CIRSA

Whistleblowing Channel Operating Policy

September 2026



Contents

1. Purpose 3

2. Scope of application 3

3. ’s Principles of Conduct 3

4. Channels of communication 4

5. How it works 4

6. Protection of the whistleblower 6

7. Responsibilities 6

8. Data protection, processing and retention 7

9. Communication and dissemination 7

10. Approval, validity and dissemination 7

11. Appendices 9

1. Purpose

The CIRSA Group (the "Group" or "CIRSA") is committed to upholding the highest ethical standards in all its operations and to complying with all applicable laws and regulations. To support this commitment, this Whistleblowing Channel Operating Policy (the "Policy") has been established to enable directors, managers, employees, suppliers, customers and any other interested parties to report any behaviour that may be inappropriate or unlawful without fear of reprisal.

This Policy is based on the European Whistleblowing Directive 2019/1937 of the European Parliament and of the Council of 23 October 2019 and its transposition into Spanish law through Act 2/2023 of 20 February, which regulates the protection of persons reporting regulatory breaches and combats corruption (the "Act 2/2023"), in compliance with the provisions of Article 5.2.h) of the said Act 2/2023. Furthermore, the local requirements and specific circumstances of the countries in which the Group operates will be taken into account, as well as international best practice in this area.

2. Scope of application

This Policy is binding on all members of the Board of Directors, senior management and all other employees of CIRSA, as well as on all those subject to their authority, to the extent applicable. Furthermore, it is binding and applies to all companies in which CIRSA holds, directly or indirectly, a majority of the shares, holdings or voting rights, or in which it has appointed, or has the power to appoint, the majority of the members of the governing or administrative body, such that it effectively controls the company.

Finally, CIRSA's directors, senior managers and employees, to whom other sector-specific rules or policies, or those derived from the national legislation of the countries in which they operate, may additionally apply, shall also comply with them.

3. 's Principles of Conduct

In accordance with the operating principles set out in the aforementioned regulations and to ensure the effective implementation of communication channels, this Policy provides for the development of the scope and content of procedures and the handling of communications based on the following principles of conduct:

1) It allows for communications to be made in writing, as well as by analogue and electronic means, and also in person if the whistleblower so requires;
2) It ensures that communications may be made anonymously;
3) Ensures the prompt processing of all communications (including anonymous ones);
4) Guarantees acknowledgement of receipt of the communication within a maximum of 7 days;
5) Ensures that reports received are analysed equally, regardless of who the whistleblower is;
6) Guarantees the confidentiality of the information contained in communications, paying particular attention to details relating to the whistleblower's identity and other personal data;
7) It allows for the ad hoc appointment of an investigation team, as well as the appointment of a case manager who will process the communications and maintain contact with the informant. Where necessary, they will be responsible for requesting further information and providing a response;
8) It establishes a general time limit of 3 months to respond to the whistleblower regarding the processing of the report, starting from the date of acknowledgement of receipt; and

9) Ensures that there are no reprisals or any kind of negative consequences for the whistleblower, provided they act in good faith.

4. Channels of communication

As part of the Group's compliance culture, a platform known as the Whistleblowing Channel (the "Channel") has been introduced. This tool enables compliance with European and local regulations in all countries where the Group operates, allowing for the anonymous – if desired – and confidential reporting of possible irregularities of potential significance that may occur within CIRSA or on its behalf.

In addition to the Whistleblowing Channel, anyone wishing to contact CIRSA to make enquiries or report any situation may do so by writing to the Corporate Compliance and Business Ethics Department at the following postal address:

CIRSA Servicios Corporativos, S.L.

Corporate Compliance and Business Ethics Department – Corporate Compliance Officer

Carretera de Castellar, 298

08226 – Terrassa (Barcelona) Spain

Annex I contains the postal addresses in each of the countries where the Group operates.

In some countries where the Group operates, it is possible to channel communications through various public bodies. These bodies, referred to as Independent Whistleblower Protection Authorities, are detailed in Annex II of this Policy.

At the whistleblower's request, a report may also be made in person at a meeting, which must take place within a maximum of 7 days of the request being made. In this case, the meeting must be recorded or transcribed, in full compliance with data protection regulations.

Generally speaking, if a report is submitted via a channel or means of communication, or through a person other than those indicated above – for example, verbally to a line manager – it must be forwarded to the Corporate Compliance and Business Ethics Department within a maximum of 7 days of receipt, with simultaneous notification of the forwarding to the whistleblower.

5. How it works

5.1. Who can use the Whistleblowing Channel?

The Whistleblowing Channel is available to any employee of the CIRSA Group who wishes to report a possible breach, as well as to other individuals who, whilst not employees, are aware of the possible existence of any breach in their professional and/or commercial dealings. Specifically, it applies to:

- Employees and former employees.
- Self-employed individuals.
- Shareholders.
- Members of the CIRSA Group's board of directors, management or supervisory body.
- Suppliers, contractors and subcontractors.
- Legal representatives of employees or intermediaries.
- Volunteers.
- Trainees.

