ITAÚ UNIBANCO HOLDING S.A.

PUBLIC DISCLOSURE VERSION

CORPORATE INFORMATION SECURITY AND CYBER SECURITY POLICY

1. OBJECTIVE

Establish the principles, guidelines, and responsibilities related to information security, protecting the institution's, clients', and the general public's information, in compliance with market best practices and applicable regulations.

2. TARGET AUDIENCE

Employees of Itaú Unibanco Holding and its controlled companies in Brazil and abroad, as well as entities maintained or managed by the Itaú Unibanco Conglomerate.

3. INTRODUCTION

Information is the institution's main asset. Therefore, Itaú Unibanco Holding S.A. defines the Information Security and Cyber Security strategy to protect the integrity, availability, and confidentiality of information.

This strategy is based on detection, prevention, monitoring, and incident response, and it strengthens the management of cyber security risk and the construction of a robust foundation for Itaú Unibanco's increasingly digital future.

To achieve this goal, we use an expanded perimeter protection strategy. This concept considers that information must be protected regardless of where it is—whether internally, in an affiliate, in a cloud service, with a service provider, or in an international unit—throughout its entire lifecycle, from collection to disposal.

4. INFORMATION SECURITY PRINCIPLES

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

- **Confidentiality**: Ensure that access to information is granted only to authorized individuals.
- **Availability**: Ensure that authorized individuals have access to information whenever necessary.
- **Integrity**: Ensure the accuracy and completeness of information and its processing methods, as well as transparency in dealings with all involved parties.

5. GUIDELINES

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

The Corporate Information Security and Cyber Security Policy is reviewed annually by Itaú Unibanco and applies in Brazil and abroad.

The inclusion of guidelines or exceptions due to regulatory requirements and their publication in international units will be identified by the unit's information security officer, who must formally submit the proposed guidelines or exceptions in advance for approval by the Cyber Security Directorate.

Adherence to this Policy and any deviations, both in Brazil and in international units, are periodically reported by the Cyber Security Directorate to the Executive Committee, Audit Committee, and other risk committees.

Information must be used transparently, for the purposes communicated to the client and in accordance with applicable legislation, as described in the internal documents.

The guidelines and any exceptions are complemented by procedures with specific rules that must be observed.

6. CYBER SECURITY PROGRAM

The Cyber Security Program aims to monitor, assess, and analyze the performance and compliance of processes related to Information Security and Cyber Security. It is based on risk management, using the Security Risk Map methodology, which enables a structured evaluation of the control environment.

In addition, the program is structured as an internal maturity model, with annual periodic assessments, allowing continuous monitoring of the evolution and effectiveness of the security practices adopted by the organization.

The program is guided by the following principles:

- Applicable regulations;
- Best practices;
- Global scenarios;
- Risk analyses conducted by the institution itself.

According to their level of criticality, the program's actions are divided into:

- **Critical**: Consist of emergency and immediate corrections to mitigate imminent risks;
- **Sustainment**: Short/medium-term initiatives to mitigate risk in the current environment, keeping it secure, respecting the institution's risk appetite, and allowing long-term/structural actions to be carried out;
- **Structural**: Medium/long-term initiatives that address the root cause of risks and prepare Itaú Unibanco for the future.

7. INFORMATION SECURITY PROCESSES

To ensure that the information handled is adequately protected, Itaú Unibanco adopts the following processes:

a) Asset Management

An asset is understood as anything the institution considers relevant to the business, including technological assets (e.g., software and hardware) and non-technological assets (e.g., people, processes, and physical dependencies), provided they are related to information protection.

Technological assets, according to their criticality, must be identified, inventoried, kept up to date, assigned an owner, securely disposed of, and protected against unauthorized access. Protection can be physical (e.g., rooms with controlled access) or logical (e.g., hardening configurations, patch management, authentication, authorization, and monitoring).

Itaú Unibanco's assets, as well as those of clients and the general public, must be handled ethically and confidentially, in accordance with applicable laws and internal regulations, promoting proper use and preventing undue exposure of information.

b) Information Classification

Information must be classified according to its level of confidentiality, as described in the internal documents.

