INFORMATION TECHNOLOGY POLICY

TABLE OF CONTENTS

1 PURPOSE

The purpose of this Policy is to set out guidelines for the selection, adoption, use and operation of information technology resources, in order to comply with the requirements of regulatory bodies, internal and external customers, and those derived from business strategies and objectives of B3 S.A. – Brasil, Bolsa, Balcão, as well as to monitor and maintain its operating environments.

2 SCOPE

This Policy applies to all administrators, employees, interns, suppliers, service providers and partners of B3 S.A. – Brasil, Bolsa, Balcão, its subsidiaries abroad, B3 Bank, BSM Market Supervision, Cetip Info Tecnologia S.A., B3 Social, and other associations (Company).

3 REFERENCES

This Policy was prepared in line with the main international references and standards related to the concepts, rules and responsibilities underlying information technology frameworks, including:

- The Company's Information Security Policy;
- Control Objectives for Information and Related Technologies (COBIT);
- Information Technology Infrastructure Library (ITIL);
- U.S. National Institute of Standards and Technology (NIST);
- The Open Group Architecture Framework (TOGAF);
- Project Management Body of Knowledge (PMBOK®); and
- Scaled Agile Framework (SAFe).

4 GUIDELINES

For technically planning projects and conducting operational and strategic activities, the Chief Technology and Cyber Security Officer shall follow the guidelines listed below, considering best practices and an efficient and safe use of information technology.

4.1 Promoting alignment with internal and external customer needs

(a) Understand customer and market demands, regulatory specifications and the specifications of the Company’s products and services to provide the most appropriate technological solutions to address them;

(b) Meet internal and external customer demands, providing technological solutions to add value to their business; and

(c) Take the necessary actions to ensure information technology service availability, in accordance with the service level agreements signed with internal and external customers.

4.2 Providing quality IT services

(a) Ensure that projects, services and maintenance carried out by the information technology areas be validated in compliance with the provisions of the relevant areas’ specific rules, before being conveyed to the Company’s operating environment; and

(b) Monitor indicators and metrics of information technology systems, environments and services to identify potential improvements to and mitigate risks faced by the Company and internal and external customers.

4.3 Following technical guidelines for contracting services and technological solutions provided by third parties

The Chief Technology and Cyber Security Officer shall also manage the approval and selection process for:

Computing equipment	Office automation, data center, communication networks, imaging and printing, and any other equipment requiring connection to the Company's computer network or to any other equipment that is already connected to the Company's computer network;
Computing systems	Information systems, smartphone applications, software or equipment designed or acquired by the Company for internal or external use;
Technology providers	Information technology solutions or services connected via dedicated links or the internet, including cloud services such as software as a service (SaaS), infrastructure as a service (IaaS), platform as a service (PaaS), or any other similar service;
Cyber protection technologies and services	Cyber security services and platforms ensuring that the technology assets supporting B3's business be adequately monitored and protected; and

Services or consulting	Specialized information technology service providers.

Only the IT areas subordinated to the Chief Technology and Cyber Security Officer shall manage the technical relationship between the Company and companies that meet any of the requirements above, but without interfering with the relationship the business areas, which functionally demand and collaborate with technical solutions, might have with any such companies.

4.4 Organizing IT service demands

Development and infrastructure demands submitted to the information technology area shall follow the steps listed below:

(a) Any and all such demands are formally filed with the IT area and will follow all approval flows defined in specific rules issued by each IT department and B3;

(b) The IT area classifies and conducts every project associated with the development of new products and maintenance of existing products based on the methodologies and tools it has defined, according to established rules and procedures;

(c) The IT area develops a processing capacity plan for a proper infrastructure dimensioning, promoting business continuity and reducing incidents and degradation of performance by the services rendered by B3; and

(d) The IT area manages both the demand and the information technology processes by taking into account the best technological solutions and architectural practices suitable to business needs.

4.5 Coordinating the preparation of the Technology Master Plan

(a) Act on the drafting, maintenance and applicability of the Technology Master Plan, in line with the Company's strategic guidelines; and

(b) Monitor and seek ways to implement the Company's guidelines and goals for budget execution and technological resource management optimization.

4.6 Enabling innovation and expanded technology service offerings

(a) Keep information on the life cycle of the technologies adopted by the Company updated;

(b) Be on the alert for technological innovation trends and new products designed by major IT software, hardware and service providers;

(c) The Company must dedicate resources to reviewing and introducing new technologies, in addition to fostering partnerships, in order to leverage the products and services it provides, thus benefiting its business and customers and furthering market evolution and its own development;

(d) Be updated with technological advancements that might enable the creation of value for the Company and reinforce its ability to preserve value; and

(e) Encourage and advance best practices in the use of information technology by the Company's subsidiaries.

4.7 Promoting technology environment and information system consistency and reliability

(a) Establish an adequate management for the computing processing capacity of the technology environment;

(b) Set out an adequate protection against cyber risks identified in technology environments;

(c) Adapt infrastructure, applications and technology processes for resilience and operational continuity purposes, according to business needs;

(d) Map, assess, mitigate and accept the risks inherent in technology activities aligned with B3's corporate risk management program; and

(e) Establish rules and procedures aiming at developing B3's IT system solutions, in line with best market practices.

5 RESPONSIBILITIES

5.1 Chief Technology and Cyber Security Officer

- Defines information technology guidelines aligned with the Company's strategic objectives and their dissemination among the staff covered by this Policy;
- Defines the organizational structure, responsibilities and powers of the managing directors and associate directors reporting to him or her; and
- Disseminates good technology practices and provides training for his or her staff on the Company's official methodologies and tools, aiming at capturing the maximum value of such methodologies and tools.

5.2 Managing directors and associate directors reporting to the Chief Technology and Cyber Security Officer

- Give publicity to this Policy and provide compliance of their departments' practices with this Policy;
- Report to the Chief Technology and Cyber Security Officer all violations of this Policy, and take corrective actions to immediately mitigate identified risks; and

- Report to the Governance and Integrated Management Department all violations of this Policy.

5.3 All B3's staff

- Use the official tools provided by the technology team to submit service requests and monitoring;
- Report any identified noncompliance with this Policy to the Governance and Integrated Management Department; and
- Assure the preservation of technology operating environments, adequately employing the tools provided by the technology teams, and submit to the powers and clearances defined in the procedures of each area.

6 FINAL PROVISIONS

The above provisions apply to the entire Company upon publication of this Policy.

7 CONTROL INFORMATION

Validity: As of June 25, 2021.

1st version: June 1, 2018.

Areas responsible for this document:

Responsible for	Area
Drafting	IT Governance Department
Revision	Trading, Finance and Corporate Systems Department Governance and Integrated Management Department Chief Technology and Cyber Security Officer Corporate Governance and Nomination Committee
Approval	Executive Board Board of Directors

Change log:

Version	Changed section	Reason	Date
01	First version	NA	June 1, 2018
02	Scope and formatting	Adjustment to new governance of B3's subsidiaries Alignment with new template	August 17, 2020
03	References Guidelines Responsibilities	Adjustment to new area structure	June 25,2021