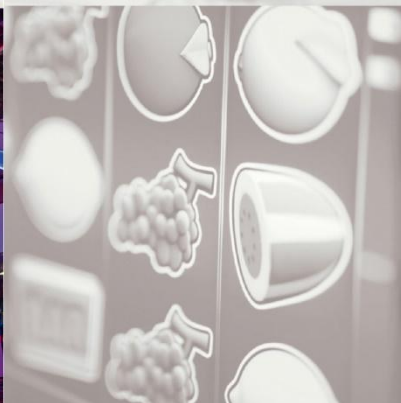
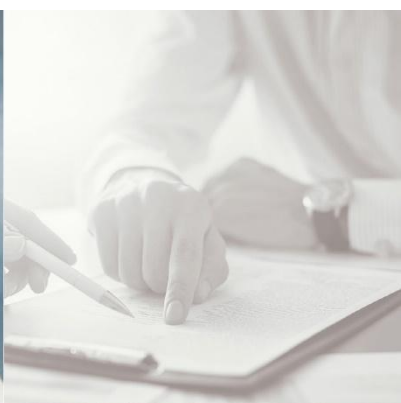


Extract from the Information Security Policy
November/2025



Contents

1. Purpose 3

2. Scope 3

3. Description of the policy content 3

 3.1. Information Security principles 3

 3.2. Roles and responsibilities 4

 3.3. Security management objectives 5

 3.4. Disciplinary sanctions 6

 3.5. Review 6

4. Approval, effective date and dissemination 6

1. Purpose

At the CIRSA Group, Information Security is not only a regulatory obligation, but also a strategic pillar underpinning our operational continuity, technological resilience and data protection. Effective management strengthens the trust of our customers, employees and partners, protects our corporate reputation and significantly reduces the risks associated with incidents and/or cyber threats.

This vision goes beyond compliance: it entails a culture of shared responsibility, embedded in every process, system and relationship with third parties. Security is therefore a collective commitment involving everyone who is part of the Group.

In line with the above, and recognising the value of its information and the need to ensure its availability, integrity, confidentiality, authenticity and traceability, the CIRSA Group's management team considers it essential to establish an Information Security Policy to safeguard business operations.

This also aims to ensure compliance with all legal, regulatory and contractual obligations applicable to information security at any given time.

It therefore develops and implements an Information Security Policy governing the Security Management framework and the activities arising from it.

2. Scope

This Policy applies to the entire CIRSA Group and/or any of its companies, subsidiaries or Group entities, regardless of their geographical location and the functions assigned to them.

It also applies to all employees, external service providers and/or collaborators who have access to and/or use CIRSA Group information. This Policy must therefore be accessible to all of them.

The content of this Policy is based on the guidelines established in the applicable legal framework, the ISO/IEC 27001:2022 security standard and the CIRSA Group's security rules.

The provisions of this document are binding on all personnel providing services to the Organisation, whether permanently or temporarily, including external suppliers' personnel where appropriate and where they use the Organisation's Information Systems.

3. Description of the policy content

3.1. Information Security principles

Given the importance of information systems, the CIRSA Group's Management establishes the following fundamental information security principles:

Principle of regulatory compliance

All information systems shall comply with applicable legal, regulatory and sector-specific requirements affecting information security, particularly those relating to personal data protection and the security of systems, data, communications and electronic services.

Principle of risk management

Risks must be minimised to acceptable levels, seeking a balance between security controls and the nature of the information. Security objectives must be established, reviewed and consistent with information security considerations.

Principles of confidentiality, integrity, availability, authenticity and traceability

- **The confidentiality** of information must be guaranteed, ensuring that only authorised individuals have access to it.
- **The integrity** of the information used must be ensured so that it is concise and precise, with particular emphasis on the accuracy of both its content and the processes involved.
- **The availability** of information must be guaranteed, ensuring the continuity of the business supported by information services through contingency plans.
- **The authenticity** of information and the legitimacy of the source of its transmission must be guaranteed.
- **The traceability** of actions must be guaranteed, enabling the Organisation to identify operations, queries or changes involving information.

Principle of proportionality

Controls to mitigate asset security risks must be implemented by seeking a balance between security measures, the nature of the information and the risk.