For this purpose, business needs, sharing or access restrictions, and the potential impacts of improper use of information must be considered. Based on the confidentiality classification, the necessary protections must be established throughout its entire lifecycle.

The information lifecycle includes: Creation, Handling, Storage, Transport, and Disposal.

c) Access Management

Access grants, reviews, and removals must use Itaú Unibanco's corporate tools and processes.

Accesses must be traceable to allow the identification of the individual employee or service provider who accessed or modified the information, ensuring accountability.

Access granting must follow the least privilege principle, meaning users should have access only to the information resources strictly necessary for the proper performance of their activities and duly authorized.

Segregation of duties must permeate all critical processes, preventing a single individual from executing and controlling the process throughout its entire lifecycle.

The identification of any employee must be unique, personal, and non-transferable, qualifying them as responsible for the actions performed.

Passwords are confidential, personal, and non-transferable information and must be used as an electronic signature; sharing passwords is strictly prohibited.

d) Risk Management

Risks must be identified through established processes for threat analysis, vulnerability identification, and assessment of probabilities and impacts on Itaú Unibanco's assets, so that appropriate protections can be recommended. These recommendations are discussed in the relevant forums.

Products, processes, and technologies must have proper Information Security risk management to reduce risks to acceptable levels, regardless of whether they are within Itaú Unibanco Holding's infrastructure, partners, or service providers.

Technologies used by the institution must be in versions supported by their manufacturers and properly updated according to patch management processes. Any exceptions must be approved by the appropriate authority or have compensating controls in place.

e) Risk Management for Service Providers and Partners

Service providers and partners contracted by Itaú Unibanco must be classified according to criteria described in internal procedure and its annexes.

Based on this classification, the service provider or partner will undergo a risk assessment, which may include on-site validation of Information Security controls, remote evaluation of evidence, or other assessments, as well as monitoring of 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, as defined by regulations, are described in the internal procedures

f) Information Security and Cyber Security Incident Handling

The Cyber Security area monitors the security of Itaú Unibanco's technology environment in Brazil, analyzing events and alerts to identify possible incidents.

Incidents identified through alerts are classified according to impact, based on criteria adopted by Itaú Unibanco. Their level of relevance considers aspects such as impact on the financial system and compromise of client and public data, as described in the Information Security and Cyber Security Incident Handling Plan (Brazil).

All incidents undergo an evaluation process, where all relevant information is recorded, such as cause, impact, classification, and other necessary details. After evaluation, according to the governance described in the Information Security and Cyber Security Incident Handling Plan (Brazil), incidents classified as relevant and recommended for communication must be reported to the Regulator and/or the data subject, as well as to the Audit Committee (CAUD). If internal employees are involved, cases will be reported for joint action with the Inspection department.

Information about incidents that may impact other financial institutions in Brazil must be shared with other institutions to help mitigate risk, in compliance with legal and regulatory requirements.

Abroad, the management of information security and cyber incidents is carried out by each International Unit, which must promptly report them to the Cyber Security Directorate in Brazil.

The Cyber Security Directorate will prepare annual reports containing relevant incidents that occurred during the period, actions taken for prevention and incident response, and results of continuity tests. This report must be presented to the Risk Committee, the Audit Committee, and the Board of Directors, in compliance with legal and regulatory requirements.

To improve incident response capability, Itaú Unibanco conducts semiannual business continuity tests simulating critical Cyber Security incident scenarios that may compromise the availability and/or confidentiality of information.

To anticipate new threats, Itaú Unibanco maintains threat intelligence processes and actively participates in cybersecurity forums within the industry and government, in Brazil and abroad, to strengthen defenses.

Every employee must be proactive and diligent in identifying, reporting to the Cyber Security Directorate, and mitigating risks related to information security.

g) Information Security 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 and Cyber Security, as part of the Integrity and Ethics Program.

