Information security manual

20 June 2025

Retail Business - Spain

Content

Version history:

Version	Author	Approved by	Status	Reason for the problem/change	Date
v1	Retail Business Spain	Retail Business CEO	Approved	• First version	20/06/2025

1. Introduction

1.1. Purpose

This Information Security Manual (also referred to as the Retail Business Spain Information Security Policy) sets out general information security guidelines that the Retail Business Spain (hereinafter, RBS) must apply to protect itself appropriately against threats that could to some extent affect the confidentiality, integrity, availability, traceability and authenticity of information, causing loss or misuse of assets, damage to its image and reputation and/or interruption of the processes that support the business. In turn, the information security goals are defined.

By approving this Manual, RBS expresses its determination and commitment to achieving a level of information security appropriate to its needs, ensuring the uniform protection of assets and the proper management of associated risks. Likewise, it is committed to the continuous improvement of the Information Security Management System and to complying with the goals set and all applicable regulations, both internal and external.

1.2. Scope of application

This document is compulsorily applicable to all RBS personnel, as well as to the collaborating entities involved in the use and protection of the information owned by RBS and the systems that support it. Cybersecurity breaches, as well as possible penalties are covered in Iberdrola's collective agreement.

This Manual (or Information Security Policy) must be accessible to all RBS members and must be available to stakeholders.

The scope of certification at ENS medium level and ISO 27001 is: "*The information system that supports the digital channel contracting process for Group Retail business - Spain and the Public Charging Process, according to the declaration of applicability in force on the date of issue of the certificate.*"

1.3. Definitions:

The following definitions are provided to enable a common understanding of the relevant cybersecurity concepts included in this document:

- **CoE:** Centre of Excellence. Department whose purpose is to obtain digital products that add value to the business and the end customer.
- **RBS:** Retail Business Spain It is one of Iberdrola's three main businesses.
- **BISO:** Business Information Security Officer. Holds the role of CISO but is on the front line of defence, working in the business of which they are BISO.
- **GDPR:** The General Data Protection Regulation (GDPR) is a European Union regulation that governs the processing of personal data of natural persons within the EU.

- **ISMS**: The information security management system is a structured framework used to manage, control and improve the security of your information in a comprehensive manner.

1.4. Reference documentation and contacts

- Corporate Security Policy.
- Cybersecurity Risk Policy.
- Personal Data Protection Policy.
- Operational Resilience Policy.
- CCN-STIC Series: The standards, instructions, guidelines and recommendations developed by the National Cryptology Centre (CCN in Spanish) for compliance with the security standards required by the National Security Framework have been taken as a reference.
- ISO/IEC 27014.
- ISO/IEC 27001.
- Code of good governance for cybersecurity – CNMV.
- Iberdrola Group Cybersecurity Framework.
- ciberseguridad_negocio_clientes_es@iberdrola.es

2. Information Security

The measures implemented at RBS to safeguard information security are based on ensuring the following:

- Confidentiality: ownership of the information, ensuring that it is accessible only to personnel authorised to access such information.
- Integrity: ownership of the information, guaranteeing the accuracy of the data transported or stored, ensuring that it has not been altered, lost or destroyed, whether accidentally or intentionally, by software or hardware errors or by environmental conditions.
- Availability: ownership of information, ensuring that it is accessible and usable by authorised users or processes when required.
- Authenticity: ownership of information, which guarantees that an entity is who it claims to be or guarantees the source from which the data originates.
- Traceability: ownership of information, whereby it is guaranteed that the actions of an entity can be attributed exclusively to that entity.

In the same way, the following **basic principles** are taken into account:

- Security as an integrated process.

- Risk-based security management.
- Prevention, detection, response and recovery.
- Existence of lines of defence.
- Continuous monitoring.
- Periodic evaluation.
- Differentiation of responsibilities.

Finally, the current Security Manual (the Security Policy) is developed taking into account the following **minimum requirements** (which are expanded upon in the various documents that make up the regulatory body):

- Organisation and implementation of the security process.
- Risk management and assessment
- Personnel management,
- Professionalism.
- Access authorisation and control
- Protection of the facilities
- Acquisition of security products and contracting of security services
- Least privilege.
- System integrity and updating.
- Protection of stored and in-transit information.
- Prevention of other interconnected information systems.
- Activity logging and malicious code detection.
- Security incidents.
- Business continuity.
- Continuous improvement of the security process.

