1 Area in charge of the matter

1.1 Institutional Security Management

2 Scope

2.1 This Policy serves as a guideline for the behavior of BB Seguridade and its subsidiaries. Investees are expected to structure their administration in accordance with these guidelines, considering their specific needs as well as the legal and regulatory aspects to which they are subject.

3 Target Audience

3.1 This Policy covers all members of governance bodies, employees and third parties in the exercise of their professional activities related to the Company.

4 Regulation

4.1 Decree No. 9.637, of December 26, 2018.

5 Frequency of Reviews

5.1 This Policy must be reviewed every three years or, exceptionally, at any time, and submitted to the Board of Directors for its approval.

6 Executive Summary

6.1 This Policy aims to establish the guidelines related to information security and cybersecurity management, pursuant to the applicable legislation and regulations, demonstrating the Company's commitment to the protection of corporate information and other information assets.

7 Concepts

7.1 For the purposes of this Policy, the following concepts are adopted:

7.1.1 **Access Administrator**: Person who manages the right to access information by electronic means within the premises.

7.1.2 **Assets**: Goods and rights that the company holds at a certain time.

7.1.3 **Information Asset**: Database and files, contracts and agreements, system documentation, research information, user manuals, training material, support or operating procedures, business continuity plans, reorganization procedures, audit trails and information stored, regardless of the means or place of custody.

7.1.4 **Authentication:** Information attribute that guarantees the authorship or veracity of data and information.

7.1.5 **Information Life Cycle**: Comprises all stages of the information life cycle, namely: production, handling, reproduction, transport, transmission, storage, and disposal.

7.1.6 **Information Classification**: Identify the levels of protection that the information demands.

7.1.7 **Confidentiality**: Property that guarantees that the information is available or disclosed to an authorized user.

7.1.8 **Availability**: Property of being accessible and usable by an authorized user.

7.1.9 **Information Manager**: Area in charge of the information management (in its various forms - printed, written, electronic, etc.), throughout its life cycle, within the scope of its duties and/or responsibilities.

7.1.10 **Information Security Incidents**: Any action that may cause breach of confidentiality, integrity, and/or disclosure of the Company's information.

7.1.11 **Information**: Data, whether processed or not, that can be used for the production and transmission of knowledge, contained in any media, support, or format.

7.1.12 **Integrity**: Safeguard of the accuracy and completeness of information and processing methods so that changes are planned and authorized.

7.1.13 **Non-repudiation:** Definition that guarantees that a person is not able to deny to having performed an action.

7.1.14 **Governance Bodies**: Structures created to promote maximum alignment between the Company's management (agents) and the interests of the partners (major): General Meeting, Board of Directors, Supervisory Board, Audit Committee, Independent Audit, Internal Audit, Technical Committees, and Executive Board.

7.1.15 **Principle of Segregation of Duties**: Consists of the separation of duties or responsibilities between different people, particularly the key functions or activities of authorization, execution, approval, registration, and review or audit.

7.1.16 **Information Security**: Preservation of the confidentiality, integrity and availability, authentication, and non-repudiation of information.

7.1.17 **Cybersecurity:** a framework composed of guidelines, processes, people, and tools — including those of the controller Banco do Brasil — organized in an integrated manner to defend against and respond to threats, vulnerabilities, and intentional internal and external attacks that could directly impact the confidentiality, integrity, and availability of systems and information supporting the Company's business.

7.1.18 **Information Handling:** a set of actions and controls that, when applied, aim to protect information throughout its entire lifecycle, regardless of the medium in which it resides (physical or digital).

7.1.19 **Third Parties**: Individuals, who are not employees of the Company, and legal entities, who establish a relationship with the Company for purposes of service, contractual provision, or legal imposition.

7.1.20 **User**: One who has access to corporate information.

