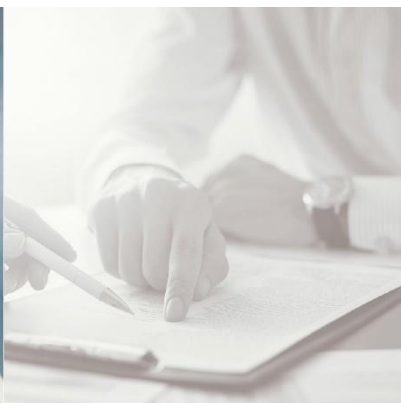


Artificial Intelligence Use and Governance Policy
September/2026



Contents

1. Introduction 3

2. Purpose 3

3. Scope 3

4. Operating principles 4

5. Governance, control and risk management 5

6. Artificial Intelligence Use and Governance Programme 6

7. Approval, effective date and dissemination 8

1. Introduction

The Board of Directors of Cirsa Enterprises, S.A. (“**CIRSA**” or the “**Company**”) considers that promoting and developing a culture of responsible artificial intelligence use is essential to the sustainable development of its business model, innovation, operational efficiency and long-term value creation at Cirsa Enterprises, S.A. and its subsidiaries (the “**CIRSA Group**” or the “**Group**”).

Artificial intelligence offers significant opportunities to improve processes, services, information analysis, automation, fraud prevention, customer service, responsible gaming and decision-making support. However, its use may give rise to legal, ethical, technological, operational and reputational risks, and risks affecting people’s rights, which must be appropriately identified, assessed and managed.

For the purposes of this Policy, an artificial intelligence system means any system or software capable of generating content, making predictions, classifications or recommendations, or assisting decision-making through machine learning techniques, generative models, algorithmic rules or other automated processing methods. Generative artificial intelligence means artificial intelligence capable of creating text, images, audio, video, code or other content from instructions or input data.

This Policy shall be interpreted consistently with the CIRSA Group’s corporate governance system and its internal policies on regulatory compliance, privacy, information security, cybersecurity, responsible gaming, sustainability, contracting with third parties and other applicable internal rules.

2. Purpose

This Artificial Intelligence Use and Governance Policy (the “**Policy**”) establishes the principles, general guidelines, minimum rules of use and responsibilities that shall guide the design, development, acquisition, implementation, oversight and use of artificial intelligence systems within the CIRSA Group.

Its purpose is to promote innovation and efficiency in a safe, ethical, transparent and proportionate manner, in compliance with applicable legislation, including, in particular, European artificial intelligence regulation, personal data protection legislation, gaming regulation, consumer and user legislation, digital services legislation and applicable cybersecurity and information security requirements.

The Policy also seeks to ensure that artificial intelligence is used as a tool for support and improvement, without replacing the responsibility, professional judgement and oversight of the CIRSA Group’s competent individuals and bodies.

3. Scope

This Policy applies to the CIRSA Group and is binding on all individuals, departments, units and companies involved in the design, development, acquisition, implementation, oversight or use of artificial intelligence systems in the course of their professional activities.

The use of artificial intelligence systems encompasses any application or solution using artificial intelligence techniques in the Group’s activities, including generative artificial intelligence tools, predictive analytics systems, machine learning, advanced automation,

recommendation engines, decision-support systems, virtual assistants, chatbots and any other technology based on artificial intelligence.

These systems may be applied, among other areas, to land-based casino operations, online gaming and sports betting platforms, marketing, personalisation and customer management, fraud prevention, security, customer service, digital channels, data analysis, internal process automation, document management, legal, financial or administrative support, and decision-support tools.

This Policy applies both to artificial intelligence systems developed internally and to those provided by third parties, including technology providers, partners, consultants or other entities with which the CIRSA Group has contractual relationships. Such third parties shall be encouraged to act in accordance with the principles and guidelines established in this Policy, incorporating the relevant requirements into contractual agreements where appropriate.

Without prejudice to the foregoing, Group companies may develop internal rules, specific procedures, operational guidelines or instructions for use that give effect to this Policy, provided that they comply with its content, principles and minimum standards of conduct.

4. Operating principles

The design, development, implementation, acquisition and use of artificial intelligence systems within the CIRSA Group shall be governed by the following principles:

