CIRSA

ETHICS HOTLINE CHANNEL OPERATING POLICY

2021

CONTENTS

1. INTRODUCTION

1.1. Rationale for the reform

The CIRSA Group champions the principles of ethics, integrity, respect for the law, transparency and honesty and rejects any kind of wrongful conduct. Our operations are designed to make sure that everyone who is part of the company strictly complies with the law at all times and in every place where these operations are carried out. Likewise, and as stipulated in the Group's Code of Conduct, it upholds strict compliance with the company's commitments and obligations in relations with customers, suppliers, partners and its surroundings in general. This is the foundation for preventing any potentially unlawful actions which would have a significant impact on the company's reputation and its business.

Against the background of the culture of compliance prevailing throughout the Group and as part of the continuous improvement plans on compliance policies it is rolling out, a new platform has been set up to host the company's Ethics Hotline Channel. This channel means we can continue to comply with the new European directives, enhance the Group's high standards of regulatory compliance and maintain a firm commitment to society in general since the platform makes it possible to report confidentially, anonymously if so desired, and any potentially significant irregularities which may take place in the company or in its name.

This compliance is one of the reasons why the company is a leader in its industry and a benchmark in business.

1.2. Regulatory background

An Ethics Hotline Channel is a key component in regulatory compliance and occupational health and safety models. Thus, under Article 31(a)(5)(4) of the Criminal Code, "organisation and management models (...) shall include the obligation to report any potential hazards and breaches to the body responsible for monitoring the operation and observance of the risk prevention model". Similarly, Article 31(a)(5)(5) of the Criminal Code stipulates that there must be a compliance-related disciplinary system when it says that "(...) organisation and management models (...) shall establish a disciplinary system which appropriately punishes non-compliance with the measures laid down in the model". Both issues are addressed in the preparation of this Policy in order to effectively comply with legal requirements.

From the point of view of the CIRSA Group's internal regulations, this Policy is to be considered an integral part of the Group's Global Compliance Management System. CIRSA would like to make it clear that the Ethics Hotline Channel Operating Policy is not intended to replace the competencies of its regular management departments. Relations between them are thus to be based on complementarity, coordination and collaboration in order to achieve the best possible outcomes.

This Policy's content and structure follow the guidelines set out in the following regulations:

Firstly, it complies with Circular 1/2016 of the Public Prosecutor's Office of 22 January on the criminal liability of legal entities pursuant to the amendment of the Criminal Code by Act 1/2015, which states that companies must have in place appropriate internal regulations specifically protecting whistleblowers to ensure company employees can report potentially unlawful conduct.

It also complies with ISO 37001 on Bribery and Corruption Management Systems, which includes a special reference to the process to be followed in the investigation of reports, pointing out the need to draw up internal procedures for reports that ensure: (i) the effectiveness of the actions carried out, (ii) the proficiency of the persons in charge of the investigation, (iii) the need to ensure the involvement and cooperation of other units, and (iv) the confidentiality of the report, the investigation and the decision.
Meanwhile, ISO 37301 for Compliance Management Systems stipulates the need for whistleblowing channels. Thus in the section about raising concerns, it states: "even where not required by local regulation, organisations should consider developing a whistleblowing mechanism that allows anonymity or confidentiality through which

employees and actors of the organisation can report or seek guidance in terms of compliance breaches without fear of retaliation". This standard additionally specifically refers to the requirements and recommendations included in ISO 37002 on whistleblowing management systems and whistleblowing channels which has been used as a basis for drawing up this Policy.

Also significant in this field is legislation on data protection and safeguarding whistleblowers, especially following the protection of whistleblowers under Directive (EU) 1937/2019 of 23 October 2019 on the protection of persons who report breaches of Union law. This Directive is designed to enable whistleblowers to report any possible breaches of EU law in an organisation both internally and to the authorities via channels which ensure the safety of the whistleblower without fear of retaliation from the company.

Hence in compliance with the Directive's requirements and to set up regular and alternative internal reporting channels, this CIRSA Group Ethics Hotline Channel Operating Policy sets out the scope and content of whistleblowing procedures and processing. In this respect, it lays down the following requirements:

1. Reports may be made in writing and by analogue and electronic means and also in person if the whistleblower so wishes;
2. Acknowledgement of receipt of the report within at most seven days;
3. The Compliance Body may appoint a special Investigation Team until the case is completed and also appoint a case manager who will process the report and liaise with the whistleblower. They will be responsible for asking for additional information and providing a response where necessary;
4. Diligent handling of all reports (including anonymous reports);
5. A general deadline of three months from the acknowledgement of receipt to respond to the whistleblower on the handling of their report.

