Secuoya
content group

POLICY ON THE RESPONSIBLE USE OF ARTIFICIAL INTELLIGENCE

Secuoya, Grupo de Comunicación, S.A. and its Group Companies

HEADQUARTERS:
Avenida de España, 4
28760, Tres Cantos, Madrid
+34 913 717 569

REGISTERED OFFICE:
Gran Vía de Colón, 12
18010, Granada,
+34 958 216 898

Index

1. INTRODUCTION 3
2. DEFINITIONS 3
3. SCOPE 5
4. GENERAL PRINCIPLES OF ACTION 6
5. SPECIFIC GUIDELINES FOR USE 7
6. GENERAL RULES APPLICABLE TO THE INDIVIDUAL USE OF AIT 9
7. TRAINING 10
8. SUPERVISION, CONTROL AND REVIEW 10
9. APPROVAL AND ENTRY INTO FORCE 11

1. INTRODUCTION

Secuoya Grupo de Comunicación, S.A. ("Secuoya", "Secuoya Content Group" or "the Group") together with the companies within its Group, as well as all Professionals and Collaborators who carry out their activities within the Group, act in compliance with applicable law and in accordance with the highest ethical and professional standards.

In line with these principles and with Regulation (EU) 2024/1689 on Artificial Intelligence (the "AI Act"), this Policy on the Responsible Use of Artificial Intelligence (from now on, the "Policy") establishes the framework governing the development, adoption and use of artificial intelligence ("AI") tools within the Group.

This Policy is part of Secuoya's internal regulatory framework, complements the Code of Ethics, the Compliance Manual and other corporate policies on security, privacy and good governance, and is binding on all individuals and entities to whom it applies.

The purpose of the Policy is to promote the responsible, ethical, safe and transparent use of AI, providing Secuoya's Professionals and Collaborators with clear guidelines that enable them to:

- Improve the efficiency and quality of their work through the appropriate use of approved AI tools.
- Protect the information and privacy of personal and corporate data by applying the principles of confidentiality, minimisation and security by design.
- Act in an ethical, responsible and transparent manner in all interactions with AI systems, ensuring human oversight and respect for fundamental rights.
- Boost creativity, innovation and professional development, fostering a safe, trustworthy and sustainable working environment that supports equal opportunities and respect for human dignity.

This policy is progressively aligned with the European regulatory framework established by the Artificial Intelligence Regulation (AI Act), applicable from 2024, and will be reviewed as its implementation phases advance.

Any use of AI tools or hybrid artificial intelligence (HIA) systems by Professionals, Collaborators or third parties that does not comply with the guidelines set out in this Policy, the Code of Ethics or the Group's internal rules shall be the sole responsibility of the user. Under no circumstances shall Secuoya Content Group or the companies within the Group be liable for any damage, loss or consequences arising from the improper, unauthorised or negligent use of such tools.

2. DEFINITIONS

For the purposes of this Policy, the following terms shall have the following meanings:

- Artificial Intelligence (AI)/Artificial Intelligence Tool (AIT): Any system, programme or application designed to operate with varying levels of autonomy and capable of generating automated results (predictions, recommendations, decisions or content) through machine learning algorithms or other AI techniques.

- Corporate AIT: AI tool provided or previously validated and approved by Secuoya for professional use, following assessments by CISO/IT (security), DPO (privacy) and Compliance (ethics and permitted use) where applicable.

- Personal Use AIT: An external AI tool that is neither provided nor validated by Secuoya. Its use for professional purposes requires prior authorisation from the CISO/IT function and review by the DPO and Compliance in order to verify privacy, intellectual property and regulatory compliance risks.

- Professional/Collaborator: Any individual who works for or collaborates directly with any company within the Group and who has access to the Group's systems or information.

- Artificial Intelligence Regulation (AIR): Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence, as well as any rules that may replace or further develop it.

- Personal data: Any information relating to an identified or identifiable natural person, as defined in Regulation (EU) 2016/679 (GDPR) and Organic Law 3/2018, including any data that allows a person to be identified directly or indirectly (name, image, voice, contact details, online identifiers, etc.).

- Supervisory and Control Body: Secuoya's internal body regulated under the Compliance Manual, with autonomy and independence, responsible for overseeing compliance with corporate policies, including this Policy, and for proposing corrective or disciplinary measures.

- Inputs/Outputs:

  Inputs: Data, content or information entered into an AIT for processing (text, images, videos, sounds or other).

  Outputs: Results generated by an AIT (reports, text, images, decisions, recommendations or other).

- AI bias: Any systematic tendency or inclination that may produce unfair, inaccurate or discriminatory outcomes in an AIT, resulting from biased training data, incorrect assumptions or inadequate algorithms.

