CODE: NG.FER.SI.001

TITLE: Corporate Cybersecurity Policy

VERSION: 1.0

SCOPE: General

DATE OF FIRST PUBLICATION: 27/01/2022

CANCELS: N/A

DATE OF PUBLICATION OF THE CURRENT VERSION: 27/01/2022

LANGUAGE OF THE ORIGINAL VERSION: Spanish

APPROVED BY: CEO

ISSUING AREA: Cybersecurity Department

REVIEW HISTORY

Version	Date of dissemination	Reason and summary of changes	Cancels/Replaces:
1.0	27/01/2022	N/A – Initial version of document.	N/A

INDEX

INTRODUCTION

Ferrovial recognizes the strategic importance of its Digital Products and Services (hereinafter, "IT"), its Industrial Systems (hereinafter, "OT"), its Internet Connected Assets (hereinafter, "IoT") and the Information that is generated and used in all the processes and operations that support the Company's business activities, as it represents an essential element for the creation and delivery of value to its *stakeholders*.

Ferrovial also considers that the rules and procedures that regulate the creation, treatment, operation and control of these assets are a key factor both in the performance of its activity and in its reputation.

To that purpose, this Corporate Cybersecurity Policy, (hereinafter, "Security Policy"), is based on a set of principles and objectives that will govern the strategy and scope of action of Cybersecurity within Ferrovial.

PURPOSE

The purpose of this Policy is to establish the fundamental Security principles that ensure in Ferrovial the protection of the integrity, confidentiality and availability of its IT, its OT, its IoT and the Information generated and used in all the business processes and operations of its business activities.

SCOPE

The current Policy applies to Ferrovial S.A. and the commercial associations comprising its consolidated group and, in general, to any entity under its direct or indirect control ("Ferrovial"). These refers to, any entity where Ferrovial has most of the voting rights in the administrative or management body.

As far as possible, the approval of the alignment of local Security practice with this Policy will be promoted in the decision-making bodies of those entities where Ferrovial does not have control.

In addition, this Policy may be complemented and developed by the different Security Policies, procedures and standards that are issued for its implementation, which must be consistent with the principles established on it. The development policies will also acquire the same binding and enforceable character previously defined.

Any violation of the current Policy or the policies and procedures that are a part of it will be a reason to establish a sanction on behalf of Ferrovial, and where relevant, may result in disciplinary and/or judicial actions whenever necessary.

Enforcement

The current Corporate Cybersecurity Policy is established in accordance with the following reference standards:

- NIST CSF (National Institute of Standards in Technology Cybersecurity Framework).
- ISO/IEC 27001 & ISO/IEC 27002.
- Esquema Nacional de Seguridad (ENS).
- Cloud Security Alliance (CSA).
- CIS Critical Security Controls (Center for Internet Security).

These standards determine the technological, organizational and procedural framework with which develop, implement, control, review, maintain and improve the level of Ferrovial's Security.

All the employees, contributors and third parties covered by the scope of the current Policy and its development policies are responsible for ensuring that they, as well as any other dependent person or entity, know, respect and enforce this Policy.

The Global CISO (Chief Information Security Officer) of Ferrovial, as the responsible for aligning the Security Strategy with the vision and mission of Ferrovial, will ensure the transmission, promotion and compliance of this Policy.

This Policy has been approved by the Chief Executive Officer of Ferrovial S.A.

Cybersecurity Mission

Cybersecurity and Information Security (the "Security") in Ferrovial are responsible of ensuring the confidentiality, integrity and availability of its IT, its OT, its IoT and the information that is generated and used in all processes and operations that support their business activities, which are aligned with the following Security Principles and Objectives that sustain and guide Ferrovial's Security Strategy:

1. **Existence of a digital and technological environment with the necessary level of Security:** Provide Ferrovial' s digital and technological environment with the appropriate level of security by managing the inherent risks in it.

2. **Guarantee legal, regulatory, and contractual compliance:** Guarantee compliance with the laws and policies that apply in Ferrovial, as well as with the contractual requirements of the business activity.

3. **Adequately manage and build resilience to security incidents**: Carry out a correct security incident management to minimize their impact, as well as having the necessary resources and business continuity strategies to be able to successfully recover from them and ensure business continuity.