- Employees undergoing training or recruitment.
- Individuals related to the informant, such as work colleagues, partners or family members.
- Legal entities for which the whistleblower works or in which they hold a significant stake, and which operate within the same workplace context.

5.2.What can be reported under this Policy?

Any breach of CIRSA's Code of Ethics, as well as any regulations that may be the subject of a report via the Whistleblowing Channel. The Channel platform itself details various specific scenarios that constitute the types of reports that can be made, as well as the possibility of seeking advice or raising queries regarding conduct within the Group's professional environment. Specifically, the different types of reports covered by the Channel are as follows:

- Money laundering
- Corruption or bribery
- Employment issues
- Discrimination or harassment
- Breaches of accounting, financial and tax regulations
- Data protection
- Insider dealing
- Information security
- Conflict of interest
- Other unethical behaviour

Anyone who deliberately and knowingly communicates incorrect or misleading information will not receive the Organisation's support or protection. Furthermore, each specific case will be analysed with a view to imposing proportionate disciplinary measures against anyone who communicates information in bad faith.

Finally, it is important to note that the Channel is not the appropriate means for reporting emergencies or situations requiring an immediate response

5.3.What information should be provided when submitting a report?

The information provided must be as complete and accurate as possible. The whistleblower must therefore share all the information they have regarding the possible breaches. Furthermore, it is preferable to provide, or for the report to clearly refer to, any evidence or documents supporting the claim. This enables the case to be handled as quickly and effectively as possible.

5.4.What happens when a report is received?

CIRSA has defined a procedure for handling reports received via the Whistleblowing Channel, which sets out in detail all the steps taken once a report is received, as well as the various responsibilities involved. The main stages of this process are summarised below:

- Receipt of the report: all reports will be received by the Whistleblowing Channel managers designated in each country, as well as by the head of the Whistleblowing Channel.
- Registration and acknowledgement of receipt: an acknowledgement of receipt will be sent to the person making the report within 7 calendar days of receipt, and the report will be duly registered on the Whistleblowing Channel platform, ensuring its confidentiality.

- Preliminary analysis: the content of the report will be analysed and a decision made as to whether it meets the requirements for acceptance; further information or clarification regarding the facts reported may be requested from the whistleblower.
- Investigation and report: once the report has been accepted, an investigation into the alleged facts will be launched, if necessary. This will be conducted in accordance with the principles of impartiality, equality, independence and honesty and will culminate, depending on the complexity of the case, in the issuance of a report by those leading the investigation, which will be forwarded to the Channel Manager. This phase may not exceed 3 months from the date of receipt of the report; however, it may be extended by a further 3 months should the facts involved be particularly complex.
- Closure and follow-up: once the investigation has been carried out and the report drawn up, where necessary, the appropriate corrective or disciplinary measures will be proposed; the results will be communicated, as far as possible, to all parties involved; and a follow-up system will be established to assess the effectiveness of the actions taken.
- Conflict of interest: in cases where the report directly or indirectly affects any of the Channel's managers, the Channel Manager or a member of the Compliance Body, the person concerned shall be automatically excluded from any action relating to the analysis, investigation, decision-making or follow-up of the case. In such circumstances, the handling of the report will be undertaken by unaffected individuals or bodies who can guarantee the independence, objectivity and impartiality of the process.

6. Protection of the whistleblower

CIRSA undertakes to protect any person who reports unethical or illegal behaviour in good faith from any form of retaliation. Retaliation is understood to mean any act or omission that is prohibited by law or under the Group's regulatory framework, or which, directly or indirectly, constitutes unfavourable treatment that places those subjected to it at a particular disadvantage compared to others in the workplace or professional context, solely because of their status as whistleblowers or because they have made a report.

CIRSA does not tolerate any form of retaliation. This includes threats or any other form of intimidation directed at a whistleblower.

7. Responsibilities

The following is a summary of the various responsibilities arising from the implementation of this Policy, which are set out in detail in the procedure for handling reports received via the Whistleblowing Channel:

- Board of Directors: CIRSA's Board of Directors (BoD), through the Audit and Compliance Committee (ACC), is responsible for overseeing the operation of the Channel. To this end, the compliance function, through the Corporate Compliance Officer, will report at least once a year to the Audit and Compliance Committee on the progress and nature of the communications received, distinguishing, amongst other aspects, their geographical distribution.
- Compliance Body (OdC): in each country where CIRSA operates, this collegiate body has been established to oversee the local Whistleblowing Channel.
- Corporate Compliance Officer: the CIRSA Group's Compliance Officer has been appointed as the person responsible for the overall operation of the Channel.

- **Local Channel Manager:** In each country, a local Channel Manager has been appointed who is responsible, amongst other things, for receiving, analysing and managing the Channel in the relevant country, as well as for developing training programmes in this area to raise awareness of and promote the Channel. Furthermore, regular reporting lines have been established to both the Corporate Compliance Officer and the Channel Manager Corporativo.
- **Corporate Channel Manager**: in addition to the functions defined for local managers – in this case, those based in Spain – the Corporate Channel Manager will report to the Corporate Compliance Officer on the number and type of complaints and enquiries received, the average resolution times and their geographical distribution.