- Data processing: Any operation performed on personal data (collection, recording, storage, modification, consultation, communication, deletion, etc.), in accordance with the GDPR and Spanish data protection regulations.

- Traceability: The ability to track and document the data, processes, parameters and decisions leading to a specific outcome generated by an AIT, including inputs, algorithms, models, versions and reviews. In the case of cloud-based tools or services, Secuoya shall ensure, through the IT/CISO function, that the information necessary to verify such traceability is accessible and can be retained as evidence for audit and compliance purposes.

- User: Any individual who uses, has custody of or accesses a Corporate AIT, including Professionals, Collaborators or third parties expressly authorised by Secuoya.

- Synthetic or AI-generated content: Content (text, image, audio, video or other) produced wholly or partially by an AIT, which may be mistaken for material created by a human, including so-called deepfakes.

- High Impact/High Risk: A category defined under Regulation (EU) 2024/1689 for AI systems which, by reason of their purpose or effects, may affect fundamental rights or safety (for example, AI used for recruitment, credit assessment or biometric recognition).

3. SCOPE

This Policy applies to Secuoya Grupo de Comunicación, S.A. ("Secuoya"), to all companies forming part of Secuoya Content Group within Spanish territory, and to all professionals and collaborators who carry out their activities for the Group in Spain, regardless of the nature of their legal relationship, contractual status or role.

Furthermore, this Policy shall have a guiding and referential character for investee companies, subsidiaries, joint ventures, temporary business associations (UTE) and other entities in which Secuoya exercises control or management outside Spain, insofar as local legislation so permits and to the extent that it is compatible with their legal and contractual frameworks.

The Policy shall also be binding on suppliers, contractors, consultants, freelancers and other third parties who, by reason of their activity, have access the Group's systems, data, content or resources, or who carry out projects for the Group involving the use of AI tools.

In such cases, Secuoya may include an adhesion clause or equivalent obligations in the relevant contracts, service agreements or collaboration terms, including commitments relating to information security, data protection, ethical use of AI, and Secuoya's right to audit or verify compliance where necessary, without prejudice to applicable local legislation.

This approach seeks to ensure that any individual or entity that uses or has access to AI tools on behalf of Secuoya complies with the principles of security, privacy, ethics and regulatory compliance set out in this document.

4. GENERAL PRINCIPLES OF ACTION

Secuoya undertakes to make available the necessary means to ensure the ethical, responsible and secure use of artificial intelligence, in line with its corporate values and its commitment to leadership in the audiovisual and content sector.

The principles set out below must be interpreted and applied in conjunction with the Code of Ethics, the Compliance Manual and the other corporate policies of the Group, all of which are binding on all Professionals, Collaborators and third parties associated with Secuoya. Any breach of this Policy may be treated as a violation of the obligations arising from the Code of Ethics and the applicable labour or contractual regulations.

The following principles shall guide the use of AI tools by the Group's Professionals and Collaborators, both when using directly accessible tools and when contracting or developing corporate AI solutions:

I. Privacy and data protection: Professionals must refrain from inputting personal data or confidential information of the Group or third parties into AI tools, unless the tool has been previously approved as a Corporate AIT and includes the safeguards established by the Data Protection Officer (DPO). In all cases, Regulation (EU) 2016/679 (GDPR), Organic Law 3/2018 and the Group's internal data protection policies shall apply.

II. Security and content review: AI generated results must be reviewed before use to ensure that they do not contain errors, sensitive information or material that could affect third parties or the Group's reputation, in accordance with the guidelines of the Information Security Policy and the Data Classification Policy.

III. Ethics and respect for dignity: AI must be used ethically avoiding psychological or reputational harm, deception, or detriment to third parties, and respecting Secuoya's values as well as the human rights recognised in the Code of Ethics.

IV. Intellectual property: It is prohibited to introduce or use third-party content in AI tools that may infringe copyright or intellectual property rights, unless the corresponding rights or licences have been obtained.

V. Transparency and communication: When AI is used to generate content or make significant decisions, Professionals must make it clear that an automated system

was used and, wherever possible, provide understandable explanations of its functioning and limitations.

VI. Security and reliability (applicable to corporate AIT): Corporate AITs must be secure and reliable, operate according to their intended purpose, and include control mechanisms to prevent unexpected or harmful outcomes. Systems must be robust, resilient, and designed following the principle of security and compliance by design.

VII. Prevention of bias and discrimination: Results obtained through AI must be reviewed to ensure that they do not reproduce stereotypes, prejudices or discrimination of any kind. Corporate AIT must be trained with diverse data to minimise bias and promote equal opportunities, in line with the equality and non-discrimination commitments set out in the Code of Ethics.

