RISK MANAGEMENT AND CONTROL POLICY
MERLIN PROPERTIES SOCIMI, S.A.

June 2026

The Board of Directors of MERLIN Properties, SOCIMI, S.A. (hereinafter, "**MERLIN",** "**the Group**" or "**the Company**"), has overall responsibility for risk supervision and for the existence of an effective system for risk management and internal control of the company. Therefore, the Board Regulations establish in Article 4 "General Function of the Board", those functions legally or statutorily reserved to MERLIN's Board of Directors, including the approval of the risk management and control policy and the periodic monitoring of the information and control systems. The Board of Directors, aware of the importance of this aspect, establishes, through this **Risk Management and Control Policy** (hereinafter, "**the Policy**"), with the proposal of the Audit and Control Committee, the basic mechanisms and principles for the proper management of the key risks faced by the Company.

This Policy will help the organization to achieve the strategic objectives set and identify opportunities for improvement, as well as respond to the challenges in the development of its activity in an increasingly changing environment.

The **Audit and Control Committee**, in accordance with its own Regulations is responsible for supervising everything related to the different types of risk faced by the Company, including financial or economic risks, contingent liabilities, other risks (a) off-balance sheet, (b) operational, (c) social, environmental and technological, (d) governance and talent management risks, (e) legal, and (f) political and reputational, in collaboration with the **Sustainability and Innovation Committee** and the **Appointments and Remuneration Committee**, in matters of competition.

MERLIN's Risk Management System is aligned with the international reference standards on risk management (**COSO ERM 2017** ***Enterprise Risk Management Framework – integrated with strategy and performance***) and is based on a model that identifies the Company's key Risk events, evaluates them based on the Impact and Probability of occurrence, considering the Controls in operation and monitors and reports its evolution periodically.

MERLIN's Management is responsible for leading, implementing, transmitting and managing the strategy and resources that make up the Risk Management System and assumes as a fundamental commitment to assure an adequate level of independence, based on the following principles:

- To consider Risk as any threat that an event, action or omission may prevent MERLIN from achieving its objectives, executing its strategies successfully, the correct execution of its operations or the loss of opportunities.
- Establish mechanisms for adequate Risk Management, considering its identification, evaluation, response, follow-up and reporting.
- Promote and implement the strategy, culture, resources and processes that constitute Integrated Risk Management, which will be reviewed periodically to adapt it to the situation of MERLIN and its environment.
- To attribute, among the different levels of the Organization, the responsibility of identifying, analyzing, assessing, evaluating and supervising the Risk Management System.
- To promote the establishment and implementation of guidelines, limits and mechanisms that contribute to Risk Management being carried out in accordance with the Risk Appetite accepted by the Company.
- To promote and disseminate, through training and communication, the Risk Management System, guaranteeing the dissemination of this Policy, together with the documentation that develops it.

1. Principles for Risk Management in MERLIN

Risk Management and Control is considered as a continuous process composed of a series of stages within which certain activities must be carried out. The system focuses its action on **10 basic principles** or steps:

1. Know MERLIN's strategic and business objectives.
2. Know MERLIN's control environment (which involves assessing factors such as processes, procedures, human resources involved, technological infrastructure, current regulations applicable to the Company's activities, etc.).
3. Perform an analysis of potential risks, i.e., identify activities, processes, locations, etc. (i.e., identify all activities in the same process).
4. Determine the critical response and control points of the key risks, i.e., identify the hazards present in each activity, process, place, etc., evaluate the existing controls, if any, and define which aspects of the process are critical and should be monitored.
5. Establish the maximum limits for each critical control point (which risks are tolerable and which are not). To do this, it is necessary to analyze the impact that the materialization of the risk would have and the probability of it occurring.
6. Establish a surveillance and control system for these critical points.
7. Recommend corrective action to be taken when monitoring

indicates that a particular critical point is outside the established limits (such measures may include mitigating the risk, accepting it, avoiding it, transferring it, etc.).

