ARTIFICIAL INTELLIGENCE AND DATA SCIENCE POLICY

OBJECTIVE

Establish the principles, guidelines, and directives for the development, commercialization, and responsible, ethical, transparent, and effective use of Artificial Intelligence (AI) and Data Science (DS) within the Colombina Group companies. The policy aims to support decision-making, improve operational efficiency, foster innovation, and ensure the trust of clients, employees, and other stakeholders.

SCOPE

This policy applies to all individuals involved in the design, development, implementation, use, evaluation, or supervision of AI and DS systems within the Colombina Group companies, as well as third parties who, directly or indirectly, are engaged in such activities.

DEFINITIONS

- **Artificial Intelligence (AI):** Software developed using techniques such as machine learning, logical reasoning, and advanced statistics. This software has the ability to generate results—such as predictions, recommendations, or decisions—that influence the environments with which they interact.

- **Machine Learning (ML):** A type of AI with the capacity to learn and improve from data without being explicitly programmed, using algorithms to identify patterns, make predictions, automate tasks, and enable systems to make decisions with minimal human intervention.

- **Model:** A mathematical representation created by algorithms and trained with a dataset to develop capabilities aligned with defined objectives.

- **Data Governance:** Refers to the establishment of direction, principles, duties, and responsibilities of those involved in data management, controlling data usage to ensure appropriateness, efficiency, accuracy, completeness, timeliness, security, privacy preservation, interoperability, and high quality—ready for processing and implementation in AI and DS.

Roles and Responsibilities

Senior Management: Define and approve this policy. Allocate resources for its enforcement. Ensure integration of the policy with corporate strategy.

Information Security, Cybersecurity, and Artificial Intelligence Committee: Evaluate sensitive projects, oversee ethical and social risks, monitor implementation of the policy, periodically assess risks associated with AI, and report compliance status and emerging risks to Senior Management.

Vice Presidency of Strategic Planning and Chief Technology Officer (CTO): Lead AI and DS strategy and ensure compliance with this policy.

Process Owners: Define use cases, validate results, and ensure proper interpretation of AI outputs.

Data Scientists: Design, train, and maintain models according to ethical and technical standards.

Data Engineers: Prepare and transform data; design and manage data pipelines.

Business Users: Use models responsibly, report anomalies, comply with this policy, and report incidents or risks identified in AI usage.

Legal and Compliance Department: Validate regulatory compliance of AI developments.

Suppliers and Third Parties: Ensure AI systems provided comply with this policy and observe all related contractual obligations.

Guiding Principles

Confidentiality: Protect sensitive, strategic, and personal information against unauthorized access, prioritizing personal data protection in AI and DS usage.

Integrity: Ensure the accuracy, consistency, and reliability of data and AI models. Procedures must subject AI systems to thorough risk assessments, identifying uncertainties, deviations from intended objectives, and potential negative impacts.

Availability: Ensure AI systems and outputs are accessible when required.

Ethics and Responsibility: Respect human rights, dignity, and privacy. Models that produce discriminatory biases or unjustifiable, non-explainable outcomes will not be developed or deployed. Developers and users must be accountable for AI system impacts.

Governance and Oversight: Ensure every AI solution undergoes technical, legal, and ethical validation prior to implementation, and is regulated and supervised by the IT and Information Security departments.

Privacy and Data Protection: Ensure all AI and DS-related activities comply with the Colombina Business Group's Data Protection Policy and Information Security Policies. AI systems must implement robust security measures.

Transparency: AI models must be transparent and explainable, especially when impacting decisions involving people (customers, employees, or stakeholders). Users must be clearly and timely informed when interacting with automated systems.

Data and Model Quality: AI-based decisions must rely on reliable, representative, and up-to-date data. Controls for traceability, validation, and continuous monitoring of models will be implemented.

Responsible Innovation: Promote AI and DS as enablers of digital transformation, ensuring alignment with corporate strategy and organizational values.

Policy Approval and Review

This policy will come into effect upon approval by Senior Management and must be reviewed annually by the Information Security, Cybersecurity, and Artificial Intelligence Committee. It will also be updated in line with national and international regulatory changes, as well as technological and strategic developments, to ensure alignment with the strategic needs of the Grupo Colombina.