8. Data protection, processing and retention

In the management of the Channel, compliance shall be ensured with the legal regulations on the protection of personal data applicable to the various geographical areas and companies within the Group. In particular, the following aspects shall be taken into account:

- All companies must implement the personal data security measures that are applicable in accordance with the risk level established for the Channel and, where applicable, the measures that are mandatory under the relevant legislation in each country and the Group's internal regulations on this matter. The level of security must be, at a minimum, equivalent to that provided for in the data protection compliance system for sensitive or special-category data.

Adequate compliance with the processing of personal data must be ensured, particularly with regard to the rights of data subjects to be informed about the processing of their data. All of this must be carried out in accordance with the applicable legislation in each country.

9. Communication and dissemination

For the Policy to function properly, it is essential that both those responsible and the rest of the organisation are aware of the applicable regulations. For this reason, the CIRSA Group envisages, amongst others, the following communication measures in this regard:

a) When new employees join the CIRSA Group, they will be informed about the measures established in this regard.

b) Any updates on this matter deemed relevant will be communicated to employees via the CIRSA Group's usual communication channels.

Furthermore, employees will have permanent access to all the CIRSA Group's procedures, policies and/or regulations, including this Policy.

In addition, awareness-raising and training initiatives will be promoted regarding the Whistleblowing Channel and, in particular, the safeguards and protections for whistleblowers.

10. Approval, validity and dissemination

The Operating Policy for the Whistleblowing Channel has been approved by the Board of Directors of CIRSA Enterprises, S.A. at its meeting on 25 September 2026 and came into force on the same date.

Its content will be subject to periodic review where appropriate, in order to adapt it to regulatory changes or incorporate best practice in this area; the most recent review took place on 28 July 2026. The aforementioned Board of Directors shall be the competent body for amending the Policy, subject to prior oversight by the Audit and Compliance Committee.

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

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

11. Appendices

11.1. Appendix I: Postal addresses of the countries in which the Group operates:

Panama

Gaming & Services de Panamá, S.A. – Compliance Department

Calle 50 and 58, PH Torre Global, 40th Floor

081600597 – Panama City

Colombia

Winner Group, S.A. – Compliance Department

90th Street, No. 19 C – 32, Blue Tower Building – Office 401

Santa Fe de Bogotá DC (Bogotá).

Mexico

Promociones e Inversiones de Guerrero, S.A.P.I. de C.V. – Compliance Department

Samara Shops Corporate Headquarters

70 Antonio Dovali Jaime, Tower B, 3rd Floor, Office 1

Santa Fe neighbourhood – Álvaro Obregón borough

01376 – Mexico City (Mexico DF).

Italy

Cirsa Italia Holding, S.P.A. – Sole Data Controller

Via Ludovico il Moro, No. 6/C, Palazzo Ferraris

20079 – Basiglio (Milan).

Italy – E-Play

E-PLAY24 ITA Ltd – Sole Complaints Handler

Piazzetta Business Plaza, Level 1, Office 3, Triq Ghar Il-Lembi,

Sliema SLM1605 (Malta).

Peru

Gaming and Services S.A.C. – Compliance Department

Avda. Ricardo Palma, No. 341, 2nd Floor, Room 201

15074 – Miraflores (Lima).

Peru – Apuesta Total

FREE GAMES SAC – Compliance Department

Avda. Manuel Olguin, No. 211, Office 1101, Omega Tower

Santiago de Surco, Lima, Peru.

Dominican Republic

SCB Grand Victoria Dominicana, S.R.L. – Compliance Department

Avenida Abraham Lincoln, on the corner of Avenida Correa y Cidrón

10109 – University District (Santo Domingo).

Costa Rica

Grupo Cirsa de Costa Rica, S.A. – Compliance Department

La Sabana Executive Business Centre, Tower 6, 3rd Floor

Sabana Norte – San José.

Morocco

Société du Casino Le Mirage, S.A. – Compliance Department

Club Valtur STB, Plot No. 31

80000 Agadir.

Portugal

SFP Online, S.A. – Compliance Department

Rua Dr. Calado, No. 1

3080-153 Figueira da Foz (Portugal).

11.2. Annex II: Channels of communication with public bodies

Any communication relating to this Policy, or if you have any further queries or comments, may also be made, where deemed necessary and appropriate, via one of the channels listed below:

Spain:

1) Independent Whistleblower Protection Authority (AIPI): https://www.proteccioninformante.gob.es/
2) Anti-Fraud Office of Catalonia (OAC): https://antifrau.cat/es/es
3) Valencian Anti-Fraud Agency (AVA): https://www.antifraucv.es/
4) Andalusian Anti-Fraud Office (OAAF): https://antifraudeandalucia.es/
5) Executive Service of the Commission for the Prevention of Money Laundering and Monetary Offences (SEPBLAC): https://sepblac.es/es
6) Spanish Data Protection Agency (AEPD): https://aepd.es/es
7) National Commission for the Market and Competition (CNMC): https://cnmc.es

Italy:

National Anti-Corruption Authority (ANAC): https://www.anticorruzione.it/

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