CYBERSECURITY POLICY

General principles

The cybersecurity policy of the Talgo Group (hereafter, Talgo) defines the basic principles and general framework for information security control, risks management and cyber resilience against cyber attacks, that may affect the organization or its relationships with partners and other third parties interested.

Talgo's cybersecurity policy addresses all business processes, products and services, and is applicable at all stages of the information and the management information systems life cycle.

Objective and scope

The fulfillment of this policy is obligatory for all Talgo employees and third parties with access to the information or the management information systems.

The Direction of Talgo is committed to support the cybersecurity management by means of instructions established to comply with the following basic principles:

- *Define the framework for the diffusion and fulfillment of the cybersecurity instructions.*
- *Implement constant controls to supervise the confidentiality, integrity and availability of information as well as its treatment in operations, communications as well as physical location and storage logic.*
- *Comply with legal, regulatory or contract requirements, related with cybersecurity, applicable to Talgo in direct or indirect form as well as through contract commitments in the capacity of the supplier of products or services.*
- *Declare appropriate responsibility and diligence for evaluation and management of risks, detected in cybersecurity area.*
- *Assure that the assets, information and systems of Talgo supporting it, have security and resilience levels appropriate for its criticality level.*
- *Stimulate capabilities of prevention, detection, reaction, analysis, recovery, response, investigation and coordination against cyber incidents and new threats.*
- *Establish appropriate cybersecurity requirements for contract relations with suppliers and collaborators, regulating criteria and means for exchange and sharing of information.*
- *Sensitize and enhance the awareness of staff and collaborators of Talgo about the risks, related with cybersecurity and its impact on processes and operational activities of organization, in appropriate, understandable and available manner.*
- *Provide material, economical and human resources, necessary to comply with objectives and tasks related with cybersecurity, allowing to reduce global and branch specific risks level.*
- *Expand cybersecurity capabilities at product and services, commercialized by Talgo, in line with contract and legal obligations, applicable in each case.*

The signatures of those responsible for preparing, reviewing and approving are in the Spanish version of this document; this document is an English translation of the document in Spanish. In case of discrepancies between both versions, the signed version prevails (usually in Spanish)

Carlos Palacio Oriol
President

Las Matas, 25th of October 2021