8. Implement or put into practice the measures adopted, where appropriate.
9. Establish monitoring procedures to verify the operation of the system and structure a documentation system on all appropriate procedures and records for these principles and their application.
10. Periodically assess the risks in the environment to detect new threats (monitoring that starts the cyclical process again).

2. Methodology for Risk Management and Control

The Merlin Group's Risk Management System, based on the principles, key elements and methodology set out in the **COSO Framework** ("***Committee of Sponsoring Organizations of the Treadway Commission***"), aims to minimize the volatility of results (profitability) and therefore maximize the Group's economic value, incorporating risk and uncertainty into the decision-making process to provide reasonable assurance in the achievement of the established strategic objectives, providing shareholders, other stakeholders and the market in general with an adequate level of guarantees that ensure the protection of the value generated.

Based on an integrative view of Risk Management, MERLIN has adopted a methodological approach based on the **Enterprise Risk Management Framework – integrated with strategy and performance (COSO 2017),** which clarifies the importance of enterprise risk management in strategic planning and incorporates it throughout the organization, since risk influences strategy and performance in all areas, departments and functions.

3. Company bodies that carry out Risk Management and Control

MERLIN is subject to various risks inherent to the different businesses in which it operates and the activities it carries out. In this regard, the Board of Directors considers Risk Management as an instrument that contributes to achieving greater efficiency and effectiveness in its operations.

The Board of Directors is the governing body responsible for setting the levels of risk that it considers acceptable, aware of the importance of this aspect, establishes, through this Policy, the basic mechanisms and principles for the proper management of the key risks it faces, and all this to:

- ✓ promote the fulfilment of the proposed business objectives;
- ✓ avoid losses derived from the materialization of risks;
- ✓ preserve the image and reputation of the Company and its brand;
- ✓ ensure the continuity in the analysis and detection of possible threats and new risks to analyze their impact and probability of occurrence.

For the development of Risk Management and Control, the Board of Directors has the collaboration of the Audit and Control Committee, which supervises and reports on the adequacy and effectiveness of the Risk Management and Control system.

In this regard, the **Audit and Control Committee** supports the Board in the supervision of the risk management system and is the body responsible for reviewing the effectiveness of the risk management and internal control system during the year, with the support of the Internal Audit Department.

The Audit and Control Committee is the governing body responsible for overseeing all matters relating to the different types of risk faced by MERLIN, including financial or economic risks, contingent liabilities, other off-balance-sheet, operational, environmental, technological, legal, social, political and reputational risks. Likewise, the Audit and Control Committee must evaluate, at least annually, the list of the most significant financial and non-financial risks and the level of tolerance established for each one based on the information provided by Management.

The **Appointments and Remuneration Committee and the Sustainability and Innovation Committee**, in coordination with the Audit and Control Committee, will be responsible for identifying and supervising governance, environmental and social risks, within the scope of action of each one.

The **Risk Committee,** made up of representatives of the different business and corporate areas, is a body dependent on the Audit and Control Committee that coordinates the work of first-line risk owners and supervises the design of second-line controls. This Committee is responsible for the coordination of risk management, integrating the information received from the different direct managers of risk management and reporting to the Board of Directors on a semi-annual basis together with the update of the Risk Map.

For its part, the **Operating Committee (OpCo)** is responsible for day-to-day risk management, which includes the identification, evaluation and mitigation of risks, as well as the design and implementation of action plans and evaluation of the internal control system, ensuring its operational effectiveness. MERLIN believes that the entire company must be actively involved in risk management, with MERLIN's

Management being responsible for leading, implementing, transmitting and managing the strategy and resources that make up the Risk Management System.

Finally, the **Internal Audit Directorate**, as a third line of defense, is responsible for the audit and supervision of the MERLN Risk Management System as a whole.

