CODE: NG.FER.SI-001
VERSION: 3.0
DATE OF FIRST PUBLICATION: 27/01/2022
DATE OF PUBLICATION OF THE CURRENT VERSION: 22/07/2026
APPROVED BY: CEO

TITLE: Global Cybersecurity Policy
SCOPE: General
CANCELS: v.2.0
LANGUAGE OF THE ORIGINAL VERSION: English

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
2.0	22/05/2026	Update of the corporate name to Ferrovial N.V., as the parent company of the Ferrovial Group	Previous version (NG.FER.SI-001, 27/01/2022)
3.0	22/07/2026	Alignment with applicable laws, regulations (SEC, NIS2) and cybersecurity standards (NIST CSF 2.0 and ENS). Update of cybersecurity risks, goals and capabilities.	Previous version (NG.FER.SI-001, 22/05/2026)

INDEX

Introduction and Purpose

The purpose of this Global Corporate Cybersecurity Policy (the "Policy") is to establish the fundamental Security principles and objectives, and to allocate key responsibilities for working to achieve them, that strive to ensure the protection of the confidentiality, integrity, availability, traceability and authenticity of Ferrovial's IT, OT, IoT (as defined below), and the information generated and used across its business processes and operations, in accordance with Ferrovial's levels of sensitivity and criticality, while promoting compliance with applicable laws, regulations, and contractual agreements.

Scope

The Policy applies to Ferrovial N.V. and its consolidated group and, in general, to any entity under its direct or indirect control ("Ferrovial"), which, for this purpose shall mean the ability to exercise more than 50% of the voting rights or appoint or remove a majority of the administrative or management body, except in companies whose statutorily imposed control structures dictate otherwise and who shall not be considered part of Ferrovial group for purposes of this Policy.

All employees, contributors, and third parties within the scope of this Policy and its related documents are responsible for knowing, respecting, and enforcing their requirements.

The Global CISO, responsible for aligning the Security strategy with Ferrovial's vision and mission, will be primarily responsible for the communication, promotion, and enforcement of this Policy.

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

Any violation of the Policy or the policies and procedures that are a part of it are grounds for sanction by or on behalf of Ferrovial, and where relevant, may result in disciplinary and/or judicial action.

Definitions

Definitions of relevant cybersecurity terms throughout this document are included in Annex I.

Reference Standards and Requirements

The Policy is designed to align with the reference standards and applicable requirements included in its Annex II, which may be amended from time to time by the Issuing Area, informing the approval body, to update the cybersecurity regulatory standards applicable to Ferrovial.

The foregoing standards and requirements define the technological, organizational, and procedural framework to be used to develop, implement, monitor, review, maintain, and improve Ferrovial's Security.

Security Principles & Objectives

In order to support the CIA as well as traceability and authenticity of its IT, OT, IoT and the information that supports Ferrovial business operations, cybersecurity and information security ("**Security**") in Ferrovial aim to be aligned with the following Security Principles and Objectives that in turn support Ferrovial's Security strategy:

1. **Existence of a Digital and Technological Environment with the Required Level of Security**, by identifying threats and managing associated risks, striving to ensure the protection of information, IT, OT and IoT, throughout their lifecycle.
2. **Compliance with Applicable Legal, Regulatory, and Contractual Requirements,** by identifying relevant obligations, defining appropriate control models, and supporting audits, reviews, and other compliance-related activities.
3. **Adequate Management of Security Incidents and Strengthening of Resilience,** to minimize their impact on the organization, providing Ferrovial with detection and response capabilities, as well as the resources and strategies to seek resilience, recovery, and the continuity of critical business processes.
4. **Promotion of an Appropriate Security Culture**, by raising awareness and providing Security training individuals who design, implement, operate, or use Information, IT, OT and IoT, and by integrating a Security perspective into Ferrovial's governing bodies and provide them with necessary training and awareness.
5. **Security across the Supply Chain**, by managing Security risks arising from third parties, in proportion to their criticality, and promoting Supply Chain risk-management practices that promote the achievement of Security levels consistent with those of Ferrovial where commercially practicable.
6. **Harmonization of Security across Ferrovial,** by establishing a business-aligned Security model and clearly defining roles, responsibilities, and authorities related to Security within Ferrovial.
7. **Facilitation of Digitalization, Innovation, and Adoption of New Technologies as Business Enablers,** by integrating Security into innovation initiatives and evolving security capabilities and solutions to support the business.
8. **Facilitation of Business Opportunities and Tendering Processes**, by leveraging Ferrovial's Security governance model, controls, and capabilities as a differentiating factor to support business opportunities and tendering processes.
9. **Establishing Strategic Collaborations in Security Matters,** by encouraging information sharing, including indicators and best practices, and promoting Ferrovial's active participation in sectoral and global Security forums and initiatives.