Finally, section 24 of Spain's Data Protection and Digital Rights Safeguards Act 3/2018 specifically addresses some key issues concerning internal whistleblowing information systems which are outlined below.

Firstly, that notifications or reports may be anonymous. Secondly, it includes a duty to inform employees or third parties of the existence of these information systems ("Ethics Hotline Channel"). Furthermore, it specifies that access to data should be restricted to people who have internal control and compliance duties, irrespective of whether or not they are members of the organisation, and to data processors. This does not affect access by other persons or any possible disclosure of data to third parties or to the authorities when required for taking disciplinary measures or conducting legal proceedings. Importantly, it also states that the identity and confidentiality of the data

of the people concerned must be safeguarded, in particular the data of the person who has submitted the report if they have not made it anonymously.

Finally, on the issue of the option of filing anonymous reports, Supreme Court Ruling 272/2020 of 6 February stresses and validates anonymous reporting to identify potential criminal offences which can be corroborated, as is the case in this procedure, by subsequent internal and police investigation. The Court points out that: "(...) The report made is important and, in the absence of an internal regulatory compliance programme, it is particularly crucial that during the period of the facts found a mechanism for internal action is provided in the company, recently regulated in the 'internal whistleblowing channel' which has been included in the recent Directive (EU) 2019/1937 of the European Parliament and of the Council of 23 October 2019 on the protection of persons who report breaches of Union law."

2. PURPOSE

In order to move forward with its commitment to building a robust culture of compliance going beyond any legal obligation and anchored in values and principles, the CIRSA Group recognises the importance of adopting an internal regulation (hereinafter the "Policy"). This regulation consists of the Group's Code of Conduct and Organisation, Management and Control Model. Its purpose is to set out the obligation to use the Ethics Hotline Channel and also regulate the way of using the application hosting it (hereinafter the "platform") to provide advice and certainty in the decision-making process of any person who becomes aware of possible offences.

Accordingly, to provide the tools required to help detect any potential unlawful acts and protect everyone in the Group and its reputation with our stakeholders, the Company has improved its Ethics Hotline Channel by setting up and implementing a platform for receiving, reviewing and handling reports (hereinafter "reports") which fully safeguards confidentiality and complies with the highest information security and data protection standards. Furthermore, these reports may be made completely anonymously at the whistleblower's choice to ensure that there is no possibility of any retaliation.

To this end, the following key issues need to be identified:

1) Who does this Policy apply to?
2) What can be reported and when should reports be made?
3) How to use the CIRSA Group's Ethics Hotline Channel. Can a report be made anonymously?
4) What happens when a report is made through the Ethics Hotline Channel?
5) The CIRSA Group's Ethics Hotline Channel Operating Policy is a universal policy applicable to all companies in the Group unless there is a statutory justification for an exception to its application.

2.1. Who does this Policy apply to?

The persons bound by this Policy (hereinafter "recipients" and/or "whistleblowers") are all employees and associates of the CIRSA Group, members of its corporate bodies, customers, suppliers, partners, consultants, shareholders and in general any person who renders services for the Group on a contractual basis and also the Group's stakeholders (hereinafter "third parties").

2.2. What can be reported and when should reports be made?

2.2.1. What can you report under this Ethics Hotline Channel Operating Policy?

This Policy encourages whistleblowers to report any concerns they may have regarding potential breaches of the CIRSA Group's Global Compliance Management System consistent with the scope defined in Directive (EU) 1937/2019. This encompasses

information on breaches in a broad sense including reasonable suspicions and actual or potential offences which have taken place or are likely to take place.

Reports which may be made for this purpose include the following:

A. CORRUPTION: : breach of laws, policies, standards, guidelines and/or procedures relating to:

- Bribery/kickbacks/influence peddling: offering to or accepting from officials, authorities and others any kind of improper advantages whether in a private business or public context,

Examples: offering or accepting commissions or monetary gifts; invitation from or through business partners apparently seeking to influence a business relationship.

- Fraud/swindle: presenting false facts, data or information or omitting true facts, data or information for the purpose of gaining or attempting to gain an unlawful financial benefit either personally or for others.