Segregation of duties in Risk Management and Control at MERLIN

	Board of Directors	Commission of Audit and Control	Sustainability Committee	Appointments and Remuneration Committee	Senior Management and Management	Risk Committee	Address of Internal Audit	Other Employees
Risk Identification		X	X	X	X	X		X
Definition level of Tolerance	X							
Evaluation of Risks					X	X		
Execution Action Plans					X			X
SGR Monitoring	X	X	X	X		X	X	
Reporting and Control					X	X	X	X

Merlin's Audit and Control Committee will carry out the functions in terms of supervision of risk management and financial and non-financial information that have been delegated to it by the Board of Directors.

Coordination between Committees

For their part, and in accordance with their respective Regulations, the Appointments and Remuneration Committee and the Sustainability and Innovation Committee are entrusted with the supervision of non-financial and sustainability information within the respective areas of action.

In this regard, both Committees, in coordination with the Audit and Control Committee, will be responsible for the identification and

supervision of governance, environmental and social risks, as well as for the supervision of non-financial information relating to the Group's governance, the environmental performance of assets, climate change management, the responsible use of resources, and the management of resources. the management of interest groups, the social impact of activities, the organization of work and employment, compliance with human rights, among others.

4. Model of the 3 lines of defense

For risk management, MERLIN applies the model of the three lines of defense, consistent with the COSO methodology and the positioning of the Institute of Internal Auditors, whereby the roles and responsibilities in risk management are structured in three clearly differentiated areas:

- **The first line** corresponds to the business managers (Operating Committee, Business Divisions and Executive Functions) who are responsible for maintaining effective internal control and executing risk control procedures on a constant basis on a day-to-day basis. In this sense, they are responsible for identifying, evaluating, controlling and mitigating risks, guiding the development and implementation of internal policies and procedures that ensure that the activities carried out are consistent with the established objectives.

- **The second line** corresponds to the Risk Committee and the rest of the control functions (Regulatory Compliance Body, Control Body in matters of the Internal Regulation of Conduct of the Securities Market, Internal Control Body in matters of prevention of money laundering, CISO and Information Security Committee) that must monitor risks and controls to ensure that the first line of defense is appropriately designed, implemented and operating as intended.

- **The third line** of defense corresponds to the Internal Audit Department, whose mission is to provide independent assurance to the Board of Directors and the Audit and Control Committee on the effectiveness and efficiency of the controls implemented in risk management.

5. MERLIN Risk Map

Merlin uses the Risk Map as a tool that aims to graphically show the result of the risk assessment process during a given measurement period.

The Audit and Control Committee, as established by its own Regulations, will review the Group's risk map with the necessary periodicity for adequate monitoring of risks.

The periodic analysis of the Risk Map is carried out at least every six months, in a coordinated manner and by each of the heads of the different business divisions by monitoring the KPIs associated with each risk and together with updating the Merlin Group's annual budget.

In this regard, the Audit and Control Committee will hold, at least annually, a meeting with the heads of the business units in which they explain the trends in the business and the associated risks, and reinforce the idea that it is the heads of the business units who are directly responsible for effectively managing risks, such as the principle that it is convenient to have a specific employee in charge assigned to each identified risk.

For the identification and supervision of environmental, social and governance risks, the Audit Committee will coordinate with the Sustainability and Innovation Committees, as well as with the Appointments and Remuneration Committee.

The Internal Audit and Risk Management Directorate is responsible for drawing up the framework for action to standardize the identification, classification, assessment, management and monitoring of risks in the different business segments.

MERLIN's Risk Map is divided into sectors (Strategic Risks, Business Risks, Resource Risks – economic, technological and human – and ESG Risks) that represent the different axes of MERLIN's strategy and that encompass the different risks identified (internal and external factors) that may affect MERLIN's objectives with respect to its Strategic Plan (long-term). Its annual (short-term) Budget, as well as the different stakeholders with which it interacts (and as established in the Stakeholder Management Policy).

The assessment of the criticality of each of the risks is determined by the binomial of the probability and impact of the risks in the different processes, activities or functions of each business division.

Subsequently, and once the risks have been identified, their impact and probability have been assessed, as well as the indicators for their monitoring, the Risk Map is prepared with the participation of each of the business divisions, as well as Senior Management, for subsequent review and validation by the board committees involved, for final validation by the Audit and Control Committee and final presentation to the Board of Directors.