VIII. Training and continuous updating: Professionals must familiarise themselves with the AI tools and, where applicable, the hybrid artificial intelligence tools they use, and participate in the training activities provided by the Group on best practices, risks, and ethical principles.

IX. Acceptable use (applicable to corporate AIT): Corporate AIT must be used exclusively for professional purposes related to assigned duties and never for personal use or activities unrelated to the Group.

X. Innovation and sustainability: Secuoya's AI strategy must drive innovation and support sustainable development, generating long-term value for the company and society, always within legal and ethical boundaries.

XI. Respect for human autonomy: The use of AI must respect people's freedom and autonomy, ensuring human supervision and control over work processes, and preventing decisions from being made entirely automatically without intervention or review.

XII. Evaluation and monitoring (applicable to corporate AIT): Corporate AITs shall be subject to ongoing evaluation and monitoring procedures to ensure their proper functioning and compliance with this Policy, guaranteeing, to the extent permitted by the technical capabilities of the tool, the traceability of their outputs.

5. SPECIFIC GUIDELINES FOR USE

Differences in use between Corporate AI Tools and Personal Use AI Tools	
Corporate AI tools (AIT)	**Personal Use AI tools (AIT)**
❖ These are AI tools that have been previously **identified, evaluated and pre-approved** by the **IT/CISO Department**, with a report from the **DPO** and validation by **Compliance**, and provided by Secuoya for professional use by authorised personnel.	❖ The use of results obtained by a Personal Use AIT for professional purposes **requires prior approval from the CISO/IT**, following review by **the DPO** and **Compliance** in cases involving personal data or corporate content.
❖ Their use is strictly limited to professional purposes related to the Group's activities. **They may not be used for personal purposes or activities unrelated to Secuoya**.	❖ Personal use of AI tools is permitted on an individual and private basis, provided that **no confidential, personal or corporate data is input**, and that no results are used in a professional context without the appropriate authorisation.
❖ **Users should not expect privacy** regarding the content generated by these tools, as they operate in corporate environments subject to monitoring and traceability.	❖ Secuoya **is not responsible** in any way for the use made of Personal Use AIT or for any content generated by them, unless the tool has been previously approved by the company.
❖ It is essential that all users of Corporate AIT are aware of and comply with the **conditions of use**, being fully aware of the potential risks, this Policy and the **recommendations and warnings** issued by IT, the DPO, and Compliance.	❖ If results from personal tools are to be incorporated into professional work, it must be ensured that **they comply with the principles of this Policy**, including those relating to privacy, intellectual property, security and ethics.
	❖ In case of any doubt regarding the reliability or suitability of a Personal Use AIT, Professionals must **consult their manager or the Compliance department** before using the outputs in corporate tasks.

Procedure for identifying and approving Corporate AIT

No AI tool may be used as a Corporate AIT without first completing the following steps:

- ❖ The IT/CISO Department has carried out a technical security assessment and registered the tool in the Corporate AIT Inventory.
- ❖ The DPO has assessed the privacy risks and, where applicable, issued a report or Data Protection Impact Assessment (DPIA).
- ❖ Compliance has validated the intended use and the relevant contract clauses with the supplier.

Only after these validations will the tool be authorised for professional use and communicated to employees along with instructions and warnings for use.

Communication will be carried out via the Incident Management or Ticketing tool (https://helpdesk.secuoyacontentgroup.com/) through which requests for new software and/or services are already managed. For systems installed locally on users' computers, special care must be taken, as internal security policies and existing tools prevent the installation of unauthorised software. For cloud systems or websites, access restrictions may be applied within the organisation's corporate networks.

6. GENERAL RULES APPLICABLE TO THE INDIVIDUAL USE OF AIT

To ensure the responsible and safe use of artificial intelligence, Secuoya establishes the following guidelines applicable to all Professionals and Collaborators, regardless of whether they use corporate or personal AI tools:

I. Risk of sensitive information leakage → Do not input any personal data, confidential or classified information of the Group's companies, employees or third parties into any AIT, unless it is an authorised Corporate AIT and the guarantees established by the Data Classification Policy and the Data Protection Officer (DPO) are met.

II. Risk of errors, incomplete or biased information → Always review the AI generated results before sharing or using them, ensuring that they do not contain errors, sensitive information or inappropriate content that could affect third parties or the Group's reputation.

III. Risk of infringing third-party rights → Respect copyright, trademarks, patents and other intellectual or industrial property rights of third parties at all times.

