ENERGYDOME

Our WORLD can't wait.

INFORMATION SECURITY POLICY



ED POL NIS 01 A

INFORMATION SECURITY POLICY

ED POL NIS 01 A

Policy

REV.	DATE	DESCRIPTION	PREPARED	REVIEWED	APPROVED
A	September 1, 2026	First issue	Filippo Molteni	Stefano Marforio	Claudio Spadacini (CEO)

☒ **Public document**: distribution to individuals outside the organization is permitted.
☐ **Internal document**: may also be consulted by individuals outside the organization.
☐ **Confidential document**: Disclosure to parties outside the organization is prohibited.

Energy Dome S.p.A. recognizes information and information systems as strategic assets essential to its operational activities, technological development, and the achievement of corporate objectives. The Company is committed to protecting information from threats that could compromise its confidentiality, integrity, and availability.

This **Information Security Policy** defines the high-level principles that guide Energy Dome's approach to information security and **cybersecurity**, establishing the responsibilities and supervisory role of Executive Management and the Board of Directors.

SCOPE

This Policy applies to Energy Dome S.p.A. and all companies belonging to the Energy Dome Group, in Italy and abroad, regardless of the country in which they operate, the geographic location of their activities, or the location of the information, information systems, technological infrastructure, and digital services used.

The scope of application includes all business processes, operational activities, projects, facilities, offices, cloud environments, application platforms, networks, devices, and any other information or technology assets managed directly or indirectly by the Group.

The Policy also applies to all employees, executives, directors, contractors, consultants, suppliers, business partners, outsourcers, and third parties who, in any capacity, process Energy Dome's information or access its systems, data, applications, networks, infrastructure, or physical and digital work environments. Each recipient is required to be familiar with and comply with the principles, responsibilities, and measures set forth in this Policy, in accordance with their role, level of authorized access, and the activities performed on behalf of or in the interest of the Group.

PRINCIPLES AND COMMITMENTS

- Protect information assets based on their value, sensitivity, and criticality, ensuring adequate levels of confidentiality, integrity, and availability;
- Adopt a risk-based approach to information security, consistent with business objectives, technological advancements, and the cyber threat landscape;
- Establish, maintain, and continuously improve an Information Security Management System aligned with internationally recognized standards, including ISO/IEC 27001;
- Comply with applicable legal, regulatory, and contractual requirements regarding information security and cybersecurity, including Directive (EU) 2022/2555 (NIS2), as transposed into Italian law by Legislative Decree No. 138 of September 4, 2024, as well as subsequent implementing and supervisory provisions issued by the competent authorities;
- Ensure the protection of personal data in accordance with Regulation (EU) 2016/679 (GDPR) and applicable Italian legislation on the protection of personal data, including Legislative Decree No. 196 of June 30, 2003, as amended;

This document is the property of ENERGY DOME SPA. Reproduction of this document, in whole or in part, and the disclosure of any related information to others without prior written consent is strictly prohibited.

- Prevent, detect, and manage cybersecurity incidents and operational disruptions in a timely and structured manner, with the aim of limiting their impact and supporting operational resilience;
- Manage information security and cybersecurity risks arising from suppliers, partners, and third parties that process or have access to Energy Dome's information or systems;
- Promote a culture of awareness, responsibility, and accountability regarding information security among employees, contractors, and relevant third parties, including through periodic training, communication, and awareness initiatives on cyber risks, security best practices, and applicable company procedures.

RESPONSIBILITIES OF THE BOARD OF DIRECTORS REGARDING CYBERSECURITY

The Board of Directors and Executive Management recognize cybersecurity and information protection as strategic and critical issues for the business.

- It provides strategic direction and oversight regarding information security and cybersecurity;
- Ensures that information security risks are identified, assessed, and managed within the **enterprise risk management** system;
- Oversees the allocation of adequate resources to maintain and improve cybersecurity and organizational resilience;
- Receives periodic updates on the effectiveness of the Information Security Management System, significant risks, and material incidents;
- Supports continuous improvement and compliance with applicable regulatory requirements.

RESPONSIBILITIES AND COMPLIANCE

All employees and third parties acting on behalf of Energy Dome are required to comply with this Policy, as well as with the rules, procedures, and internal controls established to protect information assets. Operational responsibilities regarding information security are assigned, based on their respective roles, to the IT, Risk & Compliance departments, process managers, users of information systems, and relevant third parties, so that each contributes to the identification, management, and mitigation of risks associated with the processing of information and the use of company systems.

Executive Management ensures that this Policy is implemented, communicated, and supported by appropriate governance, organizational, and supervisory measures.

REVIEW AND AVAILABILITY

This Policy is approved by the Chief Executive Officer of Energy Dome, communicated within the organization, and made publicly available. It is reviewed periodically to ensure its continued adequacy in light of changes in the business environment, risk exposure, applicable laws, and regulatory guidelines.

This document is the property of ENERGY DOME SPA. Reproduction of this document, in whole or in part, and the disclosure of any related information to others without prior written consent is strictly prohibited.