Each of the risks included in the Risk Map is assigned a person responsible for monitoring and reporting the different indicators associated with the risks.

In general, all those risks that have been identified as High Criticality are subject to continuous monitoring by both the Risk Committee and Senior Management in their meetings of the Operating Committee (OpCo), and by the Board of Directors through presentations, on a quarterly or semi-

annual basis, which are carried out to the Audit and Control Committee, with the different quantitative and/or qualitative indicators to analyze the situation and risks faced by the Group.

6. Risk Tolerance Level

The setting of appetite and the level of risk tolerance are executive functions attributed to the Board of Directors.

Risk appetite is understood as the level of risks that the Company is willing to assume or reject based on its strategic objectives, considering the expectations of its stakeholders, and risk tolerance as the determination of fluctuations in the level of risks, understood as normal around its risk appetite.

In determining the level of risk tolerance, the following are considered:

- Qualitative elements, which establish the specific risks that the organization is willing to accept based on the risks inherent to the activity and that are linked to the strategy and business plans.
- Quantitative elements, describing limits, thresholds or key risk indicators, which set out how risks and their benefits are to be assessed and/or how to assess and monitor the aggregate impact of these risks, on the premise that not all risks are measurable.

In this regard, on an annual basis, the Audit and Control Committee, at the proposal of Senior Management, submits to the Board of Directors for approval the **setting of the indicators, thresholds and limits of the main corporate risk indicators** (i.e.: LTV, ICR, FFO, etc.) and those specific to each branch of activity (GRI, NOI, etc.). occupancy rate, etc.), monitoring compliance with them on a six-monthly basis, establishing, where appropriate, the relevant action plans.

In any case, the company's ultimate objective is to maintain a risk profile (risk appetite) aligned with a medium-low risk tolerance, typical of a SOCIMI business model committed to the creation of long-term value and the generation of sustainable and growing dividends for shareholders within an environment of transparent values, ethics and responsibility in the business and social sphere.

It is important to highlight the existence of risks with **"zero tolerance",** that is, risks for which the response strategy is "avoid", which implies not proceeding with the activity that causes the risk or changing the way of acting.

The organization includes in this typology all risks related to compliance with the conditions of the SOCIMI Regime, with any other legal or regulatory breaches, with compliance with the conditions for financing and dividend distribution, risks related to criminal offences, risks related to any type of fraud, corruption or bribery (by managers and employees,

customers or suppliers of the company) and those related to the prevention of money laundering and terrorist financing.

In this regard, it is necessary to take into account those established by the **Group's Tax Strategy and Tax Policy**, which establish a series of principles of action, including strict compliance with tax obligations and payment of taxes that are legally due, not using artificial structures or structures lacking economic or business sense in order to reduce the tax burden of the company or its shareholders and the commitment not to operate in territories classified as tax havens with the main purpose of reducing the tax burden of the company or its shareholders.

Likewise, within the MERLIN Group's Governance System, there are different policies that express the Company's will to strictly comply with the highest standards of ethical and legal behavior. These policies include the **Criminal Compliance Policy, the Human Rights Respect Policy and the Money Laundering, Corruption and Bribery Prevention Policy**, based on the principle of zero tolerance towards the commission of illicit or criminal acts, so it does not allow any of its employees, regardless of their hierarchical or functional level, engages or participates in any operation or business within its business activity that involves any criminal act or fraud, corruption or bribery, or that goes against the principles set out in its **Code of Conduct** , which aims to establish the basic principles by which the Group is governed, and the rules and criteria of behaviour of the MERLIN Group's employees in order to impose preventive and proactive action in the workplace the fight against corruption and bribery in all areas of business.

7. Business Continuity Framework

MERLIN has a Business Continuity Plan (BCP) whose purpose is to strengthen organizational resilience and ensure the continuity of operations and critical services in the face of disruptive events, minimizing the impact and guaranteeing an effective recovery.

