# Information Security Manual

November 8th, 2024

## Version history:

| Version | Author | State | Reason for problem/change | Date |
|---|---|---|---|---|
| **v1** | Group Retail Business DE | Approved | • Modification of the scope of Global to Germany.<br>• Updated the footer with the iberdrola.de website | 08/11/2024 |

# 1. Introduction

## 1.1. Purpose

This Information Security Manual establishes general information security guidelines that Group Retail Business Germany (hereinafter, GRB) must apply to protect itself appropriately against threats that could affect to some extent the confidentiality, integrity, and availability of information, causing loss or misuse of assets, damage to its image and reputation and/or interruption of the processes that support the business. At the same time, the information security objectives are defined.

By approving this Manual, GRB expresses its determination and commitment to achieve a level of information security adequate to its needs that guarantees the protection of its assets in a homogeneous manner. Likewise, it is committed to the continuous improvement of the Information Security Management System.

## 1.2. Scope of application

This document is applicable, on a mandatory basis, to all GRB Germany personnel, as well as to the collaborating entities involved in the use and protection of GRB proprietary information and the systems that support it.

This Manual must be accessible to all members of GRB Germany and available on the Internet to all interested parties.

## 1.3. Reference documentation

- Corporate Security Policy (iberdrola.com).
- Cybersecurity Risk Policy (iberdrola.com).
- Personal Data Protection Policy (iberdrola.com).
- Operational Resiliency Policy (iberdrola.com).

# 2. Information security

The measures implemented in GRB to safeguard the security of information have as a cornerstone the assurance of the CIA triad:

- Confidentiality: ownership of the information, whereby it is guaranteed to be accessible only to personnel authorized to access such information.
- Integrity: property of the information, guaranteeing the accuracy of the data transported or stored, ensuring that it has not been altered, lost, or destroyed, either accidentally or intentionally, by software or hardware errors or by environmental conditions.
- Availability: property of the information, guaranteeing that it is accessible and usable by authorized users or processes when required.

The four pillars that define the information security objectives are also 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.
- Security: design and implement safeguards to minimize the level of risk in relation to the materialization of a potential cyber threat.
- Surveillance: to monitor the Organization's information events and identify potential anomalous behavior that could lead to the materialization of a possible cyber threat.
- Resiliency: to minimize the impact derived after the materialization of a possible cyber threat that could affect the Organization's business continuity capabilities.