ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Publicly Listed Company NIRE 35300010230

CORPORATE INFORMATION SECURITY AND CYBER SECURITY POLICY

OBJECTIVE

Ensure application of the principles and guidelines for protection of intellectual property and information of the organization, of its customers and of the public generally in compliance with applicable regulations and best market practices.

INTRODUCTION

Information is one of the main assets of any organization. For the proper protection of this asset, Itaú Unibanco Holding S.A. has established this Information Security and Cyber Security policy in order to ensure the application of the principles and guidelines for protection of intellectual property and information of the organization, of its customers and of the public generally.

Our Information Security and Cyber Security strategy is designed to prevent data security breaches, minimize the risks of unavailability of our services, protect integrity and prevent any information leakage. To achieve this goal, our strategy is based on expanded perimeter protection, backed by control processes for detection, prevention, monitoring of and response to incidents, ensuring cyber security risk management and building of a robust foundation for the increasingly digital future of Itaú Unibanco. The concept of an expanded perimeter considers that information should be protected regardless of where it is located, whether at a service provider or at an international unit, throughout its life cycle, from the moment it is collected to its processing, transmission, storage, analysis and disposal.

TARGET AUDIENCE

Employees of Itaú Unibanco Holding S.A. and its subsidiaries in Brazil and abroad (Conglomerate).

For the purposes of this policy, “Employees” cover all employees, young apprentices, trainees and management members of Itaú Unibanco.

RULES

General Rule

All information security policies must be available in a place accessible to employees and must be protected against any changes.

Information security policies are reviewed annually by Itaú Unibanco and are applicable in Brazil and abroad.

Review and publication thereof in international units are the responsibility of the unit itself, requiring approval by Brazil.

Compliance with this Policy and any possible breaches, in Brazil and at international units, are periodically reported by the Corporate Security Department to the Executive Committee, Audit Committee and other risk committees.

Information Security Principles

Our commitment to the proper handling of information of Itaú Unibanco, its customers and the public generally is based on the following principles:

- Confidentiality: we ensure that access to information be obtained only by authorized persons and when absolutely necessary;

- Availability: we ensure that authorized persons have access to information whenever necessary;

- Integrity: we ensure the accuracy and completeness of information and its processing methods, as well as the transparency in dealing with the public involved.

Information Security Guidelines

Information Security at Itaú Unibanco is subject to the following guidelines:

a) The information of Itaú Unibanco, its customers and the public generally shall be treated ethically and confidentially and in accordance with current laws and internal regulations, avoiding misuse and improper exposure.

b) The information shall be used transparently and solely for the purpose for which it had been collected.

c) During its life cycle, every process shall guarantee segregation of duties, through participation of more than one employee or team of employees, so that the activity is not executed and controlled by the same employee or team.

d) Information and resources shall only be accessed if such access is duly authorized.

e) The identification of any employee must be unique, personal and non-transferable, qualifying him(her) as the one responsible for the actions taken.

f) Access granting shall follow the principle of least privilege, under which users have access solely to the information resources that are essential for the full performance of their activities.

g) A password is used as electronic signature and shall be kept secret, its sharing being prohibited.

h) Every employee shall report any risks to information to the Information Security function.

i) The Information Security function shall disseminate the responsibilities for Information Security to all employees, who must understand and comply with these guidelines.

Information Security Process

In order to ensure that any information handled is adequately protected, Itaú Unibanco adopts the following processes:

a) Information Asset Management

Information Assets mean anything that could create, process, store, transmit and even delete information. They could be technological (software and hardware) and non-technological (people, processes and facilities).

Based on their criticality, information assets must be identified individually, inventoried and protected from inappropriate access, physically (controlled access rooms) and logically (shielding or hardening, patch management, authentication and authorization settings), and have their documentation and maintenance plans updated on an annual basis.

b) Classification of Information

All information must be classified according to the required confidentiality and protection, at the following levels: Restricted, Confidential, Internal and Public. Accordingly, business needs, sharing or access restriction and the impacts of misuse of information must be considered.

c) Access Management

For access granting, review and exclusion, the tools and processes of Itaú Unibanco must be used.

Any access must be traceable to ensure that all auditable actions can individually identify the employee and the service provider to be held accountable for their actions.

d) Risk Management

Risks must be identified through a process implemented to analyze vulnerabilities, threats and impacts on Itaú Unibanco's information assets, so that adequate protections be recommended.

Scenarios of information security risks are escalated to the appropriate forums for decision making.

e) Risk Management at Service Providers

Service providers engaged by the bank are classified based on certain criteria, such as: segment criticality; remote audit; more critical information handled by the vendor; manner of access to information; frequency of access to information; history of fraud and/or information leakage; certifications; date of last assessment; segment top vendor; risk rating in the last assessment.

Depending on the classification of the service provider based on the criteria above, a provider should undergo risk assessment, ranging from on-site validation of information security controls, remote assessment of evidence or other assessment processes, to monitoring of any corrections and improvements implemented by the service providers.

For the risk assessment, a Vendor Baseline is used, consisting of a document containing several security controls based on international standards and best practices of the segment.

