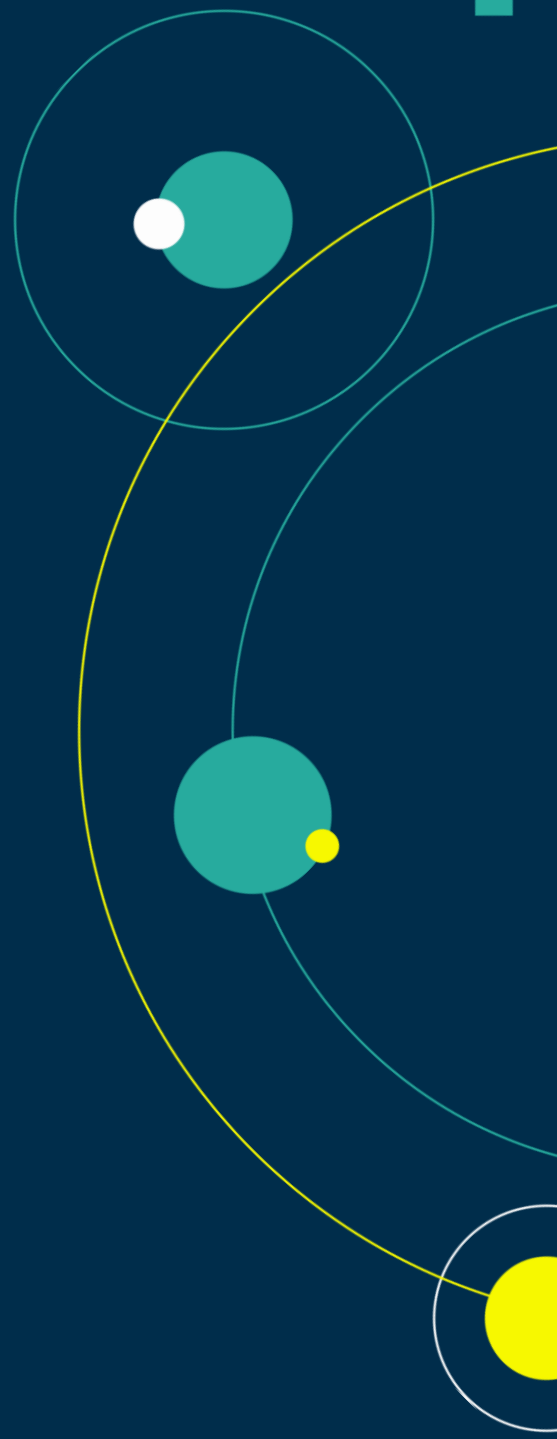




Information and Cyber Security Policy

Pol600 V.16

1. RESPONSIBLE AREA(S)

1.1. I&T Governance: Digital Governance Unit – Dites/Geati/Govit

1.2. Information Security: Cybersecurity and Digital Products Services Management Unit –
Dites/Gesec

2. SCOPE

2.1 This Policy drives the conduct of BB Tecnologia e Serviços, aims compliance needs and the legal and regulatory aspects to which BBTS is subject.

3. OBJECTIVE

3.1. The purpose of this policy is to establish principles and guidelines to be followed in the handling and protection of corporate information and the company's cyber environment.

3.2. To provide input for the established of Internal Norms, Procedures, Processes, and other documents to optimize the use of resources, improve service quality, and enable the successful management of responses to information security and cyber incidents, as well as disaster recovery.

4. REGULATIONS

4.1. CGPAR Resolution No. 41, dated August 4, 2022.

4.2. Law No. 13,709, dated August 14, 2018 – General Data Protection Law (LGPD).

5. REVIEW FREQUENCY

5.1. The Information Security Policy must be reviewed at least every three years or, in exceptional cases, at any time.

6. CONCEPTS

6.1. The following references were used in the development of this policy:

6.1.1. Decree No. 12,572, dated August 4, 2025 – National Information Security Policy

6.1.2. CGPAR Resolution No. 41, dated August 4, 2022

6.1.3. ABNT NBR ISO/IEC 27001:2022 – Information Security Management Systems – Requirements.

6.1.4. ABNT NBR ISO/IEC 27002:2022 – Code of Practice for Information Security Controls.

6.1.5. Supplementary Standard 03/IN01/DSIC/GSIPR (Institutional Security Office of the Presidency of the Republic) –Requirements for the Development of an Information and Communications Security Policy in agencies and entities of the Federal Public Administration.

6.1.6. Law No. 13,709, of August 14, 2018 – General Data Protection Law (LGPD).

6.1.7. Decree No. 10,222, of February 5, 2020 – National Cybersecurity Strategy – E-Cyber.

6.1.8. CMN Resolution No. 4,893/21 – Cybersecurity Policy and requirements for the procurement of data processing, data storage, and cloud computing services to be observed by institutions authorized to operate by the Central Bank of Brazil, of which BBTS is not regulated. Therefore, its use as a reference in the development of this policy is intended to acknowledge its importance and enhance our information and cybersecurity.