The BCP aligns with the principles of ISO 22.301 for business continuity management and integrates with the corporate risk management approach and with the **Information Security Management System (ISMS).** The document is for corporate use, periodically reviewed (at least annually) and aimed at continuous improvement.

Scope and risk-based approach
The BCP covers all of MERLIN's processes and activities, their functional dependencies, and associated resources (people, vendors, IT applications, and data), based on impact analyses (BIAs) and RTO/RPO recovery objectives. It considers relevant risk scenarios (including unavailability of buildings, personnel, technology, suppliers and data) and defines strategies and recovery plans associated with these scenarios, prioritized according to criticality.

Governance, responsibilities and activation
Continuity management is articulated through a governance framework in which the **Security and Continuity Committee** stands out, with decision-making capacity and escalation to the management bodies, and with the possibility of activating the **Crisis Management Team** and incident management teams. Roles and responsibilities are established for: definition of strategic lines, approval and supervision of the BCP, coordination during contingencies, and reporting on the status and evolution of crises.

Risks and unavailability scenarios
The BCP incorporates a risk analysis to prioritize threats and guide mitigation and recovery measures. Unavailability scenarios are structured that include, among others: governance and compliance, technological unavailability, unavailability of personnel, unavailability of buildings and unavailability of suppliers, which serve as the basis for the design of strategies and plans.

Recovery strategies and plans
For each scenario, a catalogue of preventive and reactive strategies is defined (e.g.: teleworking and relocation, cross-training and knowledge protection, redundancies/alternate data center and backups, diversification or substitution of suppliers, specific measures in the event of data unavailability/ransomware). Recovery plans detail typical phases: validation/activation, communications, situation assessment, execution of measures, coordination with suppliers/customers/regulators when applicable, monitoring, documentation, return to normality and lessons learned.

Maintenance, training and testing
The BCP is managed as a living document with a minimum annual review and update in the face of relevant changes (structure, processes, technology, locations, suppliers, test results and incidents). A formal training and awareness-raising approach and a testing program are established, with evaluation of results and action plans to reinforce continuous improvement.

8. Third-Party Risk Management - Supply Chain

Third-Party Risk Management (TPRM) is an essential component of the Group's Risk Management System, insofar as MERLIN outsources critical activities – including facility management, execution of works and renovations, financial intermediation and the provision of technological services – the poor implementation of which can lead to economic losses, reputational damage, regulatory breaches or operational interruptions.

This section is applicable to all relationships with third parties that, due to their nature, volume or criticality for the Group's operations, are identified as relevant in the periodic evaluation process of the Corporate Risk Map.

Third-party risk management in the MERLIN Group is governed by the

following principles:

- **Proportionality**: the level of diligence applied in the assessment of third-party risk will be proportional to the potential impact of the relationship on the Group's objectives, considering the economic volume of the contract, the criticality of the service provided, access to the Group's assets or information systems and the possibility of reputational contagion.

- **Full lifecycle**: Third-party risk management will cover all phases of the contractual relationship, including pre-contract selection and approval, monitoring during the term of the contract, and managing the termination or replacement of the supplier.

- **Integration with the Risk Map**: the risks identified in the TPRM process will be integrated into the Group's Corporate Risk Map, under the corresponding categories according to the taxonomy established in this Policy.

- **Consistency with other Group policies**: third-party risk management will be carried out in coordination with the provisions of the Group's **Procurement Policy** and, where appropriate, with the instructions of the **Anti-Money Laundering, Corruption and Bribery Policy** and the **Information Security Policy.**

- **Zero tolerance for misconduct**: regardless of the level of criticality assigned to the supplier, the MERLIN Group will not tolerate relationships with third parties that fail to comply with its commitments in terms of ethical conduct, human rights, the environment or legal compliance, under the terms established in the Group's Code of Conduct.

9. Emerging and Artificial Intelligence Risks

In the context of the Group's Risk Management System, MERLIN has a framework for identifying, assessing and managing emerging risks, with particular attention to the risks arising from the adoption and use of artificial intelligence (hereinafter, "AI") systems.