There is a communication channel for providers of services to Itaú Unibanco in Brazil, for them to report any material incidents relating to Itaú Unibanco information stored or processed at such service providers, pursuant to legal and regulatory requirements.

f) Treatment of Information Security and Cyber Security Incidents

The Cyber Security function monitors the security of Itaú Unibanco's technology environment in Brazil, analyzing any events and alerts for the purpose of identifying any possible incidents.

The incidents identified by alerts are classified according to their impact and the criteria adopted by Itaú Unibanco. To determine their degree of significance, aspects such as compromising of customer data and impact on the financial system will be considered.

All incidents undergo a treatment and communication process, in which all incident information such as cause, impact, classification, etc. is recorded, according to the operational procedure.

In order to improve Itaú Unibanco's ability to respond to cyber security incidents, some scenarios that may affect business continuity are considered in tests.

For incidents that may impact other financial institutions in Brazil, there is process for information exchange among institutions intended for collaboration in the mitigation of incident risks, in compliance with legal and regulatory requirements.

In foreign countries, information security and cyber security incidents are managed by each International Unit.

The Information Security and cyber security incidents of Itaú Unibanco in Brazil and abroad must be reported to the Corporate Security Department in Brazil.

The Risk function will prepare an Annual Report containing any significant incidents that occurred in the period, as well as any actions taken to prevent and respond to incidents and the results of continuity tests. This report shall be presented to the Risk Committee and to the Board of Directors, in accordance with legal and regulatory requirements.

g) Information Security and Cyber Security Awareness

Itaú Unibanco disseminates the Information Security principles and guidelines through awareness and training programs, with the objective of strengthening the Information Security culture.

Periodically, awareness campaigns or face-to-face or online training sessions are offered relating to information confidentiality, integrity and availability. These campaigns are transmitted via e-mail, corporate portal, e-learning, indoor media, social networks to employees and customers.

h) Governance with Business and Technology Functions

Initiatives and projects of the business and technology functions must be aligned with information security guidelines and architectures, ensuring the confidentiality, integrity, and availability of information.

i) Physical Security of the Environment

The purpose of the Physical Security process is to establish controls relating to granting of physical access to the environment solely to authorized personnel, according to the criticality of the information previously mapped and stated to the Property Administration.

j) Security in Application System Development

The application system development process must ensure compliance with Itaú Unibanco's security policies and with good security practices.

k) Recording of Logs

Recording of logs or audit trails of the IT environment is mandatory in order to identify: who had access; when the access was made; what was accessed and how it was accessed.

The information in logs or audit trails must be protected against unauthorized modification and access.

l) Cyber Security Program

The Itaú-Unibanco Cyber Security Program is guided by the following factors:

- Current regulations;

- Best practices;

- World scenarios.

Based on its criticality, the program is divided into:

- Critical actions - Consist of emergency and immediate corrections to mitigate imminent risks;

- Sustaining Actions - Short/medium-term initiatives to mitigate risk in the current environment, keeping the environment secure, respecting the Organization's risk appetite and allowing long-term/structuring actions to be conducted;

- Structuring Actions - Medium/long-term initiatives that address the root cause of risks and prepare the Bank for the future.

m) Perimeter protection

For protection of Itaú Unibanco's infrastructure against an external attack, we use tools and controls against: DDoS attacks, Spam, Phishing, APT, Malware, invasion of network devices and servers, application attacks and external scans.

In order to protect ourselves against information leakage, we use a number of data loss prevention tools installed on workstations, the e-mail service, the WEB browsing service, the printing service, as well as disk encryption in notebooks and mobile device management solutions.

n) Governance with International Units

Every Itaú Unibanco Unit must have an information security head, who must be independent from the business and technology functions and report to the Corporate Security Department of the head office.

Independent Audit Assessment

The effectiveness of Information Security policies is checked through periodic Internal Audit assessments.

Intellectual Property

Intellectual property is composed of intangible assets, such as trademarks, distinctive signs, advertising slogans, domain names, business names, geographical indications, industrial designs, patents and utility models, intellectual works (such as literary, artistic and scientific works, database, photographs, drawings, illustrations, architectural projects, musical works, audiovisual works, texts and etc.), computer programs and business secrets (including industry and trade secrets).

Any information and intellectual property that belong to Itaú Unibanco, or that are made available by it, shall not be used for private purposes, nor passed on to others, even if they have been obtained, inferred or developed by an employee in his(her) work environment.

Statement of Responsibility

Periodically the Employees and Service Providers directly hired by Itaú Unibanco must formally execute a statement, undertaking to comply with the Information Security policies.

The contracts entered into with Itaú Unibanco must have a clause that ensures the confidentiality of information.

Disciplinary Measures

Any violations to this policy are subject to the disciplinary sanctions provided for in the internal regulations of Itaú Unibanco companies, and in the legislation in force in Brazil and in the countries where the companies are located.

GLOSSARY

Head Office: Itaú Unibanco in Brazil.

Segregation of duties: Separation of activities between potentially conflicting functions and persons, or functions and persons with privileged information, according to which an employee cannot perform more than one duty in the authorization, approval, execution, control and accounting processes.

Cyber security: refers to the set of means and technologies used to defend information systems, infrastructure, computer networks and/or personal devices, in order to prevent damage, theft, intrusion, change or destruction of information.

APT: Advanced Persistent Threat.

Approved by the Board of Directors on March 28, 2019.