6.1.9. Decree No. 11,856, dated December 26, 2023 — National Cybersecurity Policy

6.2. Information attributes: these are the pillars that underpin information security, ensuring confidentiality, integrity, availability, and authenticity;

6.2.1. **Authenticity:** ensures that data remains accurate, complete, and is not improperly altered.

6.2.2. **Confidentiality:** ensures that data remains accurate, complete, and is not improperly altered.

6.2.3. **Availability:** ensures that data remains accurate, complete, and is not altered improperly.

6.2.4. **Integrity:** ensures that data remains accurate, complete, and is not altered improperly.

6.3. **Personal Data:** any information relating to an identified or identifiable natural person;

6.4. **Privacy:** Refers to private life, intimacy, and the right to keep personal information confidential;

6.5. **Cybersecurity:** a set of actions addressing aspects of the implementation of information security measures to protect against cyberattacks;

INFORMATION AND CYBER SECURITY POLICY

6.6. **Zero Trust:** an information security-oriented strategy; these principles are designed to ensure that the network will not be accessed by any person or device unless it is deemed and validated as trustworthy. It also treats every access attempt as a threat until it is identified and validated.

7.STATEMENT

7.1. We treat information, in business management, as an asset and, therefore, it must be fully protected through practices and policies that ensure its authenticity, confidentiality, integrity, and availability;

7.2. We align information security and cybersecurity management with the company's objectives, contributing to a secure, stable, and reliable environment for conducting business;

7.3. Without prejudice to contractual terms and expected best practices, we believe that all data provided, processed, and stored by our customers, suppliers, and partners must be guided by ethical principles and that its confidentiality must be preserved throughout the entire lifecycle of the information;

7.4. We believe that our customers, suppliers, and partners should establish within their organizations measures aimed at ensuring the confidentiality, integrity, availability, and ethical handling of all information they process.

7.5. We control and identify access to information by granting individualized access authorization to each user, making that user responsible for the security, confidentiality, and privacy of the information in their custody or to which they may become privy, as well as for all actions performed using their credentials;

7.6. We authorize and grant requesters access to and use only the information necessary for the performance of their duties and responsibilities, or as required by law;

7.7. We handle the information generated, acquired, and/or held by BB Tecnologia e Serviços in such a way as to ensure that the attributes of confidentiality, integrity, and availability are maintained throughout its entire lifecycle: collection, production, handling, reproduction (copying), sharing, transport, transmission, storage, disposal, or restoration;

7.8. We classify and label information, ensuring confidentiality, integrity, and availability, applying protection commensurate with its criticality to our activities and covering all processes, including those that handle personal data, whether computerized or not;

7.9. We have established Information Security Risk Management, Cybersecurity, and Business Continuity frameworks, identifying and addressing vulnerabilities, threats, and risks that may affect our information assets and technological environments, including our data communication network and cloud computing infrastructure;

INFORMATION AND CYBER SECURITY POLICY

- 7.10. We are committed to maintaining the technology park in a safe and secure condition, in accordance with best practices in physical and technological security. Access to the Company's physical facilities is controlled and granted only to authorized personnel, with special attention given to areas where information is processed;
- 7.11. We maintain a plan for communicating and handling cyber incidents, ensuring it outlines the actions strictly necessary to respond to an identified cyber incident;
- 7.12. We promote a culture of information security and cybersecurity through an ongoing program of awareness, education, and training aimed at employees, staff, suppliers, third parties, partners, contractors, interns, and any individual or legal entity that has a relationship with the company;
- 7.13. We investigate incidents of improper handling of corporate information in accordance with applicable legal and disciplinary provisions, holding those responsible accountable. From a technical standpoint, we use tools to protect against cyber threats;
- 7.14. We invest in mechanisms for protection, monitoring, response, and recovery from cyber risks;
- 7.15. We prioritize cyber resilience to ensure appropriate measures are taken in the event of a cyber incident or potential cyber threat;
- 7.16. We value the responsible use of threat intelligence, receiving and sharing information related to previously unidentified vulnerabilities and threats;
- 7.17. We understand that the use of AI must be responsible, ethical, and governed, to protect the confidentiality of information and maintain internal and external compliance;
- 7.18. We strengthen and improve our information security and cybersecurity controls through the knowledge gained from recognizing and responding to reported incidents;
- 7.19. We keep our physical environment controlled, monitored, and protected;
- 7.20. We encourage our employees to adopt the "clean desk" policy so that important data is not exposed;
- 7.21. We understand the importance of cybersecurity risk management in the supply chain; to this end, we strive to adopt best practices aimed at enhancing cybersecurity resilience.
- 7.22. We focus our actions on achieving zero trust by investing in technology and keeping pace with market trends;
- 7.23. We strive to develop our solutions securely throughout their entire lifecycle;
- 7.24. We handle information in an ethical and responsible manner, applying it the standards, policies, applicable laws, and best practices recognized by internal and external oversight entities;
-

8.APPROVAL

8.1. Based on Technical Note 2026/0427, this policy was reviewed by the Executive Board (Direx) on 08/18/2026, approved by the Board of Directors (Conad) of BBTS on 08/27/2026 and by the Fiscal Council (Cofis) of BBTS on 09/10/2026.