These goals promote alignment with the Business and IT strategy, strengthen the management of cyber risks, support compliance with legal, regulatory, and contractual obligations, enhance the oversight of operational cyber risks, and aid efforts to ensure the organization's resilience to respond to and recover from disruptive cyber and IT-related events.

Security Capabilities

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

- **Governance**. Capabilities related to (i) understanding Ferrovial's context, processes, critical services, and relevant stakeholders; (ii) establishing and maintaining the organizational cybersecurity risk-management strategy, objectives, and policies; (iii) defining roles, responsibilities, and accountability for cybersecurity across the organization; (iv) integrating cybersecurity into enterprise risk management and decision-making processes; (v) management oversight and improvement through performance assessment and reporting; (vi) promoting a culture of compliance and ethical behaviour aligned with applicable legislative, regulatory, and contractual obligations; and (vii) managing security risks related to third parties in the Supply Chain.
- **Identification.** Capabilities related to the (i) identification, classification, and analysis of the assets relevant to Ferrovial for Security purposes; (ii) identification, analysis, and treatment of cybersecurity risks that may compromise those assets; (iii) identification of evolving legal obligations and substantive standards, and (iv) improvement through audits, reviews, and risk-mitigation processes.
- **Protection.** Capabilities related to protecting identified assets according to their level of importance for Ferrovial by (i) providing access-control mechanisms based on identity and the need-to-know and least privilege principles; (ii) promoting an appropriate Security culture and delivering training or information to employees and third parties; (iii) implementing protection mechanisms to help ensure information security; (iv) acquiring, designing, building, and configuring secure digital products and services; (v) protecting and monitoring networks and communication channels, *enforcing lines of defense in-depth in line with security architecture principles*; and (vi) establishing and enforcing procedures to help ensure the secure and appropriate use of technological resources.
- **Detection.** Capabilities related to ongoing monitoring of (i) digital products and services; (ii) digital identities and their behavior; (iii) networks and communication channels; (iv) IT, OT, and IoT infrastructure and the facilities where they are hosted; (v) internal and external cyber threats and adverse events that may impact Ferrovial's assets; and (vi) the tools and techniques used by threat agents.
- **Response**. Capabilities related to (i) defining, deploying, managing, and testing cyber-incident response plans to activate when cyber threats may impact or have impacted Ferrovial's assets; (ii) conducting detection, triage, analysis, containment, escalation, and resolution activities; and (iii) communicating with stakeholders, including those required by legislation, regulations, or contracts, as well as business units and subsidiaries.
- **Recovery.** Capabilities related to (i) ensuring the resilience of Ferrovial's assets to recover from the impact of an adverse event and return to normal operation; (ii) defining, deploying, managing, and testing recovery plans; and (iii) identifying lessons learned and applying them to prevent the recurrence or escalation of such events.

These capabilities will be developed, implemented and maintained through appropriate Security measures based on the applicable organizational structure, processes, technologies, people, and resources.

Security Risks

The Security risk categories below provide a strategic-level taxonomy of principal threat vectors applicable to Ferrovial, and which may be updated from time to time. Economic impact quantification shall be performed using criteria aligned with Ferrovial's Enterprise Risk Management framework, considering financial, operational, legal, and reputational dimensions.

RISK NAME	DESCRIPTION
Ransomware and Asset Hijacking	Encryption or block access to Ferrovial's digital assets or take control of systems, infrastructure, or services by exploiting vulnerabilities or misconfigurations.
Exfiltration and Exposure of Information	Unauthorized extraction, disclosure, or publication of Ferrovial's information, whether intentional or accidental.
Theft and Impersonation of Digital Identity	Fraudulent acquisition or misuse of digital identities to gain unauthorized access, conduct fraud, or impersonate Ferrovial personnel.
Disruption of Assets	Attacks designed to degrade, interrupt, or halt the normal operation of Ferrovial's assets.
Compromise of Supply Chain	Risks arising from vulnerabilities or attacks affecting third parties, suppliers and partners.
Deepfakes and AI-Powered Threats	Attacks using AI-generated or manipulated content to deceive individuals or systems, automate malicious actions, or evade detection mechanisms.
Crypto mining	Unauthorized use of Ferrovial's computing resources to mine cryptocurrencies.
Theft and Loss of Assets	Theft, loss, or misplacement of Ferrovial's assets, potentially exposing sensitive information or disrupting operations.
Artificial intelligence and Data Integrity Compromise	Compromise of integrity, confidentiality, or reliability of Ferrovial's data or AI models by adversarial attacks such as data poisoning, prompt injection, or model evasion, or due to the misuse of tools, skills and capabilities by employees or collaborators.
Emerging Technology and Quantum Threats	Risks associated with emerging and disruptive technologies, including the potential of quantum computing to break current asymmetric cryptographic standards.