For the purposes of this Policy, an emerging risk is understood to be any threat of a new or evolving nature, whose impact on the Group's objectives is uncertain and whose probability of materialization is undefined, but which presents a growing trend in the Company's operational, technological, regulatory or social environment and could acquire significant relevance in the medium or long term.

Emerging risks are characterized by their cross-cutting nature – they can simultaneously affect several categories of risks and by the limited availability of historical data that allows an accurate quantification of their

impact and likelihood. This nature requires a management methodology that is different from that applicable to mature risks in the Corporate Risk Map.

The risks arising from the adoption and use of AI systems currently constitute the most relevant emerging risk category for the Group, both due to the active incorporation of these technologies into MERLIN's operations and the impact of the regulatory framework.

Without prejudice to the provisions of **MERLIN's Policy on the Responsible Use of Artificial Intelligence Systems**, approved by the Board of Directors in December 2025, this section integrates the risks arising from the use of AI systems within the framework of the Group's Risk Management System, in accordance with the provisions of the EU AI Act and the COSO ERM Framework 2017.

The process of identifying and monitoring emerging risks will be integrated into the annual cycle of updating the Group's Risk Map, with the following specificities:

- **Horizon analysis**: on an annual basis, and prior to the preparation of the Risk Map, the Risk Committee, with the support of the Business Divisions, will carry out an analysis of the technological, regulatory, geopolitical and social trends relevant to the Group, in order to identify emerging threats that may not be included in the current risk taxonomy.

- **Register of emerging risks**: the emerging risks identified will be recorded in a specific section of the Corporate Risk Map, differentiated from mature risks, with an indication of the level of uncertainty, the estimated time horizon of materialization and the available monitoring indicators.

- **Revision of the taxonomy**: when an emerging risk is considered, due to its evolution, as mature – that is, when its impact and probability are quantifiable with sufficient reliability – the Internal Audit Directorate will propose its formal integration into the risk taxonomy, for submission to the Audit and Control Committee.

- **Regulatory monitoring:** MERLIN's Management, together with the Risk Committee and in coordination with the Internal Audit Department and the Regulatory Compliance Body, will actively monitor regulatory initiatives in the areas of AI, cybersecurity, data protection and sustainability, to anticipate the emergence of new compliance risks.

The **Information Security Committee** (CSI-Security), in compliance with

its functions as a second line of defense, will supervise the adequacy of the controls implemented for AI systems, reporting biannually to the Audit and Control Committee on the status of AI risk in the Group.

10. Sustainability Risk Management: TCFD and Climate Scenario Analysis

This framework is based on the recommendations of the Task Force on Climate-related Financial Disclosures (hereinafter referred to as "TCFD") of the Financial Stability Board, which the MERLIN Group has voluntarily adopted as a reference for climate risk reporting, as set out in Annex IV of the Group's Non-Financial Information Statement (NFIS). Its incorporation into the Risk Management System is intended to ensure that climate and sustainability risks receive, for internal purposes, the same systematic and periodic treatment as the rest of the categories of the Corporate Risk Map.

The scope of this sustainability risk management framework includes all the assets managed by the Group, including the portfolio of offices, shopping centers, logistics warehouses and data centers, considering that each type of asset has a differentiated exposure profile to the physical and transition risks associated with climate change.

The MERLIN Group classifies sustainability risks into two large groups, in accordance with the TCFD methodology:

A) <u>PHYSICAL RISKS</u>

- **Acute (extreme events):** Floods and torrential rains that affect logistics assets in coastal or floodplain areas; heat waves that increase energy consumption and deteriorate the office asset experience; hailstorms and extreme winds with structural damage to photovoltaic roofs.

- **Chronic (gradual change):** Sustained increase in average temperatures that raises cooling costs in the Group's Data Centers (higher consumption of water for cooling); sea level rise with an impact on asset valuations in coastal areas; water stress in regions where high-water consumption assets are located.

