INFORMATION SECURITY POLICY

In line with its mission and its values and within the current legislative framework **AR RACKING, S.A.U.** undertakes to maintain and improve the information security and continuity of its activity.

AR RACKING's Information Security Policy is designed to guarantee the protection of all its information assets and the technology used for their processing from deliberate or accidental internal or external threats, in order to ensure their integrity, availability and confidentiality, assisting the company in efficiently meeting its strategic goals.

To support the policy, AR RACKING has an Information Security Management System (ISMS) promoted by the Management that provides a systematic approach to risk management.

Accordingly, AR RACKING maintains the following application guidelines to be taken into account within the framework of the Information Security Management System (ISMS):

- **Confidentiality**: The information processed by AR RACKING shall be known exclusively by authorised persons, after identification, at the time and by the means enabled.
- **Integrity**: The information processed by AR RACKING shall be complete, accurate and valid, and its content shall be that provided by the affected parties.
- **Availability:** The information processed by AR RACKING shall be accessible and usable by authorised and identified users at all times, guaranteeing its persistence in the event of any foreseen circumstances.
- **Legality**: In order to ensure that the information meets our needs, a management system will be implemented that complies with the current legislation and our contractual and corporate commitments, and that provides an appropriate working framework.

Information Security Policy

> Promote a culture throughout the organisation designed to protect the information assets.
> Disseminate, consolidate and fulfil the policy.
> Implement the security measures.
> Keep the policies, regulations and procedures up to date, in order to ensure their timeliness and level of effectiveness.
> Promote measures and practices that ensure the continuity of the activity.

Scope

> The policy is applicable to all AR RACKING personnel and to external individuals connected to the company through service contracts or agreements with third parties.

> The policy is applicable to all areas of the company, its resources and all internal processes. In line with the above, the security of the information processed by AR RACKING constitutes a key strategic asset to ensure business continuity.

> It is mandatory and may result in legal repercussions or disciplinary measures if breached.

Dissemination of the Policy

The Information Security Policy must be known by all collaborators and employees of AR RACKING, with the CISO being the primary person responsible for its dissemination. It must be communicated to the entire Organisation and be available on media accessible to all.

José Manuel Lucio
Managing Director

Version	Date	Description of the changes	Revised by	Approved by
1	**1/Sep 21**	Definition and approval	**AZ**	**JML**
2	**31/Maz 25**	Change of document name	**AZ**	**JML**