ITAÚ UNIBANCO HOLDING S.A.

CNPJ 60.872.504/0001-23 Publicly-held Company NIRE 35300010230

INFORMATION AND CYBER SECURITY CORPORATE POLICY

OBJECTIVE

To establish the principles, guidelines and assignments related to information security, protecting the information of the institution, customers, and the general public, following the best market practices and applicable regulations.

TARGET AUDIENCE

Employees of Itaú Unibanco Holding and its subsidiaries in Brazil and abroad and entities maintained or managed by the Itaú Unibanco Conglomerate.

INTRODUCTION

Information is one of the main assets of the institution. Thus, Itaú Unibanco Holding S.A has defined its Information Security and Cyber Security strategy in order to protect the integrity, availability, and confidentiality of its information.

This strategy is based on detecting, preventing, monitoring, and responding to incidents in addition to strengthening cybersecurity risk management and the construction of a robust foundation for the increasingly digital future of Itaú Unibanco.

To achieve this goal, we employ an expanded perimeter protection strategy. This concept advocates that information must be protected throughout its life cycle, from collection to disposal, no matter where it is, whether internally, in an affiliate, in a service provider or in an international unit.

PRINCIPLES OF INFORMATION SECURITY

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

- **Confidentiality:** To ensure that only authorized people obtain access to information;
- **Availability:** To ensure that authorized people have access to information whenever necessary;
- **Integrity:** To ensure the accuracy and completeness of any information and of the methods used to process it, as well as transparency in dealing with the stakeholders involved.

GUIDELINES

All information security policies must be available in a place employees can access and protected from changes.

The information security policies are reviewed every year by Itaú Unibanco both in Brazil and abroad.

The employee in charge of information security at each subsidiary will identify any guidelines or exceptions arising from regulatory requirements and the need for their publication in subsidiaries abroad, formalizing and submitting the proposed guidelines or exceptions in advance for approval by the Corporate Security Department in the Head Office.

Adoption of this Policy and possible deviations, in Brazil and in subsidiaries abroad, shall be periodically reported by the Corporate Security Department to the Executive Committee, the Audit Committee and other risk committees.

All information must be used in a transparent manner, for the purposes the client was informed of and in accordance with current legislation.

Any guidelines and possible exceptions shall be complemented using procedures with specific rules that must be observed.

INFORMATION SECURITY PROCEDURES

To ensure the information handled is properly protected, Itaú Unibanco has adopted the following procedures:

a) Asset Management

An asset is defined as anything that the institution deems relevant to the business, from technological assets (e.g. software and hardware) to non-technological assets (e.g. personnel, procedures, and facilities) as long as they are related to protecting information.

Assets, according to their criticality, must be identified, catalogued, kept up to date, have an owner, disposed of safely and be protected against improper access. The protection can be both physical (e.g. rooms with controlled access) and logical (e.g. shielding or hardening configurations, patch management, authentication, and authorization).

The assets of Itaú Unibanco, its customers and the general public must be handled in an ethical and confidential manner and in accordance with the laws in force and internal standards, promoting their proper use and preventing undue exposure of information.

b) Information and Data Classification

Information should be classified based on its confidentiality, according to internal documents.

To this end, any business-specific needs, sharing of or restrictions on access and the impact of any possible misuse of the information must be considered. The necessary protections must be defined over the course of the life cycle of the information, based on its confidentiality classification.

The information life cycle comprises: Creation, handling, storage, transport, and disposal.

c) Access Management

Any granting, revising or exclusion of access must use the tools and corporate processes of Itaú Unibanco.

Access must be traceable, enabling any employee or service provider accessing or changing information to be identified, allowing them to be held accountable.

The granting of access must follow the principle of least privilege, whereby users only have access to the information resources vital to the full performance of their duties.

Segregation of duties must permeate all critical processes, preventing one single person from executing and controlling the entire process throughout its life cycle.

Every employee must possess a unique, personal, and non-transferable identification, establishing his or her responsibility for any actions taken.

A password is a confidential, personal, and non-transferable type of information, to be used as an electronic signature and not to be shared.

d) Risk Management

Risks must be identified through an established process to analyze any threats, vulnerabilities, probabilities, and possible impact on the assets of Itaú Unibanco so that appropriate protection may be recommended. Recommendations are to be discussed in the appropriate forums.

Products, processes, and technologies must be subject to proper Information Security risk management in order to mitigate risks to acceptable levels, be they within the infrastructure of Itaú Unibanco Holding or that of its partners or service providers.