Periodically, awareness campaigns or training sessions are made available, which may be in-person or online, covering topics related to confidentiality, integrity, and availability of information. These campaigns are delivered through emails, the corporate portal, e-learning platforms, media, or social networks to employees and clients.

h) Governance with Business and Technology Areas

Initiatives and projects from business and technology areas must be aligned with the principles and guidelines of information security.

i) Physical Security of the 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 Application Systems Development

The system development process must ensure compliance with the internal documents for International Units, as well as the institution's security best practices.

Production environments must be segregated from other environments and accessible only through the application by previously authorized users or by approved tools.

k) Secure Configuration

The secure configuration process must ensure compliance with internal procedure as defined by the Information Security Architecture area, establishing a secure configuration for the systems acquired by the institution in accordance with security best practices.

l) Log Recording

It is mandatory to record logs or audit trails of the computing environment for all platforms, in order to allow identification of: who accessed, when the access occurred, what was accessed, and how it was accessed.

m) Perimeter Protection

To protect Itaú Unibanco's infrastructure against external attacks, we use, at a minimum, tools and controls against: denial-of-service attacks (DDoS), Spam, Phishing, APT/Malware, network device and server intrusions, application attacks, as well as external and internal vulnerability scans and penetration tests.

To mitigate the risk of information leakage, we use preventive tools installed on mobile devices, workstations, and servers, in email services, web browsing services, and printing services, in addition to encryption for data at rest and in transit.

To enhance protection, physical or logical connection to the institution's corporate network is not allowed for personal equipment that is unmanaged or not approved by Itaú Unibanco.

n) Internal Protection

To protect Itaú Unibanco's infrastructure against internal attacks, we use an approved antimalware tool to counter cyber threats. The antimalware is responsible for detecting, protecting, and mitigating these threats.

o) Governance with International Units

International units must have an Information Security officer, independent from business and technology areas, who reports in a matrix structure to the Cyber Security Directorate.

p) Cyber Resilience

Cyber Resilience is the ability to manage and recover the environment in the face of cyberattacks, protecting the integrity and confidentiality of data. It is one of the fundamental principles of Itaú Unibanco Holding S.A.'s Organizational Resilience Program, as described in the internal document

7.1. Intellectual Property

Intellectual property refers to the protection applied to intangible assets, such as: trademarks, distinctive signs, advertising slogans, domain names, trade names, geographical indications, industrial designs, invention patents and utility model patents, 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).

All inventions, creations, works, and improvements that have been or may be created or developed by the employee for Itaú Unibanco, in the capacity of administrator, employee, and/or intern, during the entire term of the mandate, employment contract, or internship contract, belong exclusively to Itaú Unibanco. Any information and content whose intellectual property belongs to Itaú Unibanco, or has been made available by it—including information and content obtained, inferred, or developed by the employee in their work environment or using the institution's resources—must not be used for personal purposes or disclosed to third parties without Itaú Unibanco's prior and express authorization.

It is the duty of all employees to ensure the protection of Itaú Unibanco's intellectual property.

7.2. Responsibility Statement

Periodically, Itaú Unibanco employees must formally adhere to a statement, committing to act in accordance with Information Security policies.

Contracts signed with Itaú Unibanco must include a clause that ensures the confidentiality of information and the obligation to comply with current regulations related to information security.

8. ROLES AND RESPONSIBILITIES

The corporate policies, strategies, and processes for Information Security are supervised in Brazil and abroad by the Cyber Security Directorate and discussed in specific risk forums of the areas and in Executive Committees that address Operational Risk or Technology.

8.1. Employee

Protecting the organization's information and acting proactively and consciously to ensure the integrity, confidentiality, and availability of corporate data, in compliance with Information Security policies, are actions that constitute a shared responsibility of all employees.