- **Legality and regulatory compliance.** Artificial intelligence systems shall at all times be used in accordance with applicable legislation and the Group's internal policies, particularly regarding personal data protection, gaming regulation, consumer and user rights, cybersecurity, intellectual property, trade secrets, anti-money laundering, competition law and artificial intelligence.
- **Human-centred approach and user protection.** Artificial intelligence systems shall be used as tools to serve people, with full respect for human dignity, fundamental rights and the legitimate interests of customers, users, employees and other stakeholders.
- **Transparency, traceability and explainability.** CIRSA shall promote the transparent use of artificial intelligence systems and, where appropriate, their explainability, ensuring traceability of their operation, documentation of significant uses and identification of automated interactions where relevant to the user.
- **Data protection, confidentiality and security.** Data processing shall comply with the principles of lawfulness, fairness, transparency, minimisation, accuracy, purpose limitation, confidentiality, integrity and security, adopting appropriate measures to prevent unauthorised access, misuse, information leaks or risks compromising the Group's systems and information.
- **Bias prevention and non-discrimination.** The development and use of artificial intelligence systems that avoid unjustified bias, discriminatory outcomes or unintended effects on individuals or groups shall be promoted, particularly where these may affect users, customers, employees or third parties.
- **Human oversight, control and accountability.** Systems with a significant impact on users, employees, third parties or the business shall be subject to appropriate human oversight.

Ultimate responsibility for any business decision shall always rest with the Group's competent individuals or bodies and may not be transferred to artificial intelligence systems.

- **Quality, accuracy and verification of outputs.** Outputs generated by artificial intelligence systems shall be reviewed before use whenever they may have significant internal or external effects. Users shall not assume that AI-generated content is complete, up to date, accurate or legally valid without appropriate verification.
- **Proportionality, necessity and sustainability.** The use of artificial intelligence shall be appropriate, necessary and proportionate to the intended purposes, avoiding excessive or unnecessary processing and promoting efficient use of technological resources, considering their environmental impact where possible.
- **Prohibited uses.** The use of artificial intelligence systems contrary to applicable legislation, this Policy or corporate values is prohibited, including systems intended for improper manipulation, exploitation of vulnerabilities, discrimination, unlawful use of data, infringement of intellectual or industrial property rights, generation of misleading, fraudulent or harmful content, or automated decision-making without the required oversight.

5. Governance, control and risk management

An appropriate governance model shall be established to ensure the responsible, secure and legally compliant use of artificial intelligence systems, ensuring their alignment with the principles set out in this Policy and with the Company's corporate governance system.

The Board of Directors is responsible for approving this Policy and for ultimate oversight of the use of artificial intelligence, ensuring that such use is consistent with the Group's strategy, corporate values and commitments to sustainability, regulatory compliance and responsible gaming.

The Sustainability, Technology and Innovation Committee shall oversee the effective implementation of this Policy, ensuring that artificial intelligence use is aligned with the principles of sustainability, technological innovation, user protection and long-term value creation.

The CIRSA Group shall also appoint an Artificial Intelligence Use and Governance Committee with the following duties: implementing compliance with this Policy, assessing AI use cases, conducting risk analyses, promoting good practices and training, and coordinating compliance with Regulation (EU) 2024/1689 on Artificial Intelligence.

The Corporate Organisation and Systems Department, or whichever department assumes its functions at any given time, shall be responsible for promoting the development, implementation, approval and maintenance of artificial intelligence systems in accordance with the security, quality, resilience, interoperability and control standards established by the Group.

The Compliance function, in coordination with Legal, Data Protection, Information Security and the relevant departments, shall ensure that artificial intelligence uses comply with applicable legislation, particularly regarding data protection, gaming regulation, consumer rights, cybersecurity, risk prevention and good market practices.

Department heads shall identify artificial intelligence uses within their remit, ensure that authorised or validated tools are used, ensure human oversight of outputs,

promote compliance with this Policy and report incidents, risks or assessment needs where appropriate.

Users shall use only tools authorised or permitted by the Group, verify the accuracy and suitability of generated outputs, protect confidential information and personal data, refrain from entering unauthorised information into external tools, and report incidents, significant errors or inappropriate uses.

A risk-based approach shall be adopted for the design, development, acquisition, implementation and use of artificial intelligence systems. Systems shall be classified according to, among other factors, their purpose, level of automation, types of data used, potential impact on people, effect on the business and level of regulatory or reputational exposure. This classification shall be based on the categories and obligations laid down in the applicable European legislation, namely Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024.

As a general rule, the Group shall distinguish between systems presenting unacceptable risk, high risk, limited risk and low or minimal risk. The development, acquisition or use of systems presenting unacceptable risk is prohibited. Higher-risk systems shall be subject to prior assessments, enhanced validation, human oversight, appropriate documentation and continuous monitoring and follow-up mechanisms.

Artificial intelligence systems shall be managed throughout their lifecycle, from design or acquisition to review, updating or withdrawal. Before they are put into operation, their necessity, proportionality, purpose, associated risks, types of data used, security measures and compliance with applicable legislation shall be assessed.

Depending on the level of risk, proportionate control, oversight and audit mechanisms shall be implemented. These may include impact assessments, system registers, technical and functional documentation, decision traceability, review by internal control functions, incident management and, where appropriate, external or independent assessments.