IV. Risk of generating offensive or discriminatory content → Act ethically and responsibly, avoiding the generation of outputs that may be discriminatory, offensive, or harmful to individuals or the Group, in line with the equality and non-discrimination commitments in the Code of Ethics.

V. Risks of data exposure or system breaches → When using external platforms, follow the security best practices defined by the IT/CISO Department and stay informed about risks, ethical principles and safe AI usage recommendations.

VI. Risk of discriminatory bias → Critically review results to identify potential biases and provide regular feedback to internal managers (IT/CISO, DPO or Compliance) regarding the functionality and effectiveness of the tools, in order to improve their accuracy and utility.

The use of artificial intelligence also entails a series of rights and responsibilities that must be observed by every Professional:

- Right to an explanation: Professionals have the right to request and receive an explanation regarding decisions or outputs generated by AI tools (AIT) that have a

direct impact on their work or employment conditions. This right ensures transparency and fosters trust in interactions with such tools.

- Personal responsibility: Each professional is responsible for using AI ethically and safely, acting with due diligence when reviewing and applying the results obtained, and complying with all the risks, principles and guidelines set out in this Policy.

- Responsibility for reporting incidents: Each Professional must immediately report any security breach, misuse or suspected mishandling of data to the information security managers (IT Department/CISO), the Data Protection Officer (DPO) or through the channels enabled on the Employee Portal and Secuoya's Ethics Channel, following the procedures established in the Security Breaches Policy. Reports should be submitted via the Incident Management or Helpdesk tool (https://helpdesk.secuoyacontentgroup.com/), through which incidents related to IT and Information Security are managed.

7. TRAINING

To ensure the responsible and safe use of artificial intelligence, Secuoya will provide the necessary training solely to Professionals and Collaborators who use AI tools provided or approved by the Group, integrating it into the annual training plans of the units concerned.

Each professional with access to corporate AI tools must:

- Receive initial training, delivered or coordinated by Secuoya, on the use of the tools they employ, associated risks, ethical principles and applicable security standards.

- Stay up to date with regulatory or technical changes as determined by the IT Department or the Compliance area.

- Apply the knowledge in their daily work, reviewing AI generated outputs and acting in accordance with Secuoya's principles and guidelines.

- In case of any doubts, consult with the Compliance Department, the DPO or IT Management following the established internal channels.

8. SUPERVISION, CONTROL AND REVIEW

Secuoya will establish mechanisms for supervision and control to ensure that the use of artificial intelligence by its Professionals is conducted responsibly, ethically and in accordance with this Policy. These mechanisms shall include, at a minimum, the following elements:

- Management guidelines: Clear criteria will be defined for identifying and managing risks associated with AI, through specific policies, training sessions, and informational briefings. These guidelines will ensure that all Professionals are aware of the applicable standards of security, privacy, and ethics.

- Periodic review: Regular evaluations of AIT usage will be conducted, including risk assessments, incident reviews, and best practices, with the aim of continuously improving this Policy and its application. AI tool usage must be documented, specifying the purpose and version used, for traceability and accountability purposes.

- Policy update: The Policy will be reviewed and updated on a regular basis to adapt to regulatory, technological or strategic changes, ensuring that it remains useful and effective for all Group's Professionals.

- Incident management: Any incident, security breach or misuse of AI must be reported immediately to the IT/CISO Department or, where appropriate, to the Data Protection Officer (DPO), using the designated internal channels (Employee Portal and Ethics Channel). The Supervisory and Control Body (OSC) will receive regular information on relevant incidents in order to carry out its monitoring functions.

- CISO functions: The Chief Information Security Officer (CISO) is responsible for coordinating the technical security assessment of AIT, keeping the corporate AIT Inventory up to date, managing reported incidents and providing the Supervisory and Control Body (OSC) with the necessary reports for oversight and control.

9. APPROVAL AND ENTRY INTO FORCE

This Policy on the Responsible Use of Artificial Intelligence was approved by the Board of Directors of Secuoya on 19 December 2025, as recorded in the corresponding minutes.

The Supervisory and Control Body (OSC), as the compliance oversight body, may propose to the Board of Directors any amendments it deems necessary to maintain adequate control over the Group's activities, ensure compliance with applicable legislation and internal procedures, and minimise the risk of non-compliance.

Furthermore, the Policy will be progressively aligned with the European regulatory framework established by the Regulation (EU) on Artificial Intelligence (AI Act) and with applicable sector-specific regulations, including future rules governing the use of AI in the audiovisual and artistic sectors, and will be reviewed as implementation phases advance or new specific provisions are adopted.

Any update or modification to this Policy must also be approved by the Board of Directors and will come into force on the date indicated in the approval agreement, remaining in force until it is expressly replaced, modified or repealed.