ICBC do Brasil Banco Múltiplo S.A.

Information Security and Cyber Security Policy - Public

PUBLIC INFORMATION
The information contained in this document has been classified by the owner as PUBLIC.

1. INTRODUCTION

The purpose of the cybersecurity policy is to outline our organization's commitment to safeguarding our digital assets. This policy applies to all employees, third parties, clients and partners who have access to our infrastructure.

2. ROLES AND RESPONSIBILITIES

All employees, third parties, clients and partners share the responsibility of ensuring security for our digital assets. While our cybersecurity and IT team take the lead in maintaining security, everyone has a role to play in keeping our organization secure.

3. INFORMATION SECURITY PRINCIPLES

- **Authenticity:** guarantee that the information comes from the announced source so that its authorship and originality can be confirmed.

- **Confidentiality:** guarantee that access to information is obtained only by authorized people.

- **Integrity:** guarantee the accuracy and completeness of the information and its processing methods, in order to protect it against improper, intentional or accidental changes, during the custody or transmission.

- **Availability:** Ensure that authorized users can gain access to the information and corresponding assets whenever necessary.

4. SECURITY CONTROLS

A combination of technical and administrative measures are implemented to protect our digital assets. These measures include, but are not limited to, access controls, encryption, firewalls, intrusion detection, and antivirus software.

5. ACCESS CONTROL

To ensure efficient access control, we have adopted robust authentication, policy-based authorization, and function segregation. We follow a secure password policy, assigning access profiles according to responsibilities and monitoring access logs. By following these practices, we are protecting the system's data and resources against unauthorized use and access.

6. INFORMATION CLASSIFICATION

Information should be categorized based on their confidentiality, using the following levels: Restricted, Confidential, Internal, and Public. When doing so, business-related needs, sharing or restricting access, and consequences of improper information use must be taken into consideration.

7. INCIDENT RESPONSE

In the event of a cybersecurity incident, we will follow our incident response plan to contain and mitigate the situation. All employees must report any suspected or actual cybersecurity incidents to our cybersecurity team immediately.

8. EMPLOYEE TRAINING AND AWARENESS

We will provide regular training to all employees to increase their awareness of cybersecurity risks and best practices. We will also conduct ongoing security awareness campaigns to remind everyone of their responsibilities in protecting our digital assets.

9. INCIDENT MANAGEMENT BY THIRD PARTY PROVIDERS

ICBC Brasil contracts with service providers are formalized, evaluated in terms of risk criticality, monitored and revision. When any third-party provider contracted by ICBC Brasil has access to the bank's information and information systems, the contract or service agreement must specify the provider's security responsibility and the security requirements that must be followed.

10. COMPLIANCE AND REGULATIONS

Data security is a major concern for any company using cloud services. When it comes to third-party providers, it's important to ensure they are compliant with applicable laws and regulations and follow rigorous security practices. This may include using encryption to protect sensitive data, deploying firewalls to prevent unauthorized access, and implementing policies that monitor and flag suspicious activity. Additionally, companies should have a contingency plan in case of data breaches and ensure their employees are trained in safe data usage practices.

11. COMPLIANCE AND REGULATIONS

We will adhere to all relevant laws and regulations related to cybersecurity. Our cybersecurity team will stay informed about the latest laws and regulations, ensuring our organization remains compliant, including BACEN Res. 4893.

12. POLICY REVIEW AND UPDATES

We will regularly review and update this cybersecurity policy to ensure its continued relevance and effectiveness. All employees, third parties, clients and partners will be notified of any policy updates.

The effectiveness of Information Security policies is verified through periodic assessments by the Internal Audit.

Approved by the Board of Directors on 03/20/2023.