Examples: issuing inflated invoices in order to keep the extra money; credit fraud; grant fraud; insurance fraud; forgery of identity documents, keys or other means of identification; tampering with machines or testing methods.

- Theft: unauthorised taking of money or other property for personal use or to give it to a third party.

Examples: theft of goods from the warehouse; retaining company funds or work materials.

- Breach of accounting and financial reporting rules/offences against tax and social security authorities: fraudulent misrepresentation of transactions, inadequate controls over an organisation's operations.

Examples: false information about income, expenditure, assets or property; fraudulent misrepresentation of transactions; destruction of supporting documents; hiding assets.

B. MONEY LAUNDERING

Breach of prevention of money laundering and terrorist financing legislation, policies, manuals and/or procedures by introducing illegally obtained money or illegally acquired assets into the legal economic and financial system.

Examples: transfer of funds through a "tax haven"; a business associate's attempt to settle all or part of a transaction in cash; indications of the business associate's ties with criminal or terrorist organisations; doubts as to the identity of the customer or suspicions that the customer is acting as a front for a third party.

C. DATA PROTECTION

Breach of data protection and telecommunications secrecy legislation, policies, manuals and/or procedures.

Examples: unauthorised collection, processing or disclosure of personal data; unauthorised technical surveillance of employees; use of data for private purposes;

using customer data for commercial purposes without their consent.

D. INFORMATION SECURITY

Breach of information security regulations, policies, guidelines and/or procedures designed to protect data from falsification, destruction and unauthorised release and to counter damage to computers or disclosure of secrets.

Examples: impairment of the security of computer systems and networks that seriously compromises the confidentiality, integrity or availability of information or equipment; disclosure of user accounts and passwords to unauthorised persons; cyberattacks.

E. UNETHICAL PRACTICES

Breach of behavioural standards and guidelines, professional obligations and legal requirements through intentional or unintentional improper practices or actions contrary to the Code of Conduct.

Examples: breaches of the Responsible Gambling Policy or Environmental Protection Policy; use of misleading advertising; drug trafficking; incidents in the normal conduct of gaming operations.

F. SEEKING ADVICE

Questions or queries can be raised about general issues related to compliance in the company and advice can be sought on these issues.

2.2.2. When should you make a report?

The CIRSA Group believes that the best way to promote whistleblowing is to build an environment where people feel comfortable about sharing any possible incidents which may infringe the Group's Global Compliance Management System. It therefore seeks to foster one in which events related to potential breaches of this System can be reported.

The environment described in the previous paragraph will comply with a principle which governs all the CIRSA Group's relations with its stakeholders: reports must always be made in good faith, which amounts to the implementation of a "culture of fairness" as required by Directive (EU) 1937/2019. This means that at the time of making the report, the whistleblower must have reasonable grounds to believe that the information they provide is true and concerns incidents which may potentially be offences.

2.2.3. What happens in emergencies?

Processing the reports submitted through the CIRSA Group's channels requires the body in charge of receiving them, i.e. the Compliance Body, to draw up a classification for internal use of the content of the reports which will make it possible to handle them appropriately. This classification is as follows:

- False report
- Human Resources

- High
- Medium
- Low
- Other

In all cases it is essential to ensure that you notify your line manager and/or the Group Compliance Officer as soon as possible so that once the facts have been reviewed, the issue can be addressed as efficiently as possible by processing the report in the way specified in the Fraud and Non-Compliance Investigation Protocol.

2.3. How to use the CIRSA Group's Ethics Hotline Channel. Can a report be made anonymously?

2.3.1. How to submit a report

Reports can be made under this Policy through any of the following channels:

a) Main channels:

1. On the public corporate website under CSR - Compliance - Ethics Hotline Channel by clicking the following link: https://www.cirsa.com/
2. On the Intranet under Shortcuts – Ethics Hotline Channel via the following link: https://cirsa.sharepoint.com/sites/es_intranet
3. Or directly via the following link: https://www.bkms-system.com/COMPLIANCE-CIRSA

b) Other channels:

4. Staff:
   i. Line manager
   ii. Member of the Compliance Body (Corporate Human Resources Director, Corporate Internal Audit Director and Corporate Legal and Compliance Director)
   iii. Member of the Compliance Unit
5. Email: compliance@cirsa.com
6. Post:
   CIRSA Servicios Corporativos, S.L.
   Área de Compliance
   Carretera de Castellar, 338
   08226 – Terrassa (Barcelona) Spain

2.3.2. What information should you provide when sending a report?

The CIRSA Group recommends that the information provided in a report should be as complete and accurate as possible. It therefore asks whistleblowers to include all the information in detail known to them regarding potential offences in their reports. Any supporting evidence or documents should also preferably be provided or the report should clearly refer to them as this will allow the case to be handled as quickly and efficiently as possible.

