# INFORMATION SECURITY POLICY

## TABLE OF CONTENTS

1 PURPOSE ..... 3

2 SCOPE ..... 3

3 REFERENCES ..... 3

4 CONCEPTS ..... 3

5 GUIDELINES ..... 4

6 RESPONSIBILITIES ..... 5

7 CONTROL INFORMATION ..... 8

## 1 PURPOSE

The purpose of this policy is to establish information security concepts and guidelines in order to protect the Company, its customers, and the general public.

## 2 SCOPE

This policy applies to the management, staff, interns and service providers of B3 S.A. – Brasil, Bolsa e Balcão and its subsidiaries and affiliates in Brazil and abroad (“Company”).

## 3 REFERENCES

- Code of Conduct.
- Corporate Risk Management Policy.
- Business Continuity Policy.
- Information Technology Policy.
- ABNT NBR ISO IEC 27002:2005.
- IOSCO Guidance on Cyber Resilience for Financial Market Infrastructures.

## 4 CONCEPTS

Information security as addressed in this policy is characterized by preservation of the following concepts:

- Confidentiality: ensuring that information can be accessed only by authorized persons for the necessary period;
- Availability: ensuring that information is available to authorized persons whenever necessary;

- Integrity: ensuring that information is complete, accurate and unadulterated, and that it has not been modified or destroyed in an unauthorized or accidental manner during its entire life cycle.

## 5 GUIDELINES

Information is a valuable asset of the utmost importance to the Company and fundamental to its business success, hence requiring proper protection.

Information security consists of the implementation of measures to protect the ownership, confidentiality, availability and integrity of information in any form and medium, physical or digital, from existing risks or threats, to prevent its improper, inadequate or illegal use, and to ensure that it is used in compliance with internal policies and procedures. To this end, the following guidelines should be observed.

### 5.1 Ownership, monitoring and classification of information

All information produced by the management, staff, interns and service providers, in both physical and digital format, is the sole property of the Company, including information made available to it and authorized by third parties, and must be used exclusively for its business objectives.

All the Company's equipment, means of communication and systems are subject to monitoring, and all personal information handled by these systems and this equipment or supplied to the Company is also subject to such control. All executive officers, managers, staff, interns and service provider are aware of this monitoring.

A method must be implemented to classify information according to its level of confidentiality and criticality to the Company's business.

All information must have an owner. Owners are formally designated as responsible for authorizing access to the information under their responsibility.

Information must be adequately protected and labeled in compliance with the

Company's information security guidelines throughout its life cycle, from creation to access, handling, storage, reproduction, transport and disposal.

### 5.2 Access and identity

Access to the Company's information and technological environments must be controlled in accordance with their classification and periodically reviewed so as to ensure that they can be accessed only by authorized persons with the privileges required to perform their activities.

### 5.3 Disposal of information

Disposal of information must be performed in such a way as to make its reconstruction impossible, as appropriate to the physical or digital storage medium. Information disposal must comply with the legal or regulatory timeframes for storage and take into account the needs of the business or area, whichever are greater.

### 5.4 Suppliers and external parties

Contracts with service providers that have access to the Company's information, systems and/or environments must contain clauses assuring compliance with its information security rules and penalties for non-compliance.

### 5.5 Business continuity

The Company's business continuity management establishes and maintains a strategic and operational framework designed to manage and respond to any interruption in the processes that support its business activities. This framework is governed by the Business Continuity Policy.

## 6 RESPONSIBILITIES

### 6.1 Management, staff, interns and service providers

- Comply with the information security rules.

- Protect information from unauthorized access, modification, destruction and disclosure.
- Ensure that the technological resources, information and systems at their disposal are used only in pursuit of the Company's business objectives.
- Comply with the laws and norms that regulate intellectual property.
- Refrain from discussing, citing or sharing confidential information in public environments and exposed areas (aircraft, buses, trains, restaurants, social meetings etc.), including comments and opinions in blogs and social media.
- Refrain from sharing confidential information of all kinds.
- Immediately report to Information Security any non-compliance with or violation of this policy and/or its norms and procedures.

### 6.2 Management

- Oversee and orient teams with regard to security practices and processes and access to systems.

### 6.3 Information Security

- Disseminate the Information Security Policy and Norms to management, staff, interns and service providers.
- Promote information security awareness activities for management, staff, interns and service providers.
- Propose measures to enhance information security.
- Establish norms and procedures to implement information security, covering the ownership and use of information, management of access and identity, and responding to information security incidents.

### 6.4 Administration, Supplies and Property

- Ensure that contracts with service providers with access to the Company's information, systems and/or environments contain clauses assuring compliance with this Policy and with the Company's information security rules, as well as penalties for non-compliance.

## 7 CONTROL INFORMATION

**Validity**: From June 2018.

**1st version**: 06/01/2018.

### Areas responsible for the document:

| Responsible for: | Area |
|---|---|
| Drafting | Information Security Unit |
| Revision | Governance and Integrated Management Department<br>Legal Department |
| Approval | Core Executive Committee<br>Board of Directors |

### Change log:

| Version | Item changed | Rationale | Date |
|---|---|---|---|
| 01 | Original version | N/A | 06/01/2018 |