2.1. Mission, Vision and Context of the Organisation

The Group's Mission is based on creating value in a sustainable manner in the development of all its activities, for its shareholders, employees, customers and other stakeholders and, in general, for citizens and society as a whole. The Mission is complemented by the Vision, which reflects the aspiration to be the leading multinational group in the energy sector, playing a leading role in a better future by creating value in a sustainable manner with a quality service for people, in an efficient, secure, sustainable and environmentally friendly way. The Group's Mission and Vision are based on a firm commitment to certain Values, including dynamism, integration and Sustainable Energy. Within this last value, Security is positioned as an essential pillar for its achievement. This translates into the consolidation of Comprehensive Security as a fundamental pillar in Iberdrola's decision-making, continuously promoting innovative and sustainable security practices in all operations, thus contributing to the resilience, reliability and overall success of the Group in a constantly changing hybrid environment.

Retail Business Spain occupies a prominent position within the business strategy of Iberdrola S.A. (hereinafter, Iberdrola or the Organisation), as one of its main lines of business. This line focuses on the marketing and supply of energy, as well as on the provision of products and services focused on decarbonisation.

In the scope of Retail Business Spain, Iberdrola is dedicated to meeting the needs of end users by offering sustainable energy solutions. Its goal is to provide clean energy and innovative services that contribute to the transition towards a more environmentally-friendly energy model. Moreover, within this business line, Iberdrola also plays a key role in the purchase and sale of energy in wholesale markets, thus consolidating its position in the energy market.

In addition to Retail Business Spain, Iberdrola has other equally important lines of business These include the Group Grid Business, which is dedicated to the construction, operation and maintenance of electricity infrastructures, such as transmission lines, substations and transformer stations. These infrastructures are essential to guarantee the efficient supply of electricity from the production centres to the end user.

Iberdrola is also actively involved in the Renewables Business of the Group, where it specialises in the generation of electricity from renewable sources, such as wind, solar thermal, and photovoltaic energy, among others. This line of business reflects Iberdrola's commitment to the generation of clean and sustainable energy, thus contributing to the mitigation of climate change and the preservation of the environment.

For further details on the company's corporate purpose, please refer to the published resources Towards a global corporate purpose - Iberdrola.

2.2. Objectives

Likewise, the six information security objectives are identified, taking into account the basic principles of action established in the Corporate Security Policy

- Governance: Establish and maintain a governance model to manage and operate information security through a risk management oriented approach.
- Identification: Understand the environment and identify risks to its systems, assets, data, and capabilities.
- Protection: Design and implement safeguards to minimise the level of risk in relation to the materialisation of a potential cyber threat.
- Detection: Monitor the Organisation's information events and identify potential anomalous behaviour that could lead to the materialisation of a possible cyber threat.
- Response: Take all necessary actions to manage, analyse, respond to, escalate and mitigate identified incidents.
- Recovery: Restore assets and operations affected by a cybersecurity incident.

2.3. Cybersecurity organisation

Iberdrola is organised in such a way that the security of the Management System is controlled and guaranteed through the assignment, communication and coordination of the different roles and responsibilities in the area of information security, in order to ensure that the Management System complies with the requirements for information security.

2.3.1. Triple line of defence Iberdrola Global Cybersecurity

The internal control system of Iberdrola and the companies of the Group is configured by reference to international best practices. Accordingly, this control system is based on combined assurance around three lines of defence, providing an integrated view of how the various parts of the Organisation interact in an effective, coordinated manner, making the internal management and control processes of the Organisation's significant risks more effective.

More detail on each of the lines of defence is provided below:

- First line of defence: includes all proprietary risk functions. In this regard, the first lines will appoint Business Information Security Officers (BISOs) who will head up the definition and oversee the implementation of a specific cybersecurity plan by their business organisations, aligned with the overall cybersecurity strategy, standards and frameworks, and ensure that they are supported by adequate cybersecurity resources (people and budget). TAS (IT), Business and Corporate Areas are located in this line.

- Second line of defence: includes those functions that define the overall framework for cybersecurity governance and control, establish global regulations, standards and criteria, and support and oversee the implementation of front-line cybersecurity plans as well as the identification of relevant risks. This line includes Corporate Risks, Corporate Security and Resilience, and Cybersecurity.

