Corporate Information and Cybersecurity Policy

The **Corporate Information and Cyber Security Policy** has the following basic guidelines:

1) Ensure the confidentiality, integrity, and availability of the Organization's information through the use of Information and Cybersecurity mechanisms, balancing risk factors, technology, and cost.

2) Ensure adequate protection of information and systems against unauthorized access, copying, reading, modification, destruction, and disclosure.

3) Ensure that information assets are used only for purposes approved by the Organization and are subject to monitoring, traceability, and auditing.

4) Ensure the participation of the Organization's professionals in the Corporate Information and Cybersecurity Awareness and Education Program.

5) Ensure the existence of effective incident management and cyber resilience processes that enable the Organization to anticipate, resist, respond, recover, and adapt to adverse cyber events. These processes should ensure the protection of critical assets, rapid communication and coordination between the areas involved, senior management, communication with personal data subjects and regulators, where applicable, and the maintenance of the trust of internal and external stakeholders, minimizing operational, reputational, and strategic impacts.

6) Ensure the resolution of vulnerabilities, whether systemic or in business processes, considering the responsibilities of each area involved and the respective business managers, with due prioritization according to risk and business impact, reducing weaknesses in the Organization's environment.

7) Inform Customers and Users about the necessary Information and Cyber Security precautions when using financial products and services.

8) Ensure that risks arising from relationships with service providers and contracted partners are identified, assessed, classified, mitigated, and monitored according to the criticality of the service, regulatory and contractual requirements.

9) Ensure compliance with this Policy and the Organization's Corporate Information Security Rules and Standards.

10) Ensure senior management's commitment to the continuous improvement of the processes and resources necessary for Information and Cyber Security.

We declare that this is a true copy of the Corporate Information and Cyber Security Policy, approved at the Extraordinary Meeting of the Board of Directors (RECA) No. 1,762, dated May 9, 2011, whose latest revision, with amendments, was recorded at the Ordinary Meeting of the Board of Directors (ROCA) held on January 29, 2026.

Banco Bradesco S.A.