INFORMATION SECURITY POLICY

Ineco, a reference engineering and consultancy company in sustainable mobility and digital transformation, reaffirms its firm commitment to ensure information security in all its processes, with this document as a reference framework for this commitment, which applies to all phases of the information life cycle (generation, distribution, storage, processing, transport, consultation and destruction), as well as to the information systems that support it.

Ineco adopts security controls aimed at preserving the **five dimensions** of information security at all times:

- ***Confidentiality***: Ensure that only duly authorized persons have access to data and systems.
- ***Integrity***: Ensuring the accuracy of the information in the systems against alteration, loss or destruction, whether accidental or fraudulent.
- ***Availability***: Ensure that information and systems can be used in the time and manner required.
- ***Traceability***: Ensuring that the actions of an entity can be attributed exclusively to that entity.
- ***Authenticity***: Guarantee that an entity is who it claims to be, or that it guarantees the source from which the data originates.

The **basic principles** regulating this policy are as follows:

- To provide the material, economic and human **resources** necessary to carry out the tasks related to information security.
- To define as **strategic assets of the company** the information and the systems that support it, expressing the determination to achieve the necessary levels of security and acceptable risk that certify its protection in a profitable way, guaranteeing the security and controlled access to the information, and thus improve the quality of the services offered by the company to its customers.
- To implement the **relevant controls** to ensure the secure treatment of information in operations and the appropriate security measures in the networks through which the information is transmitted, thus guaranteeing the necessary protection.
- To have on the part of the organization's employees, the **appropriate awareness aspects** in order to ensure that the Information Security policy has the maximum dissemination within the company, developing short, medium and long term goals and incorporating specific motivation and training techniques.
- To be the main tool for **ensuring Information Security** and the objectives of the system. Likewise, regulations, standards, procedures and attributions of each person in charge will be defined, with a specific scope within the Management System.
- To establish **appropriate security requirements** in contractual relationships with suppliers and collaborators. Potential security incidents will be managed quickly, effectively and appropriately, along with conflict resolution mechanisms to minimize their potential impact.
- To comply with **legal requirements, contractual regulations and any other requirements** related to information security that are applicable to Ineco shall be mandatory.
- To promote the commitment and the search for **continuous improvement** of the information security management system.

Ineco is committed to spreading this policy and making it available to all stakeholders, promoting and ensuring its compliance.

April 8th, 2022

Sergio Vázquez Torrón

Chairman