Principle of responsibility

All CIRSA Group members must act responsibly in relation to information security, complying with the established rules and controls.

Principle of continuous improvement

The effectiveness of the security controls implemented within the Organisation shall be reviewed regularly to improve the ability to adapt to constantly evolving risks and the technological environment.

Principle of ongoing readiness and cooperation

With authorities and regulatory bodies whenever necessary, as part of the CIRSA Group's commitment to service and responsibility towards the society in which it operates.

3.2. Roles and responsibilities

Information Security within the CIRSA Group is managed through a defined organisational structure that ensures appropriate decision-making, effective implementation and rigorous compliance with legal and regulatory obligations. This structure is based on coordinated collaboration among the following key parties:

1. The Information Security Committee, responsible for defining the strategy, setting objectives and prioritising the resources needed to ensure an appropriate level of security throughout the Organisation.
2. The Information Security Officer, responsible for leading the operational implementation of the defined strategy, and coordinating and overseeing the implementation of the Security Plan.

3. The Delegated Data Protection Committee, whose role is to advise on and oversee compliance with personal data protection and privacy legislation, working closely with the Information Security Officer.
4. The Crisis Committee, a body activated only in exceptional circumstances to coordinate the response to critical incidents that may affect business continuity or the Group's reputation.

In addition to the above, two essential parties complement this structure:

- The Management Committee, which provides the institutional support needed to implement this Policy, allocates strategic resources and ensures fulfilment of commitments made to third parties.
- All CIRSA Group personnel, who are responsible for understanding and applying this Policy in their daily activities, taking part in the relevant training and reporting any security incidents detected.

This structure enables comprehensive and efficient management, aligned with the principles of responsibility, prevention and continuous improvement, ensuring that Information Security is a cross-cutting, strategic component of all Group activities.

3.3. Security management objectives

Mitigate information security risks

- Maintain a risk management process with a clear methodology.
- Identify threats that may put the Organisation at risk.
- Conduct risk analyses periodically.
- Establish an acceptable risk threshold, above which the Organisation must approve a Treatment Plan. This plan shall identify countermeasures to be implemented within a schedule approved by the Security Committee and establish controls to measure their effectiveness.
- Explicitly acknowledge acceptance of untreated or unmanaged risks, so that all parties involved are aware of unmanaged security risks.
- Provide a reference and action framework to protect information system assets against internal or external, deliberate or unintentional threats, in order to ensure information security and availability.

Maintain the confidentiality, integrity and availability of information assets

- The security dimensions (confidentiality, integrity and availability) of each information asset must be maintained at acceptable levels so as not to affect its properties or the proper development of the Organisation.

Improve the cybersecurity culture within the Organisation

- Promote awareness and training among both internal and external personnel through information security training activities, awareness campaigns and similar initiatives.
- To address ongoing cybersecurity threats, resources must be provided to enable CIRSA Group employees to detect threats, identify them efficiently and report them to incident management teams.

- These resources must also be suitable for reducing and blocking these threats where necessary.

3.4. Disciplinary sanctions

Any breach of this Information Security Policy may result in appropriate disciplinary action in accordance with the legal and contractual provisions in force within the Company.

All CIRSA Group employees, external service providers and/or collaborators are also responsible for notifying the Cybersecurity Department immediately upon becoming aware of any departure from the applicable rules and/or any security incident, via ciberseguridad@cirsa.com and, in all cases, no later than twelve (12) hours after detection by the employee, external service provider and/or collaborator.

3.5. Review

This Policy must be reviewed periodically by the Security Committee, at intervals of no more than one year, without prejudice to any amendments that may be required as a result of significant changes within the Organisation.

It may also be reviewed at the request of:

- The Management Committee.
- Any member of the Security Committee.
- The Security Officer.

4. Approval, effective date and dissemination

This Policy was approved by the Board of Directors of CIRSA Enterprises, S.A. at its meeting on 20 November 2025.

This Policy takes effect on the date of its approval. Its content shall be reviewed periodically, where appropriate, to adapt it to regulatory changes or incorporate best practices in this area. The Board of Directors shall be the body authorised to amend it, following oversight by the relevant Board Committee.

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