B) <u>TRANSITION RISKS:</u>

- **Regulatory and legal**: Tightening of energy performance requirements for buildings (European Energy Performance of Buildings Directive); introduction or expansion of the CO2 market; new sustainability reporting requirements (CSRD) for tenants that affect the Group's green clause requirements.

- **Market and competitive**: Growing preference of tenants for buildings with high sustainability certifications (BREEAM/LEED Excellent or Outstanding) that could affect the occupancy of assets with lower certification; reduction in the appraisal value of assets not adapted to the energy transition (stranded assets); pressure from institutional investors with ESG mandates on the sustainability profile of the portfolio.

- **Technological:** Costs associated with the implementation of energy efficiency technologies in existing assets to meet the required efficiency standards (retrofitting); uncertainty about the cost and availability of energy storage technologies that support the Group's photovoltaic self-consumption.

- **Reputational**: Negative perception by investors, sustainability analysts or ESG rating agencies in the face of insufficient progress in the objectives of the Group's "Road to Net Zero" Plan or in the face of discrepancies between the declared commitments and the actual performance of the assets.

The MERLIN Group will carry out, at least every two years (coinciding with the update of its sustainability strategy), an analysis of climate scenarios aimed at assessing the resilience of the Group's asset portfolio and business model to different climate change trajectories.

The results of the scenario analysis will be integrated into the Corporate Risk Map, under category (g) of climate and sustainability risks, and will be reported to the Board of Directors as part of the annual review of the Risk Management System. In addition, the results of the analysis will be the basis of the TCFD Annex that the Group publishes in its Non-Financial Information Statement, ensuring consistency between the external report and the internal management of climate risk.

The risk management set out in this section shall be articulated in a manner consistent with the Group's "**Road to Net Zero**" strategy, ensuring that:

- **The Group's emission reduction targets, validated by the Science Based Targets initiative (SBTi), are reflected in the Risk Map** as strategic objectives whose non-compliance constitutes a reputational and market risk.

- **The opportunities associated with the energy transition will be systematically assessed** as a counterpart to the risks identified, in application of the risk-opportunity binomial management approach established in section 2 of this Policy.

- **The external climate risk report in accordance with the TCFD methodology (published in Annex IV of the Group's NFIS) faithfully reflects the results of the internal management** established in this section, ensuring consistency between the information published and the Group's Risk Management System.

Regarding sustainability risks, the **Audit and Control Committee** will be responsible for supervising the effectiveness of the process of identification and assessment of sustainability risks, the six-monthly review of the sustainability KRIs, the approval of the analysis of TCFD scenarios for publication in the NFIS and coordination with the Sustainability and Innovation Committee.

For its part, the **Sustainability and Innovation Committee** will be responsible for supervising the Group's sustainability strategy and its coherence with the Risk Management System, the quarterly review of the sustainability KRIs, the monitoring of the plan to update the climate objectives and the supervision of the TCFD report.

11. Global Supervision of the Risk Management and Control System

The MERLIN Group has a **Risk Management System** based on a comprehensive and systematic approach. This system is conceived as a key tool in the management of uncertainty, and as such, the objective is to help reduce threats and take advantage of opportunities that may arise in the Company's and its Group's businesses.

The MERLIN Group's Risk Management System aims to minimize the volatility of profitability and, therefore, maximize the Group's economic value, incorporating risk and uncertainty into the decision-making process to provide reasonable assurance in the achievement of the established strategic objectives, providing shareholders with, to other stakeholders and to the market in general an adequate level of guarantees that ensures the protection of the value generated.

For the development of Risk Management and Control, the Board of Directors has the collaboration of the Audit and Control Committee, which supervises and reports on the adequacy and effectiveness of the Risk Management and Control system.

The Audit and Control Committee is the body responsible for supervising the Company's Risk Management and Control system (including internal controls) and verifying its adequacy and integrity.

For the supervision of environmental, social and governance risks, the Audit Committee will coordinate with the Sustainability and Innovation Committees, as well as with the Appointments and Remuneration Committee.

Thus, the Audit and Control Committee carry out this supervisory function through the Internal Audit Department, which annually checks the adequacy and integrity of the Risk Management System implemented by the Company's Management.

