SUMMARY OF THE ENS AND ISO 27001 POLICY

This document constitutes an institutional and informative summary of the Information Security Policy of ARA VINC GESTIÓ DOCUMENTAL, S.L. (**aradoc**). Its purpose is to inform transparently clients, suppliers, partners, public administrations and other interested parties (stakeholders) about the principles, commitments and general guidelines that govern information security management within the organization.
This summary is based on the **security policies formally approved by Management**, integrated into the Integrated Management System (SIG) of **aradoc**, and **does not replace** the full internal regulations nor the associated operational procedures.

The Information Security Policy of **aradoc** is aligned with:

- The **National Security Scheme (ENS)**, in accordance with Royal Decree 311/2022, **with a HIGH security level**.
- The **ISO/IEC 27001:2022** Information Security Management Systems standard.
- Other integrated management standards and the applicable regulations on personal data protection.

Scope of Information Security

The security policy applies to the **information systems supporting the document management services** of **aradoc**, including, among others:

- Transport and document logistics.
- Custody and preservation of documentation.
- Handling and processing of information.
- Secure destruction of media and documents.

It is mandatory for all internal and external personnel who have access to the organization's information systems, including suppliers and partners, regardless of the type of contractual relationship.

Basic Security Principles

Information security at **aradoc** is based on the principles established by the ENS and ISO/IEC 27001, among which the following stand out:

- **Global security approach**, considering people, processes, technology, and facilities.
- **Risk-based management**, identifying, analysing, and treating risks that may affect the confidentiality, integrity and availability of information.
- **Prevention, detection, response, and recovery** in the face of security incidents.
- **Defence in depth**, through organisational, technical and physical measures applied in multiple layers.
- **Clear assignment of responsibilities**, ensuring separation of duties and avoiding conflicts of interest.
- **Continuous improvement**, through periodic reviews, audits, and improvement actions within the security system.

Organisation and Responsibilities

aradoc has a **clearly defined security organisational structure**, led by Management and coordinated through an **Information Security Committee**.
The main roles include:

- Security Manager.
- Systems Manager.
- Information Owner.
- Service Manager.
- Data Protection Officer (DPO).

These roles have specific responsibilities related to information protection, risk management, system oversight, incident handling, and regulatory compliance.

Risk Management and Regulatory Compliance

The organisation carries out **periodic risk analyses**, updated at least annually or whenever significant changes occur in systems, services or the information processed.
aradoc commits to:

- Complying with applicable legislation on information security and data protection.
- Applying the appropriate security measures according to the risk level identified.
- Ensuring that residual risks are formally accepted by the corresponding responsible parties.

General Security Measures

Without detailing sensitive technical aspects, the policy includes, among others, the following lines of action:

- **Access control** based on the principle of least privilege.
- **Protection of facilities and systems**, with controlled physical and logical access.
- **Secure asset management**, including hardware, software, and information.
- **Protection of stored and transmitted information**, through adequate technical and organisational measures.
- **Activity logging and monitoring**, in compliance with data protection regulations.
- **Security incident management**, with procedures for detection, analysis, response, and communication.
- **Business continuity**, through backups and contingency plans.

Training, Awareness and Continuous Improvement

aradoc considers **training and awareness in information security** essential to ensure the protection of systems and the information processed. All personnel receive adequate information about their responsibilities and good security practices.
The Information Security Management System is reviewed and improved continuously, incorporating:

- Results of internal and external audits.
- Lessons learned from security incidents.
- Relevant regulatory, technological and organisational changes.

This approach ensures the ongoing adequacy of the security system to the **HIGH ENS level** and to the requirements of ISO/IEC 27001.
This document is **exclusively informative and educational**, and is published with the aim of strengthening transparency and the trust of interested parties. To review the detailed policies, standards and procedures applicable to security, the internal documents approved by aradoc must be consulted.
The organisation reserves the right to update this summary when significant changes occur in its Information Security Policy.

Barcelona,12.01.2026
Josep Ribera Serra