4. **Promote an appropriate Security culture:** Train all the people who design, implement and/or use IT, OT, IoT and Ferrovial's Information to be able to identify and act on threats and security events that may take place in the practice of their daily activities.

5. **Harmonize Security between different business units and subsidiary companies:** Encourage all business units to deploy appropriate and proportional security measures from a risk management perspective.

6. **Facilitate digitalization, innovation, and the adoption of new technologies as a support for the Business:** Manage the risks associated with the digitalization, the innovation, and the adoption of new technologies, facilitating the creation of new business models based on them.

7. **Facilitate business opportunities and tendering processes:** By valuing the Security models, best practices and technologies deployed by Ferrovial as a differentiator from its competitors.

8. **Establish strategic collaborations in Security matter**: Stablish strategic collaborations to increase the level of Security in Ferrovial, in the Security ecosystem and in society in general.

Cybersecurity Capabilities

The fundamental principles outlined above are developed through a set of capabilities:

- **Identification.** Capabilities related to (i) the identification of the organization's context, processes, and critical services; (ii) the identification, classification and analysis of all assets relevant to the organization; (iii) the identification and treatment of risks that may compromise them; (iv) and to ensure legislative, regulatory and contractual compliance related to the development of the business activity.

- **Protection.** Capabilities related to (i) the protection of the identified assets according to their level of importance for Ferrovial; (ii) the design and construction of secure digital products and services, (iii) access control mechanisms based on identity and the need to know and use; (iv) the protection of internal and external communications; (v) the control of asset operations; (vi) the control of the supply chain, (vii) the control of cryptographic keys; (viii) as well as promoting an appropriate security culture.

- **Detection.** Capabilities related to (i) the monitoring of digital products and services, (ii) network communications, (iii) the IT infrastructure and (iv) those facilities where they are hosted at, to (v) detect and classify cyber threats, both internal and external, and their adverse events that may impact Ferrovial 's assets.

- **Response**. Capabilities related to the (i) deployment, management and testing of response plans to the materialization of cyber threats, (ii) and communication with stakeholders, including those required by legislation, regulations, or contracts.

- **Recovery.** Capabilities related to (i) the resilience of Ferrovial 's assets to recover from the impact of an adverse event and return to its normal state, (ii) and to identify lessons learned that are subsequently deployed to prevent the extension of such events.

All these capabilities will be implemented through the appropriate Security measures based on the organizational structure, processes, technologies and people; and the deployment of a framework aligned with best market practices.

Cybersecurity Risks

The capabilities outlined above must be developed to ensure the proper management of the following cybersecurity risks that may impact in Ferrovial business activity:

Cyberthreats Category: risks associated with existing threat agents in cyberspace, (such as mafias, organized crime, malicious nation state-sponsored agents, hacktivists, insiders, etc.) which may compromise the security and normal operation of Ferrovial 's IT, OT and IoT and Information through different types of cyberattacks.

1. **Theft and impersonation of the digital identity**: Risk of suffering the theft of a digital identity for the subsequent illicit exploitation of the same, including access to confidential, professional, and personal information, blackmail, fraud to third parties, etc.

2. **Disruption and asset hijacking:** Risk that Ferrovial assets suffer a cyberattack with the purpose of causing a significant disruption in its operation or stopping its operation due to a hijacking. Distributed Denial of Service (DDoS) attacks are also included, aimed at saturating an asset's capacity, causing critical degradation in its functioning or operation.

3. **Breach, leakage, disclosure and hijacking of Information**: Risk that Ferrovial information will be revealed, stolen, or hijacked in an unauthorized manner or without the knowledge of the organization, either intentionally or accidentally. The leakage, disclosure or hijacking of information also may lead to a non-compliance with the regulatory frameworks implemented and it could be a subject to sanctions.

4. **Insiders**: Risk of suffering attacks of different nature (theft or leak of information, impersonation, denial/disruption of service, deployment of malware...) carried out by an employee or collaborator, current or former, who has or had have, legitimate access to the assets of the organization, and which may have, intentionally or unintentionally, abused such access.