The technologies the institution employs must be in manufacture-supported and duly updated versions. Any exceptions must be approved at the competent level of authority or have compensatory controls.

e) Service Provider and Third-Party Risk Management

The service providers and partners hired by the bank should be classified considering some criteria, as internal documents.

Depending on the classification, the service provider will undergo risk assessment, which may include on-site validation of IS controls, remote assessment of evidence or other assessments, in addition to monitoring any corrections and improvements implemented by the service providers and partners.

Service providers and partners must report relevant incidents (as defined in item 6.f of this document) related to Itaú Unibanco information stored or processed by them in compliance with legal and regulatory requirements.

f) Handling of Information Security and Cyber Security Incidents

The Cyber Security Department monitors the security of the technological environment of Itaú Unibanco in Brazil, analyzing any events and alerts to identify possible incidents.

The incidents that are identified by the alerts are classified according to impact under the criteria adopted by Itaú Unibanco. To their degree of relevance, aspects such as impact on the financial system and commitment of data from clients and the general public will be considered. Incidents classified as relevant must be reported to the Regulator, the data owner, and the Audit Committee (CAUD) when they involve personal data that may entail risk or cause relevant damage to the data owners.

All incidents must undergo an analysis and notification process wherein all pertinent information is recorded, such as the cause, impact, classification, etc.

Information on incidents that may impact other financial institutions in Brazil must be shared with those institutions so as to mitigate any risks, in accordance with legal and regulatory requirements.

Information and cyber security incident management abroad is to be carried out by each International Unit which must report such incidents immediately to the Corporate Security Department in Brazil.

The Risk Management Department will prepare an Annual Report containing the relevant incidents occurring in the period, any incident prevention and response actions taken and continuity tests results. This report must be submitted to the Risk Committee, the Audit Committee and the Board of Directors, in accordance with legal and regulatory requirements..

In order to improve its incident response capabilities, Itaú Unibanco performs business continuity tests simulating critical Cyber Security incident scenarios which may compromise information availability and/or confidentiality.

Every employee must be proactive and diligent in identifying and mitigating any information security related risks and in communicating them to the Information Security Department.

g) Information and Cyber Security Awareness

Itaú Unibanco promotes the dissemination of Information Security principles and guidelines through awareness and training programs to strengthen the culture of Information Security.

In person or online awareness campaigns or training sessions regarding information confidentiality, integrity and availability are offered periodically. These campaigns are offered to employees and customers via e-mails, the corporate portal, e-learning sites, electronic media, and social networks.

h) Business and Technology Department Governance

The initiatives and projects of the business and technology departments must be aligned with the information security principles and guidelines.

i) Security of the Physical Environment

The Physical Security process establishes controls related to the concession of physical access to the environments, according to the criticality of the information handled in these environments, as described in internal documents.

j) Security in the Development of Application Systems

The systems development process should be in compliance with the internal documents, as well as the institution's general good security practices.

The productive environments must be segregated from the other environments and accessed only via application by previously authorized users or with approved tools.

k) Log Recording

All computing environment logs or audit trails must be recorded for all platforms in order to identify who accessed the information and when, what, and how it was accessed.

This information must be protected from changes and unauthorized access.

l) Cyber Security Program

O The Cyber Security Program of Itaú Unibanco is guided by the following:

- Regulations in force;
- Best practices;

- World scenarios;
- The institution's own risk analysis.

Depending on how critical the information is, the actions of the program are divided into:

- **Critical Actions:** Emergency and immediate corrections to mitigate imminent risks;
- **Support Actions:** Short/medium term risk mitigation initiatives in the current environment, ensuring environment safety while respecting the institution's appetite for risk and allowing for long-term/structuring actions to be carried out;
- **Structuring Actions:** Medium/long-term initiatives that address the root cause of risks and which prepare the bank for the future.

m) Perimeter Protection

To protect its infrastructure against external attack, Itaú Unibanco employs, at a minimum, tools and controls against DDoS, spam, phishing, and APT/ malware attacks, invasion of network devices and servers, attacks on applications and external scans.

To mitigate the risk of information leakage, the bank uses preventive tools installed on mobile devices, workstations, the e-mail service, the WEB browser service, and the printing service, in addition to encryption of data at rest and in transit.

For increased protection, physical or logical connection to the institution's corporate network by private or unmanaged or unapproved equipment is not permitted.

n) International Subsidiaries Governance

International subsidiaries must have an information security officer, independent of the business and technology departments, who reports to the Corporate Security Department.