2.3.3. Identification when making a report: anonymity

The Ethics Hotline Channel allows reports to be made anonymously.
However, the CIRSA Group encourages whistleblowers to identify themselves by providing their name and contact details when submitting a report. This will enable the staff handling it to contact the whistleblower to ask for additional information and clarification, provide support and assistance, conduct follow-up where necessary, etc. CIRSA also considers that this is the best way of demonstrating the high standards underpinning this Policy by confirming the principle of non-retaliation when a report is made.
In this respect, it should be noted that when a (non-anonymous) report is submitted, the CIRSA Group ensures that the internal whistleblowing procedure will be performed securely to safeguard the confidentiality of the whistleblower's identity and other related information.

2.3.4 What happens when a report is made through the CIRSA Group's alternative channels?

The CIRSA Group uses a digital platform to support the administration of alternative channels as required by Directive 1937/2019.

Reports made through alternative channels are stored directly on the platform which has robust information security measures in place designed to safeguard the integrity, availability and confidentiality of the information. The platform allows the whistleblower to specify the place, date, company, division, etc. concerned together with the persons related to their report. It also provides the option of anonymous reporting and enables the whistleblower to attach supporting documents to their report to corroborate what it says.

The Compliance Unit will acknowledge receipt within seven working days.

Once acknowledgement of receipt has been received and irrespective of whether the whistleblower has identified themselves or has submitted the report anonymously by accessing the reporting mailbox, the person designated internally by the CIRSA Group may contact the whistleblower directly to identify themselves as the investigator and provide the whistleblower with comments and updates. The report will be processed within a reasonable period of no more than three months from the acknowledgement of receipt, which may be extended to six months in cases of particular significance or complexity. However, after the first three months from receipt of the report, any personal information concerning the whistleblower, the people mentioned or third parties will be removed from the whistleblowing channel unless its retention is essential in order to provide evidence of the operation of the Crime Prevention Model.

It is important to note that the platform only sends these reports to specific people in the CIRSA Group who are expressly authorised and trained to manage them. Likewise,

the internal team which handles any documents provided is trained on how to deal with them effectively and ensure their confidentiality.

The operating procedure is that when the report points to a possible breach of the CIRSA Group's Global Compliance Management System, an investigation will be initiated in accordance with the Fraud and Non-Compliance Investigation Protocol.

CIRSA will provide information to the whistleblower on the report and also on the findings of the review of the issue to the extent possible. It should be noted that in some cases there may be restrictions on the updates that can be provided about the report as specified in the Group's Fraud and Non-Compliance Investigation Protocol mentioned above.

2.3.5 Fair and responsible handling of reports

The company is also bound by the principle of good faith. CIRSA respects the rights of all its employees and therefore also protects the rights of employees named in reports submitted under this Policy.

2.3.6 Prohibition of retaliation

The CIRSA Group does not tolerate any form of retaliation. This includes threats or any other form of intimidation of a person who reports incidents under this Policy.

2.3.7 What does good faith mean from the company's and the whistleblower's point of view?

From the whistleblower's point of view, good faith means reporting with at least reasonable grounds to believe that the information about potential breaches notified was true at the time of reporting.
From the point of view of the company in this context of whistleblowing channels, good faith means that the company will not retaliate against any person for submitting a report and will protect the whistleblower's confidentiality and identity in all circumstances with only the following exceptions:

a) When it has to be disclosed to the courts or administrative authorities by law.
b) When disclosure is essential with respect to external advisers and consultants and other suppliers of the CIRSA Group for the operation of the Ethics Hotline Channel or the investigation of the reported incident as set out in section 3.6 of this Policy. In these cases, CIRSA contractually requires the utmost confidentiality from these suppliers.