5. **Cyber espionage**: Risk of theft of secrets, intellectual/industrial property or Ferrovial sensitive information by malicious nation state-sponsored agents, competitors, or other threat agents.

6. **Control and compromise of the supply chain**: Risk of having the Ferrovial' s assets compromise (theft or leak of information, unavailability/disruption of assets, fraud, blackmail...) motivated by the inadequate accreditation and supervision of services provided by partners and/or third parties, whose Security may have been compromised previously.

7. **Fraud**: Risk of financial or of business opportunity loss associated with deception techniques using digital media. Impersonation of the identity of Ferrovial employees and collaborators and of those interlocutors within a financial transaction in business processes is also included.

8. **Extortion:** Risk that Ferrovial suffers pressure through the extortion related of the possible materialization of cyber threats (business disruption by asset hijacking, disclosure of confidential information...) to obtain an economic benefit or any other benefit of different nature.

9. **Theft and loss of assets**: Risk that Ferrovial assets being stolen by malicious agents or lost by their employees and/or collaborators. This category includes elements such as computers, smartphones, tablets, and massive storage devices, as well as other elements of industrial environments.

10. **Inadequate security culture**: Risk associated with the materialization of (i) security threats based on social engineering techniques (phishing, vishing, smishing…) and/or in the exploitation of vulnerabilities, and (ii) to the inability to recognize and report any security threat that may take place in the organization (malware, impersonation, fraud…) due to a lack of Security culture, awareness and/or training.

Business Continuity Category: risks associated with an inadequate definition, implementation and maintenance of business continuity and recovery plans for all the critical processes in Ferrovial, as well as the testing and continuous improvement of these.

11. **Inadequate preparation of continuity**: Risk of (i) not having models to identify critical processes for the organization and the times, people, resources and other recovery and operation requirements needed in a serious contingency situation. It also includes the risk of (ii) not having plans for the management of the crisis, (iii) the recovery of the critical processes, (iv) its operation during the contingency and (v) the return to normality once the contingency has concluded.

12. **Inadequate contingency management**: Risk that the (i) defined contingency plans will not be effective, either because of their inadequate design or because of the lack of preparation of the people who must carry them out. This risk also includes (ii) not conducting tests and (iii) not including changes, modifications, and improvements within processes as a result of reviews and tests.

Legislation and Compliance Category: risks associated with non-compliance of Security and privacy laws, regulations, and contractual agreements to which Ferrovial, in the development of its business activity, must comply with.

13. **Inadequate identification of requirements and obligations regarding Security and/or privacy**: Risk of not identifying the laws, regulations and commitments, and associated requirements, applicable to Ferrovial in the development of its business activity.

14. **Inadequate compliance with regulations on Security and/or privacy**: Risk of receiving sanctions and losing business opportunities for failing to comply or not complying adequately with the requirements, in terms of Security and/or privacy, derived from implementing laws and regulations. It also includes non-compliance with laws and regulations specifically focused on Security.

15. **Inadequate compliance with contractual commitments in the field of Security**: Risk of suffering negative consequences (penalty, sanction, contractual termination…) for breach of contract in relation to Security in the context of the life cycle (construction, maintenance and operation) of an asset / contract managed by Ferrovial.

Cybersecurity Organization and Leadership

Ferrovial' s Cybersecurity Department will be in charge of leading the deployment of this Policy in the different business units and subsidiary companies. Accordingly, a formalized model of roles, responsibilities, and organization in matters of Security has been established that specifies:

- The roles in terms of Security at Ferrovial and in its business units and subsidiary companies.
- The Security governing Bodies at Ferrovial.
- The activities that are assigned to each of the Security roles within their scope of competence.
- How the different business units and subsidiary companies relate to each other in matters of Security.
- The level of demand in terms of Security that must be met by the different business units and subsidiary companies.
- How is set the level of demand in regards of Security.
- What information must be reported regarding Security and to which Ferrovial governing Bodies and to which Security governing Bodies.

Distribution

The Cybersecurity Department will distribute this Policy through the means it deems appropriate to all interested parties in Security matters, both internal and external.

Approval and Validity

The Corporate Cybersecurity Policy has been approved by the CEO of Ferrovial and will be applicable from the day of its publication on the Ferrovial intranet.