8 Associated Values

8.1 Reliability, Customer Focus and Feeling of Ownership.

9 Guidelines

9.1 In the formulation of this Policy, we considered the guidelines set out in the Information Security and Cybersecurity Policy of our controller, Banco do Brasil.

9.2 We treat information, in business management, as an asset.

9.3 We align information security and cybersecurity management with our business.

9.4 We plan, size, and guide the protection of information assets to meet the Company's strategic interests.

9.5 We process information throughout its life cycle in an ethical and responsible manner.

9.6 We guarantee the confidentiality, integrity, and availability of information throughout its life cycle: Production, handling, reproduction, transport, transmission, storage, and disposal.

9.7 We continuously protect and monitor information assets, reducing the possibility of operational disruption in the event of information security incidents, and we use cyber-attack prevention and response processes, controls, and technologies toward this end.

9.8 We classify the information in relation to its value or criticality for the Company.

9.9 We identify and correct vulnerabilities, threats, risks, and harmful impacts involving the Company's information assets, through periodic testing and evaluation procedures at regular intervals.

9.10 We apply protection to the information assets in a manner compatible with their impact on the Company's results and reputation, covering all processes, whether computerized or not, including when cloud computing is used.

9.11 We adopt mechanisms for the protection against misuse, fraud, damages, losses, errors, sabotage, and theft and cyber-attacks, when processing (production, handling, reproduction, transport, transmission, storage and disposal) the information generated or used by the Company.

9.12 We analyze the occurrences of removal, breach, or improper disclosure of information, under the legal and disciplinary aspects, imputing responsibility and, under the technical aspect, correcting the vulnerabilities.

9.13 We assign responsibility for the protection of information throughout its life cycle to at least one information manager.

9.14 We identify each user individually in the access control systems, holding them accountable, along with the administrator who granted the access, in duly proven cases of improper handling of corporate information carried out under their identification code.

9.15 We analyze incidents of improper handling of corporate information from legal and disciplinary perspectives, assigning accountability, and from a technical perspective, by correcting vulnerabilities.

9.16 We adhere to the principle of segregation of functions with respect to resource development, use of resources, security administration, and auditing, in the information security and cybersecurity management.

9.17 We make available to the users only the minimum information that enables them to carry out their professional activities at the Company. We do not allow the use of the information for any activity in breach of this Policy.

9.18 We disseminate information about information security and cybersecurity through permanent awareness programs, of general scope, or technical training courses for users directly involved in the use of resources.

9.19 We preserve the same information security and cybersecurity requirements adopted by the Company in the contracting of services or hiring of people and in the relationship with members of governance bodies, employees, suppliers, third parties, partners, contractors, and interns.

9.20 We grant employees and third parties access only to the information necessary for the performance of their duties and responsibilities as defined by contract or legal requirement.

9.21 We encourage companies in which we hold an interest to adopt the same principles and practices in the information security and cybersecurity management.

9.22 We define the criteria, requirements, standards, and procedures arising from this Policy in the Company's internal regulations.

Governance of Information Security and Cybersecurity of Investees

9.23 We recognize that the Company's exposure to information security and cybersecurity risks also stems from the operation of the investees.

9.24 We watch over the Company's interest by advising BB Seguridade representatives in the governance bodies of the investees on preventive and detective aspects related to information security and cybersecurity.

9.25 We promote technical exchanges between the investees, BB Seguridade, and Banco do Brasil.

9.26 We are committed to the timely reporting of information security and cybersecurity incidents between the investees aimed at a speedy resolution of incidents and exchange of technical knowledge and past experiences.

9.27 We evaluate indicators and monitor reports to governance bodies on information security and cybersecurity practices.

10 Date of Last Approval by the Board of Directors

10.1 June 27, 2025.

11 Final Provisions

11.1 Omitted cases in this Policy must be submitted for resolution by the Board of Directors.

12 Version Control Table

12.1

Effectiveness	06/27/2025 to 06/27/2028
Version	7
History of Changes	Policy update.