axians

Security Requirements for Suppliers

The best of ICT with a human touch

VINCI ENERGIES

Document Control

Security Requirements for Suppliers	Name	Department	Date
Prepared by	Seguridad Corporativa	Seguridad Corporativa	24/11/2022
Reviewed by	GRC Seguridad Corporativa	Seguridad Corporativa	06/10/2025
Approved by	Responsible Seguridad Corporativa	Seguridad Corporativa	17/10/2025

Document Version

Version	Date	Changes
v.1.0	03/02/2023	Document creation
v.1.1	06/10/2025	Inclusion of a section related to the use of cloud services

Intellectual Property Rights

TABLE OF CONTENTS

1. PURPOSE

This document outlines the information security requirements established by AXIANS for the provision of services, and it is mandatory for its SUPPLIERS within the scope of the contracted products and services.

The ultimate objective of this document is to protect the interests of AXIANS, its CLIENTS, and its EMPLOYEES in the field of information security.

2. SECURITY REQUIREMENTS

2.1. Introduction

This document has been prepared using the ISO/IEC 27001 standard, in its current version, as a reference framework for the protection of AXIANS' information. Within this document:

- The roles and responsibilities of the parties (AXIANS and the SUPPLIER) are described.
- For each defined point, the SUPPLIER confirms its ability to comply with the requirements established within the scope of the contracted service and must notify AXIANS if any of them imply an additional cost not included in the submitted financial offer.
- All the requirements described below apply exclusively to the contracted service and do not constitute an obligation for any other area of the supplier, unless otherwise agreed by the parties, depending on the nature of the service provided.

2.2. Human Resources and Supplier Security

The SUPPLIER must:

- Ensure that all its personnel have the appropriate competencies to carry out the contracted service and are aware of their information security obligations as established in this document.
- Include information security clauses in the contracts of all employees and contractors, if any, and provide evidence of compliance with this requirement upon request.
- Conduct training and awareness activities on information security. Specifically, the supplier must have a training and awareness plan, subject to periodic reviews.
- Ensure that its employees comply with the confidentiality requirements stipulated in the contract with AXIANS.
- In the event that subcontracting of any service activity is required, prior authorization from AXIANS must be obtained. The SUPPLIER is responsible for communicating the requirements of this document to the subcontractor and ensuring their compliance.

2.3. Logical Access Control

The SUPPLIER must:

- Maintain an internal access control procedure (including user creation, deletion and modification in its IT systems) based on the following information security requirements:
  - Principle of least privilege: access to systems and applications must be limited according to the collaborator's role and their "need to know."
  - Secure login (secure username/password) for all systems containing service or project information.
  - Password management for systems and applications required for the project. Passwords must be unique and non-transferable.
  - Specific and differentiated handling for privileged users (e.g., system administrators, database administrators, etc.).

2.4. Physical and Environmental Security

The SUPPLIER must:

- Protect facilities (offices, data centers, communication rooms, etc.) from which the contracted services are provided, against physical and environmental threats and disasters, including those caused by human actions, ensuring the availability of power supply, cabling, etc.
- Protect devices against unauthorized access, data loss or information damage.
- Maintain control over interventions (equipment installations and removals, inspections, etc.) in restricted areas.
- Implement physical access controls to ensure that only authorized personnel can access restricted areas.

2.5. Asset and Operations Security

The SUPPLIER must:

- Appoint an Information Security Officer or a designated contact person with whom AXIANS can communicate when necessary.

- Identify and maintain an inventory of all assets dedicated to the project/service, ensuring their proper use, maintenance and protection.
- Document and maintain operational procedures related to the service provided.
- Define Change Management procedures for changes made to systems, applications, etc.
- Implement a Capacity Management procedure, monitoring resource usage and anticipating future capacity needs to ensure compliance with the contracted service levels.
- Deploy appropriate and effective security controls to prevent attacks, intrusions, and/or malicious code infections that could affect the availability, confidentiality, and/or integrity of AXIANS' information.
- Perform backups of information, software and system images, following a retention and archiving policy that ensures the contracted service levels.
- Maintain logs that allow for the traceability of user activity, enabling the detection of anomalous behavior, failures and events that may impact information security in systems and applications dedicated to the project/service. In particular, maintain an activity log for privileged users.
- Establish and execute a Vulnerability Management procedure to ensure timely patching of systems, minimizing exposure to high and critical vulnerabilities reported by software and system vendors. In the case of critical vulnerabilities that may affect AXIANS, these must be reported as soon as possible after detection.