2.3.8 What does prohibition of retaliation mean?

Prohibition of retaliation covers any direct or indirect act or omission that may harm a whistleblower because of their report made in good faith concerning potential offences. For example, the CIRSA Group will not take any of the following actions against

whistleblowers due to submitting a report:

1. Suspension, lay-off, dismissal or equivalent measures;
2. A negative performance assessment;
3. Withholding of promotion;
4. Unjustified change of location of place of work, reduction in wages, change in working hours;
5. Coercion, intimidation, harassment or ostracism;
6. Discrimination, disadvantageous or unfair treatment;
7. Failure to renew, or early termination of, a temporary employment contract;
8. Harm, including to the person's reputation, particularly in social media, or financial loss, including loss of business and loss of income;
9. Early termination of a contract for goods or services;
10. Cancellation of a permit;
11. Other measures that could be considered retaliatory.

2.3.9 Prohibition of retaliation in case of external reports and public disclosures

Protection against retaliation also covers people who report potential offences to the authorities.
Both direct and indirect retaliation are prohibited.
The prohibition of retaliation in the Ethics Hotline Channel Operating Policy includes the following individuals:

1. Third persons who are connected with the whistleblower (such as colleagues or relatives) who could suffer retaliation in a work-related context;
2. Any person who has assisted the whistleblower in the reporting process;
3. Legal entities that the whistleblower owns, works for or is otherwise connected with in a work- or professional-related context.

If any member of the CIRSA Group takes direct or indirect retaliatory action in breach of this Policy, the Group will put in place the measures required to ensure that the retaliation ceases as soon as possible and where appropriate will take disciplinary action against the perpetrators.

3. DATA PROTECTION, PROCESSING AND RETENTION

CIRSA provides its employees and customers with this additional information on data protection (hereinafter "Data Protection Policy") which transparently and plainly sets out all the legally required information in relation to the processing management of the internal reports information system, the purposes for which their data are processed and the rights they can exercise. This Data Protection Policy will always be available on the digital platform set up as an alternative channel.

3.1. Who is the controller for your data and how can you contact them?

Managing the internal reports information system necessarily involves the processing of personal data by CIRSA:

• CIRSA SERVICIOS CORPORATIVOS, S.L (hereinafter "CIRSA"), incorporated under Spanish law, holder of tax identification code (CIF) B-25.421.199 with registered office at Carretera Castellar no. 298, 08227 Terrassa (Barcelona) and registered in the Barcelona Company Register in Volume 32339, Folio 194, Sheet B-207353.

• Any CIRSA Group company concerned as a result of the report made when it is necessary to investigate the reported facts in greater detail, take disciplinary measures and/or conduct any legal proceedings which may be needed. You can find out more about the CIRSA Group's international presence at https://www.cirsa.com/en/cirsa/international-presence/

The aforementioned companies are joint controllers for the processing of your personal data since they jointly decide on and perform the processing of personal information for the purpose of managing the internal reports information system.
If you have any queries regarding the processing of your personal data, you can email the CIRSA Group's Data Protection Officer at protecciondedatos@cirsa.com.

3.2. What are personal data and processing?

Personal data are any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Personal data processing is any operation or set of operations which is performed on your personal data such as collecting, recording, storing, using and disclosing your personal data.

3.3. What personal data do we collect and by what means?

Personal data may only be collected and identify you when you reveal your identity. In these cases, CIRSA may collect the following information through the internal reports information system:

- Name and surname
- Email address
- Phone number
- DNI, NIE or passport number
- Content of the report made

When data subjects make their reports anonymously, CIRSA will not be able to identify them and therefore will not process any personal data of these data subjects.

3.4. What rights can you exercise?

A. Right of access

You have the right to know whether CIRSA is processing your personal data and, where that is the case, to know what data it is processing.

B. Right to rectification

You have the right to rectify any of your data that are inaccurate or incomplete. To do so, you will have to specify which data you wish to rectify and provide appropriate proof of them.

C. Right to object

In the legally specified cases you may object, on grounds relating to your particular situation, at any time to the processing of your data. Remember that your objection to the processing of your data will make it impossible for CIRSA to provide you with any services you may ask for.

D. Right to erasure

You have the right to have your personal data erased. This does not mean that your data will be completely deleted but rather that they will be kept blocked in such a way as to prevent their processing, although they may be disclosed to government authorities, judges and courts for the purpose of addressing any liabilities that may have arisen as a result of the processing during their period of limitation.

E. Right to data portability

You have the right to receive your personal data that you have provided to us and/or transmit them a data controller other than CIRSA.