- Third line of defence: provides the highest level of independence and objectivity in ensuring the effectiveness of corporate governance, risk management and internal controls, including how the first and second lines of defence achieve the risk management and control objectives. This line includes the Internal Audit department, External Audits and Regulatory Audits.

2.3.2. The Information Security Committee ofRBS (1st line of defence)

The Information Security Committee of RBS is the highest governing body for cybersecurity, attended by Senior Management (and Service and Information Officers) and led by the Business Information Security Officer (BISO), who is responsible for establishing and overseeing the cybersecurity risk management strategy. This meets at least twice a year.

The functions of the SG Committee are set out in the organisation's Management System regulations, although the following are among the most notable:

- **Review and approve** the organisation's **strategy** for progress in relation to **information security.**
- **Address the concerns of the** Retail Business Management and the various departments invited to the committee.

- Serve as a **forum for regularly reporting on the state of information security to Senior Management.**
- **Annually conduct the management review meeting** required by ISO 27001 and ENS.
- **Review and ratify the cybersecurity governance model,** as well as any possible periodic changes. Likewise, **resolve conflicts of responsibility in matters of cybersecurity.**
- **Monitor and approve the results** of the organisation's periodic cybersecurity **risk analyses**.
- **Periodically review and ratify the Information Security Policy** (this document) and the various documents that make up the regulatory framework.
- **Ensure compliance with applicable legal** and sectoral regulations.
- **Promote the performance of regular audits.**
- **Promote communication, coordination of efforts, and awareness** of cybersecurity.
- **Ensure** that information **security is taken into account** in ICT projects.
- **Monitor the performance** of security **incident management processes.**
- **Approve plans to improve the organisation's information security in order to achieve continuous improvement.**
- **Prioritise actions** related to security.
- **Promote continuous improvement** of the information security management system.

2.3.3. Cybersecurity roles and responsibilities of the first line of defence

Senior Management:

- **Provide and ensure that the necessary resources** for the planning, implementation, review, and improvement of the ISMS (Information Security Management System) are available, approving cybersecurity budgets.
- **Ensure** that **responsibilities** for roles relevant to information security are **assigned and communicated** within RBS.
- **Ensure** that the ISMS achieves the information security **objectives and results** and complies with the security policy.
- **Implement measures for cybersecurity risk management and monitor their effective implementation.**To do so, they must be informed of all risk acceptance criteria and their corresponding levels and comply with everything defined in the internal risk and exception management procedures.
- **Ensure that cybersecurity training is organised regularly** for all employees.
- **Participate in** and **promote** the work of the management review committee **(Retail Business Spain Cybersecurity Committee).**
- Responsible for ensuring compliance with applicable legal and sector regulations.
- **Ensure that the necessary internal and external audits** are carried out for the proper periodic review of the ISMS.
- Perform all **duties corresponding** to them as a **member** of the Retail Business Spain **Cybersecurity Committee**.
- **Promote continuous improvement** in cybersecurity.

Information and Service Officer

- **Approve**, within their scope of action and powers, the **requirements for information and service.**
- **Determine information and service security levels**, assessing the impact of incidents that affect information security. For this, the Information and Service Officer must request a report from the Security Manager. The criteria used to establish security levels will be set out in the CCN-CERT guide defined for this purpose and in Iberdrola's internal documentation.
- **Collaborate** (with the participation of the Security Officer and the System Officer) **in the participation of performing the mandatory risk analyses** of the assets for which they are responsible and in selecting the necessary safeguards.
- Responsible for **accepting residual risks with respect to the information and services** (or assets) for which they are responsible, as calculated in the risk analysis.
- **Responsible for the use made of the information** and, therefore, for its protection. To do so, they will rely on the Security Officer, the System Officer, and the Cybersecurity Officer of the CoE.
- **Ensure that the necessary measures are implemented with regard to their assets in order to minimise any potential adverse factors that could lead to** a security incident affecting them. In doing so, they will be supported by the Security Officer, the CoE Cybersecurity Officer and the cybersecurity team.
- **Ensure that security specifications are included in the lifecycle of their service** (and its component systems), accompanied by the corresponding control procedures. For

this, they will be supported by the Security Officer, the Cybersecurity Officer of the CoE, and the cybersecurity team.

