INFORMATION SECURITY POLICY

Sociedad Ibérica de Construcciones Eléctricas, S.A. (**SICE**) is a multinational company that integrates technologies related to Traffic and Transport, Environment and Energy, Telecommunications and all types of industrial processes.

SICE's activity is mainly focused on providing value-added services through the integration of different technologies and systems, our own technologies and those of third parties, in order to offer the **best solutions, customized for each client, providing:**

- Technological capacity
- Experience
- Customised solutions
- Systems integration
- Open systems

SICE considers that lnformation Security should be a priority for the organisation. To this end, the **Management** assumes responsibility for the lnformation Security Management of the processes and activities carried out in the offices of the Headquarters and, with the full participation of the managers and all staff, undertakes:

- To maintain and periodically review an lnformation Security Management System (ISMS) in accordance with the ISO 27001 international standard, which is applicable to the hosting system in the data processing centres that support activities for the development of intelligent traffic and transport systems, security systems, as well as interna[and externa[process control.

- To **continuously improve the effectiveness** of the implemented ISMS by carrying out the actions determined after analysing the results of the information security performance and the information obtained from audits and periodic reviews.

- To foster a proactive culture of improvement by managing **risks** and **opportunities** consistent with the organisation's context and stakeholders.

- To set, plan and review **objectives** consistent with this Policy, taking into account applicable information security requirements, the results of risk assessment and risk treatment, and following up the actions identified to achieve them.

- To maintain information **confidentiality** at all times.

- To ensure information **availability** through appropriate back-up and business continuity measures.

- To maintain the **traceability** of information at all times.

- To ensure information **integrity** and **authenticity** in all processes that manage, process and store information.

- To **manage**, logically and effectively any **incidents** or weaknesses that may compromise or have compromised information confidentiality, integrity and/or availability.

- To ensure that all personnel within the scope of the ISMS have adequate **awareness** and **training** on information security.

- To comply with the applicable legal and contractual requirements for information security.

    - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT ANO OF THE COUNCIL of 27th April 2016 on the protection of natural persons with regard to the processing of personal data and on the free move- ment of such data.
    - Organic Act 3/2018, of 5th December, on Personal Data Protection and the guarantee of digital rights.
    - Royal Legislative Decree 1 / 1996 of 12th April 1996, lntellectual Property Act.
    - Royal Decree-Act 2/2018, of 13th April, amending the consolidated text of the lntellectual Property Act.
    - Act 5/2014, of 4th April, regulating Private Security activity.
    - Royal Decree 311 /2022, of 3rd May, which regulates the National Security Scheme, established in Arti- cle156.2 of Act 40/2015, of pt October, on the Legal Regime of the Public Sector.

Our management system has the following structure:

- Procedures
- Policies
- Standards and Codes

lt is implemented by means of the following minimum requirements:

a) Organisation and implementation of the security process: via procedure PG-001 lnformation Security Management and IT-IS-101-PROC-OPER-COMITÉ_SEGURIDAD_INFORMACIÓN.
b) Risk analysis and management: via procedure PG-001 lnformation Security Management
c) Personnel management: via procedure PG-001 lnformation Security Management and IT-IS-101-PROC-OPER-
d) COMITÉ_SEGURIDAD_INFORMACIÓN.
e) Professionalism: via procedure PG-001 lnformation Security Management.
f) Authorisation and access control: via the documents lnformation Systems User Guide (VINCI), IT-SIS-205-PROC-
g) USER-VPN.
h) Protection of the facilities: via the document lnformation Systems User Guide (VINCI).
i) Procurement: via procedure PG-110 Purchasing and Subcontracting.
j) Default security: via procedure PG-001 lnformation Security Management.
k) System integrity and updating: via procedure PG-001 lnformation Security Management
l) Protection of stored data and data in transit: via the lnformation Systems User Guide (VINCI).
m) Prevention in relation to other interconnected information systems by means of: the lnformation Systems User Guide (VINCI), the IT-SIS-100-PROC-USER-CODIGO-CONDUCTA-INFORMATICA, the Corporate Communication and Dissemination Policy, and the Data Protection and Processing of Confidential and Sensitive lnformation Policy.
n) Activity logging: via procedure PG-001 lnformation Security Management.
o) Security incidents: via IT-SIS-212-PROC-USER_ CAU_SICE and IT-SIS-500-PROC-OPER.
p) Continuity of activity: via documents IT-SIS-500_PROC-OPER-PLAN_CONTINGENCIA_SSI, IT-SIS-529-PROC-OPER-PLAN_RESPUESTA_INCIDENTES_SEGURIDAD and IT-SIS-525-PROC-OPER-GESTION_INCIDENTES_SEGURIDAD_GDPR.
q) Continuous improvement of the security process: via procedure PG-001 lnformation Security Management.

The system will be available in a repository, which may be accessed by eligible profiles according to our access manage- ment procedure.

The procedure IT-IS-101-PROC-OPER-COMITE_SEGURIDAD_INFORMACION contains all information on the **Information Security Committee**, hereinafter referred to as **ISC**.

The defined security roles or functions, which are completed in the job profiles and system documents, are:

Function	Duties and responsabilities
lnformation Security Officer / CISO	To determine the adequacy of technical measures To provide the best technology for the service To take decisions to meet information security and service requirements.
lnformation Systems Officer / CIO	To coordinate the implementation of the system. Continuous improvement of the system To operate the information system in accordance with the security measures determined by the securitv officer.

Their appointment and renewal shall be ratified by the **ISC**, which is the only body that can appoint, renew and dismiss them. The Security Committee is the highest body in charge of the information security management system, therefore the most important decisions related to security shall be taken by this Committee. The Security Committee consists of the following members:

- lnformation Security Officer
- lnformation Systems Officer
- Data Protection Officer
- HR Manager
- Corporate Compliance Officer
- Head of Legal Affairs
- Head of Business Development
- Head of Procurement
- Head of Quality Control
- Head of Administration and Finance
- Head of Technical Management

The **ISC** is an autonomous and executive decision-making body whose activity is not under any other unit of our company. Decisions shall be taken by a vote of the members, with a simple majority being the sote requirement. In the event of a conflict between the different persons in charge, it shall be resolved by their line manager. Failing this, the decision of the Senior Management shall prevail.

This policy is supplemented by the other policies, procedures and documents that are in place for the implementation of our management system.

All members of the Organisation are required to be aware of and comply with this lnformation Security Policy and the Security Regulations, and it is the responsibility of the **ISC** to provide the necessary means to ensure that the information reaches all interested parties.

SICE's management trusts that each person in the organisation understands the importance of the commitments indicated above, assumes them, and incorporates them into their work, as a part of general and daily management.

Alcobendas, March 2024
Managing Director