6. Artificial Intelligence Use and Governance Programme

The CIRSA Group shall establish an Artificial Intelligence Use and Governance Programme (the “Programme”) to give operational effect to the principles established in this Policy and ensure the ethical, secure and transparent use of artificial intelligence systems throughout its activities, in compliance with applicable legislation.

The Programme shall incorporate control, oversight, training and continuous improvement mechanisms throughout the lifecycle of artificial intelligence systems, to protect customers, users, employees and other stakeholders, and prevent regulatory, operational, reputational, technological and sustainability risks.

Under the Programme, the CIRSA Group shall adopt, among others, the following measures:

- **Inventory and register of artificial intelligence systems.** Identification, classification and documentation of significant artificial intelligence systems used within the Group, including their purpose, internal owner, provider, data used, authorised users, risk level and applicable controls.
- **Approval of tools and permitted uses.** Definition of criteria for authorising artificial intelligence tools and use cases, distinguishing between permitted, restricted and prohibited uses. As a general rule, permitted uses may include drafting, summarising and analysing information, automating administrative tasks,

decision-making support and generating non-critical content, always subject to human review where appropriate.

- **Restricted access to sensitive artificial intelligence capabilities.** Restriction of access to capabilities involving sensitive data, advanced profiling, behavioural analysis, biometric technologies or other tools with a significant impact on users, limiting access to authorised personnel and subjecting it to prior risk assessment.
- **Information protection rules.** Prohibition on entering confidential or strategic information, unnecessary personal data or specially protected data into unauthorised tools. Application of the principles of minimisation, necessity, confidentiality and security to all data processing using artificial intelligence.
- **Appropriate identification of artificial intelligence use.** Informing the user or recipient where relevant, particularly in automated interactions or processes that may significantly affect their rights or interests.
- **Mechanisms for reviewing automated decisions.** Ensuring human intervention where the user, employee or third party may be significantly affected, including, where applicable, channels to request review or challenge the outcome of automated decisions with a significant impact.
- **Continuous monitoring and model control.** Detection of operational deviations, loss of accuracy, performance degradation, emerging bias or unforeseen impacts, adopting the necessary corrective measures, including updating, recalibration, suspension or withdrawal of the system.
- **Periodic bias, fairness and quality assessments.** Assessments designed to avoid discriminatory or unintended effects, particularly in systems involving gaming behaviour analysis, customer segmentation, fraud prevention, marketing, customer service or other areas with potential impact on users.
- **Impact measurement and monitoring.** Monitoring the contribution of artificial intelligence systems to operational efficiency, service quality, responsible gaming policies, risk identification and mitigation, efficient use of technological resources and continuous improvement.
- **Training and awareness.** Training and awareness programmes for employees, managers and collaborators, tailored to their profile and level of responsibility, addressing the capabilities and limitations of artificial intelligence, risks, privacy, security, regulatory compliance, use of authorised tools and good practices.
- **Responsible third-party management.** Inclusion, where appropriate, of suitable contractual clauses on regulatory compliance, data protection, confidentiality, security, resilience, oversight, documentation, assistance, subcontracting, auditing and system withdrawal or replacement.
- **Incident and breach management.** Establishment of channels and procedures to report incidents, significant errors, unauthorised uses or breaches of this Policy. Non-compliance may lead to disciplinary measures under internal rules and, where applicable, appropriate legal action. Incidents involving artificial intelligence systems shall be managed under a specific protocol covering, at a minimum, identification and reporting, impact and criticality assessment, containment and mitigation, investigation of causes, corrective measures, documentation and closure, and escalation to the competent bodies where necessary. This protocol shall be coordinated with corporate procedures for incident management, cybersecurity, data protection, regulatory compliance and business continuity.

The Programme shall be reviewed at least annually, unless the Sustainability, Technology and Innovation Committee requires more frequent reviews. Reviews shall assess its effectiveness, identify opportunities for improvement and adapt it to regulatory, technological and business changes. The Group may also consider adopting international standards, good market practices or external assessments that strengthen the Programme's reliability, transparency and continuous improvement.

7. Approval, effective date and dissemination

The Artificial Intelligence Use and Governance Policy in relation to stakeholders was approved by the Board of Directors of Cirsa Enterprises, S.A. at its meeting on 25 September 2026 and took effect on that date.

Its content shall be reviewed periodically, where appropriate, to adapt it to regulatory changes or incorporate best practices in this area. Its latest review took place on 28 July 2026. The Board of Directors shall be the body authorised to amend it, following oversight by the Sustainability, Technology and Innovation Committee.

The Policy shall be available on the Group's intranet. It shall also be made available to third parties through publication on CIRSA's website.

The Spanish version of this document will prevail in the event of any discrepancy or dispute.

CIRSA
Ctra. de Castellar, 298
08226 Terrassa. Barcelona. Spain
T. 34 93 728 33 18
info@cirsa.com
www.cirsa.com