- **Complete the cybersecurity training tasks** assigned to them in the training and awareness plan.

Security Officer (BISO and RBS ISMS Officer)):

Senior Cybersecurity Officer for RBS, responsible for determining decisions to meet information and service security requirements. Heads up reporting to Senior Management.

- As Officer for the information security management system (ISMS), they are r**esponsible for heading up the planning, implementation, operation, maintenance, supervision and continuous improvement of the information security management system**.
- **Maintain the security of the information handled and the services provided by the information systems within their area of responsibility,** in accordance with the organisation's Information Security Policy.
- **Define the information security objectives** at RBS level and the resources needed to meet them, and submit them for approval. Likewise, they will be responsible for supervising compliance with these objectives.
- **Encourage Management involvement in the implementation, maintenance and continual improvement of the ISMS.** Likewise, head up the periodic reporting of the status and level of compliance of the ISMS to Management.
- **Develop and submit for approval by Senior Management** the security strategy and policies, which must include cybersecurity risk management measures, both technical and organisational, which are proportionate to managing the risks posed to the security of the networks and information systems used and to preventing and minimising the effects of cyber incidents affecting the organisation and its services.
- **Design and implement the cybersecurity governance model** of RBS**.**
- **Represent RBS** (specific geography) **in potential working groups** for cybersecurity (risks, culture, etc.) at the Spanish and global levels within Iberdrola.
- **Head up the cybersecurity department and** all human resources within it.
- **Manage the financial resources allocated** to the **cybersecurity** department of RBS, prioritising plans based on available resources.
- **Oversee the risk management strategy.**
- **Reporting and communication of the state of cybersecurity in the RBS area to Senior Management.**
- **Oversee and develop the implementation of the regulatory framework.**Likewise, carry out the assessment and coordination of the implementation of periodic security controls on the systems and services that apply to them.
- **Approve the relevant documents** according to the established approval flows.
- **Monitor compliance with applicable regulations** on network and information system security, taking all necessary measures to ensure compliance.
- **Head up** the **audit** processes of the ISMS.
- **Act as an instructor of best practices and standards** in network and information system **security**.
- Prepare and sign the systems or assets **applicability document.**

- **Forward notifications of incidents** that have a disruptive effect on the provision of services and of detected vulnerabilities to the **supervisory authorities**, through the national CSIRTs, without undue delay**.**
- **Collect, prepare and provide information or documentation to the supervisory authority and national CSIRTs national reference point**.
- **Receive, interpret, and supervise the implementation of instructions and guidelines issued by the supervisory authority**, both for normal operations and for the correction of any deficiencies observed.
- **Ensure that external companies and suppliers** comply with the information security criteria established by the organisation.
- Define and approve the RBS incident response plan. Likewise, they will be responsible for **managing and heading up cybersecurity incidents** in accordance with the responsibilities set out in the documents governing incident management.

The Security Officer **will not report hierarchically to the Systems Manager.**

Cybersecurity Officer for CoE (Centre of Excellence)

Responsible for managing the cybersecurity of CoE assets, **working** closely with **Business Information Security Officer (BISO)** of RBS on security matters, and ensuring the continuous improvement of CoE cybersecurity. The details of their duties are set out in the organisation's Management System regulations.

System Officer

Key responsibilities include:

- **Management** and/or **supervision of the development, operation and maintenance of the information system** throughout its life cycle. The operation is the direct responsibility of Corporate Systems for those assets deployed in its infrastructure.
- **Responsible for developing the specific method for managing the implementation of security in the system defined by the Security Officer** (and the Cybersecurity Officer for CoE) and for **supervising its daily operation**, which may be **carried out by administrators, operators or corporate systems** (including its specifications, installation and verification of their correct functioning).
- **Define the topology and management of the information system,** establishing the criteria for use and the services available therein.
- **Monitor and ensure the identification of vulnerabilities and threats to the assets for which they are responsible.** In doing so, they will rely on the cybersecurity team.
- **Ensure** (with the support of the cybersecurity department**) that security measures are properly integrated** into the overall security framework.
- **Adopt** appropriate corrective measures in accordance with security assessments and audits.
- **Propose the suspension of the operation of certain information, a certain service or the entire system** for as long as deemed prudent and **until the prescribed modifications have been satisfactorily implemented, in the event of serious security deficiencies** that could affect compliance with the established requirements. To do so, they can rely on the cybersecurity team. The final decision, which will be made by the organisation's management, must be agreed upon with the Officers for the information and services affected and the Security Officer.
- **Deal with the cybersecurity training tasks** assigned to them in the training and awareness plan.