8.2. Cyber Security

The Cyber Security Directorate is committed to the continuous improvement of its systems, processes, and practices to ensure the integrity, availability, and confidentiality of information. To achieve this, the following guidelines are adopted:

- Continuously enhance the quality and effectiveness of information security processes, focusing on the protection of informational assets and the mitigation of business risks;
- Protect information against internal and external threats, ensuring operational continuity and organizational resilience;
- Establish, implement, operate, monitor, and review the Integrated Management System (SGI), promoting its continuous improvement based on indicators, audits, and lessons learned;
- Define and formalize objectives, controls, and information security governance strategies, together with the Information Security Executive Committee, ensuring alignment with corporate guidelines;
- Coordinate and monitor strategic actions involving responsible areas to achieve the objectives defined by the committees;
- Promote and disseminate an organizational culture focused on information security, encouraging safe and conscious behaviors;
- Propose strategic investments that enable compliance with the objectives of the information security policy;
- Establish information security policies and standards applicable to processes, products, and technologies, focusing on consistency and compliance;
- Define minimum security standards for International Units, companies controlled 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;
- Define, monitor, manage, and report risk appetite metrics under the responsibility of Information Security, related to the executive level (Executive Committee – EC), ensuring alignment with corporate guidelines and supporting strategic decision-making.

8.3. Internal Audit

The roles and responsibilities of Internal Audit are described in the internal policy.

8.4. Operational Risk

The roles and responsibilities of Operational Risk are described in the internal policy

8.5. International Units

Act proactively in identifying, preventing, and correcting risks, and report periodically to the Cyber Security Directorate.

8.6. Companies and Entities of the Conglomerate

Companies within the conglomerate controlled in Brazil and abroad, as well as entities maintained or managed by the Itaú Unibanco Conglomerate, must assess the guidelines and requirements established in this policy and its annex, periodically reporting identified risks to the Cyber Security Directorate, and 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 considers the following aspects: impact on the Holding's image, architecture and connectivity model with the Holding, and volume of sensitive data stored.

This governance model may vary between direct evaluation and monitoring of adherence to defined controls or following a self-declaration of compliance to be carried out by the company itself.

8.7. Information Security Executive Committee

Approve the strategy, objectives, budget, and actions necessary to mitigate risks in information security processes.

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

8.9. Technology Area
Maintain the technology infrastructure available and updated with the implemented security standards, within timeframes compatible with risk levels.

8.10. Business Area
Protect Itaú Unibanco's information under its responsibility.

9. DISCIPLINARY SANCTIONS
Violations of this policy are subject to the disciplinary sanctions set forth in the internal regulations of Itaú Unibanco companies and the legislation in force where the companies are located.

10. RELATED DOCUMENTS

This Corporate Information Security and Cyber Security Policy is complemented by specific internal Information Security procedures in compliance with legal and regulatory aspects and approved by the Cyber Security Board, within the Risk Area structure of Itaú Unibanco.

Frameworks and Regulations

- CMN Resolution No. 4,893/2021 of the Central Bank

- BCB Resolution No. 85/2021 of the Central Bank

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

- CD/ANPD Resolution No. 15/2024

- CVM Resolution No. 35/2021

- BACEN Joint Resolution No. 1/2020 (Open Finance)

- SUSEP Circular No. 638/2021

- CNSP Resolution No. 415/2021 (Open Insurance)

- ANEEL Normative Resolution No. 964/2021

- Securities and Exchange Commission (SEC) – Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure

- And other regulations and laws related to the topic

- ABNT NBR ISO/IEC 27001:2022 – Information security, cybersecurity, and privacy protection – 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.

11. GLOSSARY

APT (Advanced Persistent Threat): Advanced persistent attacks.

Cyber Security: The term that refers to the set of means and technologies employed in the defense of information systems, infrastructure, computer networks, and/or personal devices, with the objective of preventing damage, theft, intrusion, alteration, or destruction of information.

Relevant Damage: An action that may impact an individual's privacy, potentially causing a high risk to their physical or moral integrity.

Technology Park: A set of infrastructure assets and technology systems.

Segregation of Duties: The separation of activities between areas and individuals who may have conflicting interests or privileged information, in which an employee cannot perform more than one function in the processes of authorization, approval, execution, control, and accounting.

Approved by the Board of Directors on 02.26.2026