ITAÚ UNIBANCO HOLDING S.A.

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

INFORMATION SECURITY AND CYBER SECURITY CORPORATE POLICY (GLOBAL)

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 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 considers that information must be protected regardless of where it is located, whether internally, in an affiliate, in a cloud service, in a service provider or in an international unit, throughout its life cycle, from collection to disposal.

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

Information security documents (policy, rules and procedures) must be available in a place accessible to employees and protected against changes.

The Corporate Policy of Information Security and Cyber Security is revised annually by Itaú Unibanco with application in Brazil and abroad.

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

Adherence to this Policy and eventual deviations, in Brazil and in units abroad, are periodically reported by the Corporate Security Board to the Executive Committee, Audit Committee and other risk committees.

The information must be used transparently, for the purposes informed to the customer and in accordance with current legislation, as described in the internal polices.

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, inventoried, kept up to date, owned, safely disposed of and protected against unauthorized access. Protection may be physical (e.g. rooms with controlled access) and logical (e.g. shielded or hardened settings, 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) Classification of Information

Information must be classified according to confidentiality, as described in the 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 approval authority or have compensatory controls.

e) Risk Management in Service Providers and Partners

Service providers and partners hired by the bank must be classified considering certain criteria, in accordance with internal procedure.

Depending on the classification, the service provider or partner will undergo a 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 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.

The guidelines for contracting relevant services in accordance with regulatory definitions are described in internal procedures.

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 with respect to their impact, according to the criteria adopted by Itaú Unibanco. For its degree of relevance, aspects such as impact on the financial system and compromise of customer and general public data will be considered , as described in the Information Security and Cyber Security Incident Handling Plan (Brazil). Incidents classified as material must be reported to the Regulator, to the data subject, and to the Audit Committee (CAUD), when they involve personal data that may pose a risk or cause material damage to data subjects and if the involvement of internal employees, cases will be reported for joint action with the Inspectorate.

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.

Abroad, the management of information security and cybernetic incidents is carried out by each International Unit, which must timely report them to the Corporate Security Department in Brazil.

The Risk Management Department will prepare an Annual Report with the relevant incidents that occurred in the period, actions taken to prevent and respond to incidents and results of continuity tests. This report must be presented 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 is to perform 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 Information Security culture, as part of the Integrity and Ethics Program, as described in internal procedure.

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 granting physical access to environments, according to the criticality of the information handled in these environments, as described in the internal documents.

j) Security in the Development of Application Systems

The systems development process must ensure adherence to the internal documents.

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

k) Secure Configuration

The secure configuration process must ensure adherence in internal procedure defined by the Information Security Architecture department, establishing a secure configuration of the systems acquired by the institution in accordance with best security practices.

l) 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.

m) Cyber Security Program

Itaú-Unibanco's *Cyber Security* Program is guided by the following principles:

- 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:** Consists of 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.

n) Perimeter Protection

To protect Itaú Unibanco's infrastructure against an external attack, we use, at a minimum, tools and controls against: DDoS attacks, *Spam*, *Phishing*, APT / *Malware*, invasion of network devices and servers, attacks on external applications and *scans* , and also penetration testing.

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.

In order to increase protection, physical or logical connection to the institution's corporate network is not allowed, by private unmanaged or non-approved equipment.

o) International Unit Governance

International units 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 utility model, 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.

The contracts signed with Itaú Unibanco must have a clause that ensures the confidentiality of information and the obligation to follow the regulations in force, referring to 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 the Internal Audit Policy.

Operational Risk
The roles and responsibilities of Operational Risk are described in the Integrated Operational Risk Management and Internal Controls 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.
- Propose investment for information security to meet 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 subsidiaries in Brazil and abroad and Entities maintained or managed by the Itaú Unibanco Conglomerate, ensuring alignment with the information security objectives defined by the Holding.

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

Conglomerate Companies and Entities
Conglomerate subsidiaries in Brazil and abroad and entities maintained or managed by Itaú Unibanco Conglomerate must assess the guidelines and requirements established in this policy and its annexes, periodically reporting the identified risks to the Corporate Security Department, adapting their internal security procedures as its business segment and risk appetite. These companies must be classified and have a governance model based on risk assessment, which considers the following aspects: Impact on the image of the Holding, Model of Architecture and Connectivity with the Holding, and Volume of sensitive data stored. This governance model can vary between assessment and direct monitoring of adherence to defined controls or following a declaration of adherence to be carried out by the company.

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
Supervise the risk management strategy, its respective processes and internal controls, as well as monitor the information security projects of the Itaú Unibanco Conglomerate.

Technology Department
Keeps the institution's technology infrastructure accessible and up to date with the security standards implemented, by the corresponding deadlines for each level of risk.

Business Department
Protects the information of Itaú Unibanco in its responsibilities.

DISCIPLINARY SANCTIONS
Violations of this policy are subject to the disciplinary sanctions provided for in internal documents, as well as the internal rules of Itaú Unibanco companies and the legislation in force where the companies are located.

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.

Frameworks and Regulations
Resolution 4,893 of the Central Bank of Brazil

- Resolution Nº 85 of the Central Bank;

- Resolution 4,752 of the Central Bank of Brazil

- General Personal Data Protection Law (LGPD) - Law No. 13,709/2018;

- Resolution Nº 35 of the CVM;

- Joint Resolution No. 1, of May 4, 2020 (Open Finance);

- SUSEP Circular 638;

- CNSP Resolution No. 415 of SUSEP, of July 30, 2021 (Open Insurance);

- And other regulations and laws related to the topic.

- ABNT NBR ISO/IEC 27001:2013 - Information technology - Security techniques - Information security management systems - Requirements;

- ABNT NBR ISO/IEC 27701:2019 - Security techniques - Extension of ABNT NBR ISO/IEC 27001 and ABNT NBR ISO/IEC 27002 for information privacy management - Requirements and guidelines;

GLOSSARY
APT: Advanced Persistent Threat

Cyber Security: Term that designates the set of means and technologies used to defend information systems, infrastructure, computer networks and/or personal devices with the goal of preventing information corruption, theft, intrusion, alterations or destruction.

Relevant Damages: Action that may impact the privacy of the individual, which may cause high risk to their physical or moral integrity.

Technology Infrastructure: set of infrastructure assets and technology systems.

Segregation of Duties: The separation of tasks between departments and personnel that are potentially in conflict or that possess privileged information, in which a single employee must not exercise more than one role in the authorization, approval, execution, control and accounting processes.

Approved by the Board of Directors on 26.01.2023