F. Right to restriction of processing

You have the right to ask us to stop processing your data if (i) you contest the accuracy of your data for the period while CIRSA verifies their accuracy; or (ii) you have exercised your right to object to processing of your data pending verification of whether CIRSA's legitimate grounds override yours as the data subject. Likewise, this right allows you to ask CIRSA to keep your personal data when (i) the processing is unlawful and as the data subject you object to the erasure of your personal data and request the restriction of their use instead; or (ii) CIRSA no longer needs your personal data for the purposes of the processing but does require them for the establishment, exercise or defence of legal claims.

You may exercise your rights by sending your request through your user profile created in the internal reports information mailbox. If you are not happy with CIRSA's processing, you may make a complaint to the Spanish Data Protection Agency (AEPD) by going to its website http://www.aepd.es.

3.5. How do we process your data?

In order to tell you transparently and in detail about the purposes for which your data are processed, we have divided the information relating to each processing operation into separate tables. This means you will be able to find all the specific information on the

processing of your data in the relevant table individually. The descriptive table contains the following information:

• **For what purposes do we process your data?**

This column explains the purposes for which your personal data are processed.

• **On what legal basis do we process your data?**

This column explains the legal basis or grounds that allow the Group to lawfully process your personal data. Data protection regulations require that your data are processed on a lawful basis or grounds which justify such processing. We therefore process your personal information using various lawful bases or grounds depending on the type of processing of your data. The lawful bases for processing your personal data may be:

- Legitimate interest
- Performance of the contract
- Performance of a task carried out in the public interest
- CIRSA's compliance with a legal obligation
- Vital interest
- Your consent

• **How long do we keep your personal data for?**

This column provides information on how long your data will be kept for as a guideline. The retention period will depend in all cases on how your personal information is processed. Please note that certain regulations may require us to keep some of your personal data for a specific period of time.

Below is a more detailed description of how CIRSA processes your personal data:

For what purposes do we process your data?	On what legal basis do we process your data?	How long do we keep your personal data for?
Learn about and investigate the commission, both in the corporation and in the actions of third parties contracted by it, of acts or conduct contrary to the law or to the applicable collective bargaining agreement.	Performance of a task carried out in the public interest.	The data subject's personal data will be processed only for the time needed to decide whether or not to initiate an investigation into the reported facts. CIRSA will erase the information from its reporting system three months after the data have been entered unless it is required to continue with the investigation.

3.6. Who do we disclose your data to?

In case of a legal requirement or basis that warrants the disclosure, CIRSA may disclose your data to:

- Legal advisers, experts, cybersecurity companies and/or other third parties needed to conduct the appropriate investigations to ascertain the facts reported by the data subjects
- Courts
- Government and administrative agencies
- Law enforcement agencies
- Members of the Compliance Body or the Compliance Unit

3.7. Who can access your data?

CIRSA notifies you that it works with third parties, specifically service providers required for the successful operation of the internal reports information system. These service providers may have access to your data in the course of their activities. This access does not constitute a transfer of data but rather access as a data processor, which is provided for and regulated in the GDPR. CIRSA safeguards your data and has therefore verified that these providers have an appropriate level of security and ensure the protection of the rights and freedoms of data subjects.

3.8. Are your data secure?

In order to ensure fair and transparent processing of your personal information, we have put in place appropriate procedures which include the implementation of technical and organisational measures addressing the potential risk and rectifying any impression identified in the personal data processed. This means that the risk of any errors is kept to a minimum and your data are handled fairly and securely.

3.9. Changes to this data protection policy

This Data Protection Policy may change over time due to alterations in the standards used by the data protection supervisory authority. CIRSA therefore reserves the right to amend this Data Protection Policy in order to ensure it conforms to these standards and also to any new case law or legislation.

4. RELATED PROCEDURES

As the Policy described in this document is directly related to other policies and/or procedures, below is a list of the ones which the CIRSA Group considers to be the most relevant for understanding the purpose and scope of this Policy.
Specifically, these are the procedures related to and/or affected by this Policy which are published on the company's website under "Compliance Policies and Procedures":

- Code of Conduct
- Corporate Governance Policy
- Criminal Offence Prevention Model
- Anti-Corruption Policy

- Information Security Policy
- Prevention of Money Laundering Policy
- Human Rights Policy
- Human Resources Policy
- Environmental Policy
- Fraud and Non-Compliance Investigation Protocol

www.cirsa.com

2021

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