2.6. Communications Security

The SUPPLIER must:

- Implement secure communication mechanisms and protocols within its facilities for the provision of the service.
- Establish secure channels (encrypted tunneling) between the SUPPLIER's facilities and AXIANS.
- Notify AXIANS of any personal data transfers outside the European Union.

2.7. Acquisition, Development and Maintenance of Systems and Software Licenses

The SUPPLIER must:

- Ensure that all software and hardware equipment supplied or used for the provision of the SUPPLIER's service has the corresponding usage license, acquired through authorized channels.
- Ensure that the SUPPLIER's proprietary software, required to carry out the contracted project/service, is developed in accordance with recognized secure software development principles and methodologies, including environment separation (production and non-production), security by design and security by default, among others.
- If the contracted service involves software development, the SUPPLIER must follow the internal secure development methodology and protocols defined by AXIANS, based on internationally recognized standards.
- Ensure that all software and hardware equipment supplied or used for the provision of the SUPPLIER's service is covered by a preventive and corrective maintenance plan.

2.8. Information Protection

The SUPPLIER must:

- Respect the obligations of confidentiality, integrity and availability of information within the scope of the service provision.
- Limit the dissemination and access to information as defined in the service, avoiding any storage that is not strictly necessary for service delivery.
- Not use the information for any purpose other than that established in the contract. Any modification to the original scope regarding the information required for service delivery must be communicated to and authorized by AXIANS.
- Implement encryption mechanisms that ensure the confidentiality of AXIANS' information, regardless of its state (in transit or at rest) and the devices on which it is handled.
- Return to AXIANS and delete from its systems/facilities, upon completion of the project/service or upon AXIANS' request, all information provided, generated or derived

from the service provision, including any copies thereof. Evidence of deletion/destruction of the information may be requested.

2.9. Use of Cloud Services

The contracting of cloud services by Axians requires a prior analysis of the service and verification by the Corporate Security area to ensure that the service complies with the security policies of Axians and VINCI Energies.

The procedure for evaluating SaaS solutions is outlined in the Cloud Services Usage Policy and must be initiated internally by the business unit or organizational unit responsible for contracting the service.

2.10. Security Incident Management

The SUPPLIER must:

- Act diligently in the event of a security incident, and is required to:
  - Report it to AXIANS within a maximum of twenty-four (24) calendar hours from the moment it becomes known, through the designated contact persons between the parties, with a copy to seguridadcorporativa@axians.es.
  - Mitigate any impact or damage the incident may cause to AXIANS.
  - Collaborate at all times with AXIANS during the investigation of the incident and provide all necessary information to clarify it.
  - Keep AXIANS' Information Security Officer informed about the status of the investigation, the actions taken and their outcomes.
  - Submit a written report to AXIANS within fifteen (15) calendar days detailing the complete incident management process.
- The SUPPLIER must have an incident notification and management procedure in place, which includes logging, classification and detailed documentation of incidents.

2.11. Audits

In order to verify, at any time, compliance with the information security requirements described in this document, AXIANS may carry out any controls and audits it deems appropriate. To this

end, the SUPPLIER authorizes AXIANS to perform the agreed audits, provided they do not interfere with the normal provision of the service.

AXIANS and its auditors will conduct such audits in a manner that causes minimal disruption to operational activities. The SUPPLIER shall facilitate the audit, granting access to all necessary information and documentation.

If AXIANS delegates the performance of such audits to a third party, the selected companies must have proven reliability, guarantee strict confidentiality and pose no conflict of interest for the SUPPLIER.