Based on the analysis of MERLIN's Vision, values and strategy, an analysis of the different components is carried out, according to the grouping of the different strategic objectives that are included in these elements (being the SOCIMI of reference, long-term value creation, generation of sustainable and growing dividends, values of transparency, ethics and responsibility).

In this regard, the risks that MERLIN identifies and assesses are classified as follows:

a) **Governance and strategy risks**: risks arising from a possible breach of the provisions of the Group's governance systems, as well as risks associated with the macroeconomic, geopolitical and social environment, and investment and divestment decisions.

b) **Business and market risks**: risks related to key variables intrinsic to the Group's different activities, across the different business of its businesses, such as the management of the real estate cycles of each branch of activity of the Group, as well as the uncertainty generated by the volatility of the level of occupancy of assets, fluctuation in the level of income, concentration of income, loss of value of the real estate assets that make up each branch of activity of the Group.

c) **Credit and financial risks**: risks related to the possibility of a counterparty defaulting on its contractual obligations and causing economic or financial loss, including replacement risks and costs, as well as those relating to interest rate volatility, inflation and those related to solvency and liquidity.

d) **Regulatory, fiscal and legal risks**: as well as those arising from regulatory changes or in the tax regulations of the SOCIMI regime.

e) **Operational risks**: risks referring to economic losses, direct or indirect, caused by external events, errors or inadequate internal processes, as well as those that affect the ability to provide an adequate response to events of any nature that affect the continuity of priority processes.

f) **Technological and information security risks**: risks related to the management and proper functioning of information technologies, as well as those motivated by the adoption of new technologies, including artificial intelligence. It also includes risks related to the security of information systems, including cybersecurity, as well as the privacy of personal data processed and compliance with related regulations.

g) **Climate and sustainability risks:** including direct damage caused by

extreme weather events (such as floods, droughts, heatwaves, etc.), as well as the need to adapt to new environmental regulations, energy efficiency requirements and growing investor and customer expectations for sustainability.

Considering the multidimensional nature of risks, taxonomy incorporates additional classification variables that facilitate their monitoring, control, and reporting. These variables include emerging risks, defined as new threats, whose impact is uncertain and whose probability is undefined, but which present an increasing trend and could become significantly relevant for the companies that make up the Group.

MERLIN's Management develops this Risk Management and Control Policy through its **Risk Management System,** which develops aspects such as responsibilities in the organization or the internal Risk Management process identified in the Annual Corporate Risk Map.

12. Policy Communication and Awareness

The Risk Management and Control Policy will be made available to all the Company's stakeholders, both internally and externally, through its **publication on the corporate website** and will be subject to appropriate communication actions for its timely understanding and implementation throughout the organization.

In addition to communication and as a reinforcement of the risk management culture in the organization, MERLIN's Management will structure an **Annual Risk Culture Program** with: (i) mandatory training differentiated by hierarchical level; (ii) tracking metrics; (iii) periodic communications on the status of the risk system; and (iv) an annual risk culture survey to measure perceived maturity. The results of this program will be reported annually to the Audit and Control Committee.

13. Approval and update

The Board of Directors of MERLIN Properties SOCIMI, S.A. has the power to approve the Company's general policies and strategies.

The Risk Management and Control Policy, in accordance with Article 9 of the Regulations of the Audit and Control Committee, shall be reviewed periodically, to ensure that it includes the international recommendations and best practices in force at all times, and shall proceed to its modification when there are variations in this matter that suggest an extraordinary review outside the annual cycle such as materialization of a critical risk, regulatory change of significant impact, a relevant acquisition or divestment, changes in the macroeconomic or geopolitical environment, or recommendation of the external auditor, among others.

Internal Audit will be responsible for submitting a proposal for modification to the Audit and Control Committee so that it can be submitted to the Board of Directors for approval.

****

This policy was initially approved by the Board of Directors in February 2016, subsequently in April 2018, March 2019, March 2021, April 2022, April 2025 and finally in its current wording in **June 2026**.