Roles, Organization, Leadership and Deployment

Ferrovial N.V's Board of Directors exercises oversight of cybersecurity risks and strategy of Ferrovial, including oversight of material cyber risks and the effectiveness of Ferrovial's cybersecurity program.

Where appropriate, Ferrovial's management bodies approve cybersecurity risk management measures, oversee their implementation, and review and update them as may be required periodically.

Where appropriate, Ferrovial's management and governing bodies shall receive regular cybersecurity training to acquire sufficient knowledge and skills to identify risks and assess cybersecurity risk management practices and their impact. Ferrovial shall promote equivalent training across the organization on a regular basis.

Employees and contractors shall report to the Cybersecurity team any potential threats identified in the course of their day-to-day activities through the channels defined by Ferrovial. They shall also receive appropriate training or information to enable them to identify and respond to such threats.

Ferrovial's Cybersecurity Department is responsible for leading the deployment of this Policy across Ferrovial. A formalized model of roles, responsibilities, and organizational structure in Security matters has been defined. This model specifies:

- The roles established to govern and deploy Security across Ferrovial.
- The activities and responsibilities assigned to each Security role within its defined scope of competence.
- How Security, risk, and control levels will be overseen by Ferrovial's bodies.
- How the Cybersecurity Department will exercise oversight of Security throughout Ferrovial.
- The collaboration and interaction model within Ferrovial.
- The criteria used to classify business units and subsidiary companies and assign them to Security Tiers.
- The Security capabilities and controls required for each Tier.
- How Security risk and control levels will be measured at a global level and reported to Ferrovial's bodies.

The complete description of Security roles, responsibilities, and governance bodies is set out in PG.FER.SI.026 (Global Roles, Responsibilities and Cybersecurity Organization). The procedure implementing the SEC cybersecurity incident disclosure requirements is defined in PG.FER.SI.030 (Cyber Incidents Disclosure Procedure).

Exceptions to this Policy

Deviations from this Policy may be permitted exceptionally taking account of, for example, business, operational, technical, or legal justifications with due consideration for associated risks, and deployment of mitigation measures, wherever feasible. Where appropriate, deviations should be time-bound and should cease once the circumstances that justified them are addressed.

Deviations shall be documented and approval from the Global CISO sought, prior to implementation, wherever feasible.

If applicable, regard shall also be had to Ferrovial's Cyber Incident Response Plan (CIRP) and related procedures, in the context of a deviation.

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. This policy does not confer any rights or remedies upon any third party.

Review

This Policy shall be reviewed at least annually by the Cybersecurity Department, and whenever significant changes occur or circumstances require it.

Validity

The Policy will be applicable from the day of its publication on the Ferrovial intranet.

ANNEX I - Definitions

- **IT (Information Technology):** Digital Products and Services supporting Ferrovial's corporate and business operations, including applications, information systems and cloud-based services.
- **OT (Operational Technology):** Industrial Systems used in Ferrovial's infrastructure and concession assets, including control systems, SCADA, and industrial automation platforms.
- **IoT (Internet of Things):** Connected assets embedding digital capabilities in physical infrastructure, including sensors, connected devices, and smart systems deployed across Ferrovial's operations.
- **Confidentiality, Integrity, and Availability (CIA):** The three core Security properties: Confidentiality, through preventing unauthorized disclosure, Integrity, via ensuring accuracy and completeness, and Availability, through ensuring timely and reliable access for authorized users.
- **Information Classification:** the process by which information assets are categorized based on their sensitivity, criticality, and business impact, in order to determine the appropriate protection measures, in accordance with Ferrovial's Information Classification Policy.
- **NIST CSF 2.0:** The National Institute of Standards and Technology Cybersecurity Framework version 2.0, the primary reference standard structuring Ferrovial's cybersecurity capabilities across Govern, Identify, Protect, Detect, Respond, and Recover functions.
- **Global CISO:** The Chief Information Security Officer responsible for defining and leading Ferrovial's Security strategy globally, as further described in PG.FER.SI.026 (Global Roles, Responsibilities and Cybersecurity Organization).
- **Security Incident:** Any event that compromises or threatens CIA of Ferrovial's IT, OT, IoT or Information, requiring a structured detection, response, and recovery process.
- **Supply Chain:** The network of third parties, suppliers, partners, and service providers whose access to or integration with Ferrovial's systems creates cybersecurity exposure requiring proportionate risk management.

ANNEX II - STANDARDS AND REQUIREMENTS

- NIST CSF (National Institute of Standards in Technology Cybersecurity Framework).
- ISO/IEC 27001 & ISO/IEC 27002.
- Royal Decree 311/2022, of 3 May, regulating the National Security Framework (ENS).
- CIS Critical Security Controls (Center for Internet Security).
- Cloud Security Alliance (CSA).
- SEC – Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure Rules.
- Directive (EU) 2022/2555 (NIS2 – Network and Information Systems Directive).