Logical Security Policy of Banca Monte dei Paschi di Siena

To safeguard its digital assets, Banca Monte dei Paschi di Siena S.p.A. has implemented a Group-wide "Information Security Management System" (ISMS) that provides general and strategic guidance for the medium and long term, in accordance with the leading international ISO/IEC 2700x (series) standards.

In this context, the guidelines for the overall Logical Security Management process are defined as follows:

- establishing strategies and policies, along with monitoring and overseeing logical security measures to protect the company's digital assets in line with the risk objectives and operational limits outlined in the Risk Appetite Framework (RAF). This includes developing measurement and evaluation frameworks to assess the achievement of targets;
- managing operational and security incidents;
- monitoring the effectiveness of implemented information security measures to ensure continuous improvement;
- developing and overseeing the Information Security Training and Awareness Plan;
- defining and monitoring security measures and control mechanisms for outsourced or third-party IT services;
- implementing defined security measures and managing security platforms on an ongoing basis;
- ensuring compliance with legal provisions relating to cybersecurity, including mandatory regulations such as GDPR and Bank of Italy Circular 285.

The above principles also apply to third parties (such as suppliers, consultants, etc.) operating within the Montepaschi Group in relation to their specific activities.

Logical Security Governance is closely integrated with various elements and processes within the organisation, including ICT and Security Risk Management, Business Continuity Management, IT Service Continuity and Incident Management).

Below are the main areas of application, aligned with the ISO 27001 domains:

- **Information security policies**: General directives, guidelines and objectives have been established as reference points for all information security regulations.
- **Information Security Organisation**: Roles and responsibilities related to information security are defined to ensure clear segregation of duties and potentially overlapping areas of responsibility. Relevant security frameworks and indicators are also defined to guide, control and monitor the protective measures and to safeguard the general principles of the MPS Group. In addition, ongoing communication with relevant authorities and industry associations is maintained to ensure continuous alignment and information sharing.
- **Human resources management**: Every employee of the Montepaschi Group, as well as any third party involved in the Group's processes, must remain constantly vigilant regarding information security. They are required to implement appropriate security measures at every stage of their work, as defined in the Group's Logical Security Policy. In addition, all personnel, including those in key positions, receive appropriate training on ICT risks and security, including information security.
- **Management of corporate assets**: Every corporate asset must be assessed against at least the parameters of CIA (Confidentiality, Integrity and Availability), with the addition of accountability. All IT resources, including hardware, software, processes and data/information belonging to the MPS Group are considered corporate assets and must be protected accordingly.
- **Access Control**: The management of access to the ICT systems and applications of the Montepaschi Group is determined on the basis of the operational activities performed by users, in accordance with their role and in compliance with the defined security measures. Access control procedures are implemented, monitored and regularly updated and include checks to detect anomalies and appropriate countermeasures to prevent unauthorised access to data.
- **Data security**: Systems and processes are in place to ensure the confidentiality, availability and integrity of information, such as encryption;
- **Physical and environmental security**: Physical access to the company's central facilities by employees and visitors (including suppliers, collaborators or customers) is authorised, tracked and monitored to prevent unauthorised access.
- **Operational security**: Structures, processes and tools are in place to protect the availability, integrity and confidentiality of company data.
- **Communication security**: Technical security solutions are used to ensure:
  - The protection of internal and external network traffic and services provided;
  - The security of customer access to services provided through self-banking channels and of transactions carried out through these channels.

- **Acquisition, development, and maintenance of the information system**: The development, acquisition and maintenance of reliable and secure application and infrastructure systems are ensured. Suppliers involved in software/hardware development and maintenance activities are required to follow defined processes in accordance with the MPS Group's security policy.
- **Third-party security**: MPS adopts a third-party governance framework aimed at assessing the security of outsourced services, processes and solutions provided by external vendors.
- **Management of cyber security incidents**: Specific responsibilities and processes are established to ensure a prompt, effective and orderly response to security incidents, including cooperation with law enforcement and other relevant operators or entities, particularly in the case of information breaches.
- **Business continuity management**: An organisational business continuity management model is in place to mitigate the impact of adverse events, including catastrophic events, and to restore normal operations based on pre-defined levels.
- **Information Security Management System (ISMS) compliance**: Security levels are maintained through continuous monitoring of the effectiveness of existing security measures and periodic reviews of the overall ISMS.