all GM Software employees.

Top Management of GM Software demonstrates the commitment to maintain and improve the ISMS defined, implemented and operated since 2008 and for which it has obtained certification of compliance to ISO/IEC 27001:2013, now updated to ISO/IEC 27001:2022 version; the principles and policies are defined and supported by procedure, forms and any documented information that is managed during the lifecycle of the management system. Particularly, top management aims to maintain the level of security through the following actions:

- providing adequate resources (people, time and economic/financial resources) to develop and maintain the ISMS (Security Committee 27001) and at the same time to keep certification according to current regulations (including through the involvement of consultants as an expert judgement)
- assigning and providing adequate autonomy and responsibility to the current (and future) IT & Security Manager and QA & CSV Manager in defining the activities, infrastructures, procedures and documentation of QMS and related activities
- by approving the policies and procedures identified for different business areas, improving sharing across organisational areas (awareness) using appropriate tools
- providing appropriate internal training and where necessary externally to resources interacting with ISMS (i.e. regular suppliers)
- by approving the management of ISMS and Risk Management by the definition of policies, procedures and methodologies for risk assessment and treatment as well as incidents management and corrective actions application
- by approving identified threats and planned controls as well as approving residual risks in the Risk Assessment Report
- by approving the definition and the tasks/resources required for the ISMS, which has as its main objective that:
    - manage protection from internal and external threats, intentional and accidental behaviours related to customer’s data and for relations with suppliers;
    - maintain and demonstrate the integrity of relationship with customers and suppliers;
    - improve reputation and trust of GM Software in the market;
- maintaining the ISMS and its certification against ISO/IEC 27001.
- specializing the ISMS towards protection of personal data to address compliance with Regulation UE 679/2016 (GDPR)

Date: 23/09/2025