GLOBAL INFORMATION SECURITY POLICY

This document sets out the Company's approach to matters relating to Information Security, in line with the organisation's strategic direction and the applicable legal, regulatory [1] and contractual requirements for the security of network and information systems.

This Policy shall be periodically reviewed and updated where appropriate, in line with the applicable regulatory requirements and to adapt to the evolving risk landscape should new types of threats to corporate information emerge.

PRINCIPLES

In particular, this Policy defines the key principles for protecting the organisation's information assets:

- "**Confidentiality**", understood as the ability to ensure that access to or disclosure of information is restricted to authorised individuals or entities only;
- "**Integrity**", understood as the ability to safeguard the accuracy and completeness of information over time;
- "**Availability**", understood as the ability to make information available, accessible and usable within the timeframes and in the manner required by authorised individuals or entities.

These principles provide a framework for managing risks that may affect corporate information and assets (applications, services, infrastructure or other components that handle information), protecting them from any threat, whether internal or external, intentional or accidental.

This Policy requires the Group's employees, suppliers (including their subcontractors), collaborators and any third party handling Pirelli's data, information or information systems to comply with the principles set out in this Policy, as well as with all applicable laws and regulations.

The Group's security is founded on key principles such as continuous risk assessment, the protection of critical assets, personnel training and incident response capability.
To ensure effective Information Security management, in line with the principles set out in this Policy, the Pirelli Group adopts a robust and structured framework, setting out, through specific internal procedures and operating instructions, the roles, responsibilities and operational procedures relating to information security.

GOVERNANCE, RISK MANAGEMENT AND CONTINUOUS IMPROVEMENT

The Board of Directors of Pirelli & C. S.p.A. is responsible for approving this Information Security and Cybersecurity Policy, in line with the applicable regulatory requirements, including the NIS2 Directive.

The Group's Top Management, supported by the Information Security department and the other relevant business departments, is responsible for the full implementation of this Policy, ensuring the effective deployment of security measures, as well as the establishment of appropriate reporting flows to the Board of Directors.

The Pirelli Group's internal control system is structured to ensure accurate reporting and adequate control coverage across all Group activities, with particular attention to areas considered potentially at risk, through

[1] For this reason, the companies within the Pirelli Group that are subject to Directive (EU) 2022/2555 (NIS2) define, implement and monitor the applicable requirements within their organisational and procedural framework consisting of policies, standards, operating procedures and guidelines.

a risk management process that also includes the cybersecurity risks of the Group and those of relevant third parties. The Pirelli Group identifies the actions required to continuously improve its security posture, risk management and alignment with regulatory requirements, as well as to ensure the implementation of its internal information security policies.

SECURITY EVENT MONITORING, INCIDENT RESPONSE AND CRISIS MANAGEMENT

The Pirelli Group adopts a structured and integrated approach to security, based on formalised processes for the continuous monitoring of security events, vulnerability management and response to any incidents and crisis events.

Specifically, the Pirelli Group identifies, analyses, prioritises and defines how to manage vulnerabilities affecting information systems, monitors and analyses security events in order to promptly identify and address threats that could compromise the confidentiality, integrity and availability of information, and adopts incident response plans covering the entire process, from identification through to the corrective actions required to reduce the likelihood of recurrence. The roles involved, communication channels and escalation procedures form part of a structured and formalised process, which also includes both external and internal communication flows.

The Pirelli Group has crisis management processes in place (including significant incidents), with escalation to business continuity plans, enabling the definition and implementation of rapid and effective actions in response to unforeseen and/or exceptional events, with the aim of restoring operations as quickly as possible and minimising potential damage.

INTEGRATED CONTROL SYSTEM FOR INFORMATION SECURITY

The Pirelli Group defines and maintains a coordinated set of technical, organisational and human resource measures to complement its Information Security management system. In this regard, the Group defines and maintains, among other things, training and awareness programmes for personnel and third parties (where applicable), implements information classification and protection processes, and ensures the secure management of assets, including their physical protection, throughout their entire lifecycle.

At the same time, the Group adopts structured models for managing digital identities and access controls designed to ensure that users are authorised to use IT resources and only access the information necessary to perform their duties ("need to know"), with privileges assigned only to the minimum extent necessary ("least privilege"), protects its physical infrastructure, and integrates security principles within the lifecycle of information systems according to a Security by Design approach. Corporate networks and communications are further protected through technical protection and segmentation solutions to safeguard the confidentiality, integrity and availability of information.

REPORTING, CONFIDENTIALITY, NON-RETALIATION AND CONSEQUENCES IN CASE OF VIOLATION

The Pirelli Group encourages the Recipients of this document to report in good faith, even anonymously, any act or omission by anyone at Pirelli, in relations with it or on its behalf, which constitutes or may constitute a violation, or inducement to violate the principles contained in this Policy. The Whistleblowing Policy, published at www.pirelli.com in multiple languages, sets out the procedure for submitting reports, how they are managed and how confidentiality and non-retaliation are guaranteed.

Pirelli shall take appropriate action in the event of a breach of this Policy, whether it is discovered through the Whistleblowing Procedure or other means. Depending on the severity, this may include corrective action (including but not limited to: communicating with the offending employee, establishing a specific action plan with the relevant managers, etc.) and/or disciplinary actions (including but not limited to: verbal and/or

written reprimands, negative performance reviews or termination), all in compliance with the applicable contractual, disciplinary, legal and regulatory system.

DOCUMENTS RELATED TO THIS POLICY

- CODE OF ETHICS and CODE OF CONDUCT
- GLOBAL PERSONAL DATA PROTECTION POLICY
- INTELLECTUAL PROPERTY POLICY
- WHISTLEBLOWING POLICY

September 2026

PIRELLI & C. S.p.A.

BOARD OF DIRECTORS