Intellectual Property

Intellectual property is the protection that covers immaterial goods such as: trademarks, distinctive signs, advertising slogans, domain names, business names, geographical indications, industrial designs, patents of inventions and modes of use, intellectual works (such as literary, artistic and scientific works, databases, photographs, drawings, illustrations, architectural projects, musical works, audiovisual works, texts, etc.), computer programs and trade secrets (including industrial and commercial secrets).

Itaú Unibanco is the exclusive owner of any and all inventions, creations, works and improvements that have been or will be created or made on behalf of Itaú Unibanco by persons acting as administrators, employees and/or interns, during the entire term of their commission or contract of employment or internship. Any information and content which is the intellectual property of Itaú Unibanco, or which it has made available, including information and content which employees obtain, infer or develop themselves, either in their work environment or using the resources of the institution, must not be used for private purposes nor transferred to third parties without prior and express authorization from Itaú Unibanco.

It is the duty of all employees to protect the intellectual property of Itaú Unibanco.

Statement of Adherence

On a regular basis, Itaú Unibanco employees must formally sign a statement of adherence in which they undertake to act in accordance with the Information Security policies.

Contracts signed with Itaú Unibanco must include a clause ensuring information confidentiality and the obligation to follow the regulations in force, regarding the topic of information security.

ROLES AND RESPONSABILITIES

Corporate Information Security policies, strategies and processes are supervised by the Corporate Security Department in Brazil and abroad and discussed in the specific risk related forums of the departments and the Executive Committees dealing with Operational Risk or Technology.

Internal Audit

Internal Audit roles and responsibilities are described in Internal Policy.

Internal Controls

Internal Controls roles and responsibilities are described in internal policy.

Corporate Security

- To improve the quality and effectiveness of the institution's processes, seeking the integrity, availability, and confidentiality of its information;
- To protect information from threats, seeking to ensure business continuity and to minimize business risks;
- To establish, implement, operate, monitor, and ensure the continuous improvement of the information security management system (ISMS).
- To define and formalize the governance objectives, controls, and strategy for information security, together with the Information Security Executive Committee.
- To coordinate actions to achieve the governance objectives and strategies for information security approved by the committees, with the participation of the responsible departments.
- To establish and promote a culture of information security.
- To propose information security investments to fulfill the objectives of this policy.
- To define information security policies and standards to be employed in the institution's processes, products, and technologies.
- Define minimum security standards for International Units and controlled Companies in Brazil and abroad and entities maintained or managed by the Itaú Unibanco Conglomerate, ensuring alignment with the information security objectives set by the Holding Company.

International Subsidiaries
To proactively identify, prevent and correct any risks and periodically report to the Corporate Security Department.

Companies and Entities in the Conglomerate
Companies in the conglomerate controlled in Brazil and abroad and entities maintained or managed by the Itaú Unibanco Conglomerate must assess the guidelines and requirements set forth in this policy and its annexes, periodically reporting the identified risks to the Corporate Security Department, adjusting their internal security procedures according to their business segment and risk appetite. These companies must be classified and have a governance model based on risk assessment, which takes the following aspects into account: Impact on the image of the Holding Company, Architecture and Connectivity with the Holding Company, and Volume of stored sensitive data. This governance model may vary between assessment and direct monitoring of adherence to the defined controls or following a declaration of adherence to be made by the company itself.

Information Security Executive Committee
To approve the strategy, objectives, budget, and actions necessary to mitigate the risks in the institution's information security processes.

Audit Committee – CAUD
S Supervising the risk management strategy, its respective processes and internal controls, as well as monitoring the information security projects of the Itaú Unibanco Conglomerate.

Technology Department

To keep the institution's technology infrastructure accessible and current with the security standards implemented, by the corresponding deadlines for each level of risk.

Business Department
To protect the information of Itaú Unibanco in its charge.

DISCIPLINARY SANCTIONS
Violations of this policy are subject to the disciplinary sanctions provided in internal policies, as well as in the internal standards of Itaú Unibanco group companies and the legislation in force in their locations.

RELATED DOCUMENTS
This Information Security Corporate Policy is complemented by specific Information Security procedures, in accordance with all legal and regulatory aspects and as approved by the Cyber Security Governance and Projects Division and the Cyber Security Operations Division, subordinate to the Corporate Security Directorate of the Itaú Unibanco Risk and Finance Department.

Approved by the Board of Directors in 25/03/2021