INFORMATION SECURITY POLICY
MERLIN PROPERTIES, SOCIMI, S.A.

April 2023

The Board of Directors of MERLIN Properties, SOCIMI, S.A. (hereinafter "**MERLIN",** the "**Group**" or the "**Company**") has approved this Information Security Policy (hereinafter also the "**Policy"),** following a report from the Appointments and Remuneration Committee and at the proposal of the Sustainability and Innovation Committee, which establishes the general principles of action with which MERLIN will protect its information in accordance with the applicable regulations at all times and with its ethical values, defined in the **Code of Conduct**, as well as with the provisions of other applicable internal regulations.

1. General aspects and scope of action

MERLIN will ensure the protection of information, regardless of the form in which it is communicated, shared or stored (hereinafter, the "**Information**"). This protection affects both information within the Group and information shared with third parties.

In this sense, Information Security is understood to be the safeguarding and protection of (i) the Information owned by the Group, regardless of whether it is in its own systems or those of third parties; and (ii) the information owned by third parties, which is found in the Group's systems.

For the purposes of this Policy, Information Systems is understood to be the set of technologies or technological means, owned by the Group or by third parties that manage, store or transmit Information (including cloud technologies or similar).

MERLIN is committed to establishing and maintaining an adequate **Information Security Management System** (also known as "**ISMS"),** in accordance with and based on the international standard ISO 27001.

The Information Security Management System preserves the confidentiality, integrity and availability of information by implementing a risk management process and gives confidence to stakeholders that risks are properly managed.

MERLIN's Information Security Management System encompasses all the information systems that support the activities carried out by the Group, such as the acquisition, sale, development, rehabilitation and operation of urban real estate for lease in Spain and Portugal.

This Policy applies to all employees, managers and directors of all the companies that make up the Group, including those investee companies over which it has effective control, within the limits provided for in the applicable regulations.

In those investee companies in which the Group does not have effective control, the representatives of MERLIN, within the scope of their possibilities, shall propose principles and guidelines consistent with those established in this Policy.

The application of the Policy may be extended, in whole or in part, to any other natural and/or legal person linked to the Group by a relationship other than employment when this is possible due to the nature of the relationship and is convenient for the fulfilment of the purpose of the same.

In accordance with the Policy, MERLIN may develop procedures to implement and ensure compliance with the obligations assumed, as well as to adapt it to the various legislations applicable to the Group.

Likewise, the application of **this Policy is complementary to other mandatory internal regulations**, such as:

- The Internal Regulations of Conduct of the Securities Market
- The Manual of Criteria and Procedures for the Communication of Information
- The Personal Data Protection Policy.
- The Personal Data Retention Regulations
- Manual for the use of Information Systems and Personal Data.

2. Objectives of the Policy

This Policy constitutes the **reference framework** by which MERLIN defines the guidelines for the effective protection of the information managed by the Group:

- **Guaranteeing the necessary degree of confidentiality** for each type of Information, in accordance with the classification established in the Information Classification Procedure.

- **Maintaining the integrity of the information**, so that it does not suffer alterations with respect to the time when it was generated by the owners or those responsible for it.

- **Ensuring the availability of the Information**, in all media and whenever necessary, ensuring business continuity and compliance with any obligations required of the Company.

3. Fundamental principles of the Policy

In pursuit of the above, MERLIN's fundamental principles of commitment are as follows:

- **Information security**: ensuring that security is an integral part of the information systems lifecycle through proper management of risks and weaknesses associated with systems.
- **Protection of systems and information**: protecting the information generated, processed or stored by the different processes, their technological infrastructure and assets, against threats from internal or external sources to the organization, ensuring that the principles of confidentiality, integrity, availability, and legality of information are complied with.
- **Classification of Information**. The information will be classified according to its value, importance and criticality for the business, so that the protection measures are adapted to the classification level of each information asset. Similarly, the classification of Information assets will be carried out taking into consideration legal and operational requirements and good practices and standards in this regard.
- **Segregation of duties**. Concentrations of risks arising from the absence of segregation of duties and the one-person dependence on business-critical functions should be avoided.
- **Information and communication**: Inform all employees of their roles, obligations and responsibilities in terms of information security and protection of personal data, as well as their obligation to report possible security incidents.
- **Access to information by third parties**: developing procedures to control the availability and access by third parties to the Information relating to MERLIN or any other third party related to the Group, encouraging communication and collaboration with interested parties.
- **Continuous improvement**: adopting continuous improvement as a strategic value and its application in all aspects of MERLIN's management, carrying out the necessary internal audits, implementing the appropriate actions and establishing the appropriate Objectives.
- **Continuity**: establishing a process for managing the continuity of information systems to ensure the recovery of the Group's critical systems and information, reducing downtime to acceptable levels.
- **Compliance**: Information systems must comply with legal and contractual requirements, as well as any other requirements that Merlin subscribes to.

4. Information Security Governance

To ensure the correct implementation of this Policy, MERLIN considers it essential to establish clear responsibilities for both supervision and implementation, being aware of the transversality that is implicitly associated with these issues.

The body responsible for Information Security is the **Board of Directors**, as the Group's highest decision-making body, which has set up the Sustainability and Innovation Committee, as a permanent internal body, of an informative and consultative nature, without executive functions, with advisory, information and proposal powers regarding technological risks.

The **Sustainability and Innovation Committee** is responsible for promoting innovation, especially in relation to digitalization and technology, for the sustainable evolution of the Company and its group, making proposals to the Board of Directors on action plans and their implementation, in coordination and consultation with the executive team.

For its part, the **Management Team** of MERLIN Properties is responsible for the transfer and integration of the guidelines and commitments contained in this policy in the decision-making and daily management of the company's activities. The management team is also responsible for the allocation of resources to comply with the commitments set out in this policy.

In addition, MERLIN has an **Information Security Committee** made up of the CEO and other members of the Management Team, whose objective is to ensure that good practices in security management are applied effectively and consistently throughout the Group. Among other functions, this committee assumes responsibility for overseeing the information security strategy, including budgets, investment and resources in security.

The **Information Security Officer** will exercise his/her control function independently, being his/her responsibility to implement this policy and monitor its compliance, as well as that of all the requirements derived from the laws, regulations and good practices in the field of Information Security that are applicable. Therefore, it is responsible for implementing a security strategy, supervising access controls, segregation of duties and, among others, ensuring adequate protection of information systems against physical, digital or environmental threats.

Finally, all **Group Employees** must know, assume and comply with the Policy, as well as the internal regulations on security and use of the systems in force, being obliged to maintain professional secrecy and confidentiality of the information handled in their work environment and must communicate, as a matter of urgency and according to the established procedures, possible incidents or security problems that are detected.

5. Control and auditing

MERLIN expressly reserves the right to adopt, in a proportional manner, the necessary surveillance and control measures to verify the correct use of the Systems it makes available to its employees, including the content of communications and devices, respecting, in all cases, the legislation in force and guaranteeing the dignity of the employee. The communication of this Policy will have the effect of prior notification to the worker.

The Group will undergo periodic reviews and controls, as well as internal and external audits, to assess overall compliance with this Policy.

The assessment of a possible breach of this Policy will be determined in the corresponding procedure, in accordance with the provisions in force, without prejudice to the legal responsibilities, including those of a punitive nature in the field of employment, which, where appropriate, may be enforceable.

6. Policy Communication

This Policy will be available to all employees and will be available to all the Company's stakeholders on the corporate website. Likewise, the Policy will be subject to appropriate communication, training and awareness-raising actions for its timely understanding and implementation.

7. Policy Update and Review

This Information Security Policy has been approved by the Board of Directors of MERLIN Properties in April 2023, entering into force at the time of its approval and being fully in force as long as there are no modifications to it.

The Board of Directors, through its Executive Committees, and particularly through its Sustainability and Innovation Committee and the Information Security Committee, will supervise the correct implementation and compliance with all the principles of action and commitments set out.

In the event of this, the modifications made to the Information Security Policy will be applicable from the day following their communication to all the people affected by this Policy.