Cybersecurity technician

The main responsibilities of the cybersecurity technician (who will be part of the cybersecurity team) are to **provide support in all cybersecurity tasks assigned by the Security Officer** (BISO) and/or their **CoE Cybersecurity Officer.**

Owner of the associated asset/risk

- **Know** all **relevant information about the asset.**
- **Ensure** that the **asset** is correctly **inventoried,** classified, and duly protected.

- **Define and periodically review access restrictions and classification of important assets**, taking into account applicable access control policies.
- Monitor the status of assets.
- **Know the assigned information security risks.**
- **Approve** the information security **risk processing plan.**
- **Accept residual** information **security risks.**
- **Monitor the status of risks.**
- **Stay up to date on emerging threats and risks,** with support from the Information Security Officer (BISO) and the entire cybersecurity department.

Retail Business Spain Employees

Employees' cybersecurity duties and responsibilities are set out in the organisation's Management System regulations.

The rest of the elements that make up the RBS cybersecurity governance model (organisation chart, RASCI matrix, communication flows, designation and revocation of roles, etc.) are defined in the ISMS regulatory framework.

2.4. Regulatory framework

- **Data privacy**
    - Organic Law 3/2018 of 5 December, governing the Protection of Personal Data.
    - REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

- **Other national legislation**
    - Cybersecurity Coordination and Governance Act, 2025.
    - Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity across the Union
    - Royal Legislative Decree 1/1996, of 12 April, approving the Consolidated Text of the Intellectual Property Act.
    - Act 34/2002, of 11 July, on Information Society Services and Electronic Commerce.
    - Act 59/2003, of 19 December, on electronic signatures.
    - Royal Decree approving the Criminal Procedure Act.
    - Act 10/2021, of 9 July, on remote working.
    - Civil and criminal code.

- **Other international legislation or regulations**
    - Regulation PCI-DSS, of June 2024.
    - Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities (CER).
    - IA Act.

- **National Security Framework**
    - Royal Decree 311/2022, of 3 May, regulating the National Security Framework.
    - CCN-STIC Guides.
    - Technical Security Instructions in accordance with the National Security Framework (Resolution of 13 October 2016 of the Secretary of State for Public Administration) and Information Systems Security Auditing (Resolution of 27 March 2018 of the Secretary of State for the Civil Service).

- **UNE-ISO/IEC 27001**
    - UNE-ISO/IEC 27001:2023 Specifications for Information Security Management Systems.
    - UNE-ISO/IEC 27002:2023 Code of good practice for Information Security Management.

2.5. Awareness and training

All personnel involved with information, services, and information systems must be trained and informed of their duties and obligations regarding information security for the implementation and monitoring of this Information Security Policy.

In order to guarantee the security of information technologies applicable to RBS systems and services, the necessary mechanisms will be put in place to implement the general and specific awareness-raising and training that is necessary and essential at all levels of the RBS organisation.

2.6. Risk Management

RBS identifies and, where appropriate, assesses and categorises the risks and opportunities inherent in its activities, processes and services, planning the necessary actions to address them, preventing undesirable effects and enhancing their favourable effects.

The processes for assessing and handling information security risks are documented in corporate documents and RBS's own documents.

With regard to the risks arising from the processing of personal data, all documents governing data protection management will be followed.

2.7. Document Review and Approval

This information security manual (which serves as the Information Security Policy for the scope of ENS and ISO 27001) is formally approved by the CEO of RBS and is binding on the RBS organisation. It will be subject to a regular review process to adapt it to new circumstances, whether technical or organisational, and prevent it from becoming obsolete. It will be reviewed at least annually to ensure its continued relevance, suitability, completeness and accuracy of what the Policy establishes and will be submitted for formal approval by Senior Management.

Likewise, RBS has internal documentation that defines the guidelines governing the regulatory body.