

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

Private Key Custody And Protection Policy

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Contents

1. Purpose	2
2. Scope	3
3. Terms and Definitions	4
4. General Guidelines	5
4.1. Principles	5
4.2. Company control and provider support	6
5. Architecture and Custody of Control Instruments	7
5.1. Wallet architecture and distribution of assets	7
5.2. Key generation and ceremonies	7
5.3. Security modules and cryptographic techniques	8
5.4. Storage, sharding and redundancy	8
6. Access and Transaction Authorization	9
6.1. Granting, approval authorities and deactivation of access	9
6.2. Transaction authorization and signing	10
7. Life Cycle, Reconciliation and Orders from Authorities	10
7.1. Rotation, reissuance and destruction	10
7.2. Reconciliation and demonstration of control	11
7.3. Court orders and asset freezing measures	11
8. Monitoring, Incidents and People	11
8.1. Monitoring, records and testing	11
8.2. Response to compromise and continuity	12
8.3. People, training and confidentiality	12
8.4. Prohibitions	12
9. Review	13

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

10. Reference Standards	13
11. Effectiveness	14
12. Version Control and History	14

1. Purpose

This Policy sets out the guidelines of Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. (the "Company") for the custody and protection of private keys and other control instruments of the virtual assets of its clients and users, in compliance with articles 43, item VI, and 49 of BCB Resolution No. 520 of November 10, 2025, with the aim of ensuring the confidentiality, integrity and availability of these instruments and, consequently, the preservation of the virtual assets held in custody and the exercise of the rights of their holders.

The Company is the custodian of its clients' virtual assets, and the provisions of this Policy relating to custody, including those that refer to articles 9 and 73 to 84 of BCB Resolution No. 520/2025, apply in full. The technology supporting custody is contracted from a technology service provider, in accordance with article 9, paragraphs 6 and 7, of the same Resolution, without transfer of custody.

The custody and control of the instruments that affect the exercise of rights related to the virtual asset, such as private keys, constitute the core of the custody activity, in accordance with article 9, item I, of BCB Resolution No. 520/2025. For this reason, this Policy is built on a premise: the Company must be able, at any time, to ensure that only the holder, or whoever the holder authorizes, disposes of the assets, to execute the instructions received in a timely manner and to prevent any unauthorized movement, including when it relies on technology or operational support from third parties or members of its economic group.

This Policy is consistent with and forms part of the Company's Cybersecurity Policy, in accordance with article 49, paragraph 4, of BCB Resolution No. 520/2025, and is part of the set of documents with which the Company demonstrates compliance with the cybersecurity rules required by article 88, item II, subitem "b", of the same Resolution.

This Policy sets out the what and the why. Technical specifications, recovery timeframes, ceremony scripts and operational flows are established in the Private Key Custody and Management Procedure, which details this Policy and is subordinate to it.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

2. Scope

It applies to all private keys and other control instruments, in any format, including full keys, key shares, seed phrases, custody platform credentials, signing devices and administrative roles in smart contracts, relating to wallets under the direct or indirect responsibility of the Company, on all networks and for all virtual assets it holds in custody or operates.

By virtue of article 49, paragraph 1, of BCB Resolution No. 520/2025, the Policy necessarily covers the private keys of virtual assets held on behalf of clients and users. By decision of the Company, it also covers, with the same minimum standard of protection, the keys of proprietary and treasury wallets and those used for liquidity provision, observing the segregation between proprietary and client assets.

It applies to officers, employees, custodians and service providers, including members of the economic group, who generate, safeguard, access, operate or support systems that interact with these instruments, as well as to the physical and logical environments in which they are generated, stored or used.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

3. Terms and Definitions

Term	Definition
Private key	Secret cryptographic data that allows transactions to be signed and thus the virtual assets associated with an address on a distributed ledger network to be disposed of.
Control instruments	Private keys and any other means that affect the exercise of rights related to the virtual asset, such as key shares, seed phrases, signing credentials and devices, approval rules configured on a custody platform, wallet code delegations, such as under the EIP-7702 standard, and administrative roles in smart contracts.
Hot wallet	Virtual asset wallet kept constantly connected to the internet, under article 2, item VI, of BCB Resolution No. 520/2025.
Warm wallet	Virtual asset wallet of an intermediate category between cold and hot wallets, kept connected to the internet with additional layers of security, under article 2, item VII, of BCB Resolution No. 520/2025.
Cold wallet	Virtual asset wallet that is not constantly connected to the internet, under article 2, item V, of BCB Resolution No. 520/2025.
Security module	Protected device or computing environment, such as a hardware security module (HSM) or secure enclave, designed to generate, store and use keys without exposing them in clear text.
Multi-party computation (MPC)	Cryptographic technique in which the key is generated and used in a distributed manner among multiple parties, without the full key ever existing in a single location.
Multi-signature (multisig)	Configuration in which a movement requires the signatures of a minimum number of independent keys, verified by the network itself or by a smart contract.
Secret sharing	Technique, such as Shamir's scheme, that splits a secret into shares, so that only a minimum number of them allows it to be reconstructed.
Quorum (m-of-n)	Minimum number of approvals, signatures or shares (m), out of the total existing (n), required to authorize an operation or to reconstruct a control instrument.
Custodian	Person formally designated to safeguard a share, device or credential and to participate in approvals or key ceremonies.
Key ceremony	Formal, scripted, witnessed and recorded procedure for the generation, backup, recovery, rotation or destruction of control instruments.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

Term	Definition
Compromise	Loss, disclosure of or unauthorized access to a control instrument, a well-founded suspicion of any of these events, or a failure that prevents its legitimate use.
Sweep	Transfer of assets from an existing address to a new address under the Company's control, as a rotation measure or to contain a compromise.

4. General Guidelines

4.1. Principles

The custody and protection of control instruments observe the principles below, which guide the interpretation of this Policy and of the Procedure:

- **Control by the Company:** the Company maintains, permanently and demonstrably, the ability to authorize, execute and prevent movements of the assets held in custody.
- **No single point of failure:** no person, device, location or provider is, on its own, sufficient to move client assets outside the approved signing rules or to change those rules, and the loss of any of them does not prevent the recovery of the assets.
- **Segregation of duties and dual control:** whoever requests does not approve, whoever approves does not execute alone, and whoever operates does not audit.
- **Least privilege:** access is granted strictly to the extent of functional need, for a fixed period when possible, and reviewed periodically.
- **Minimization of exposure:** proprietary and treasury balances held in a connected environment are the smallest compatible with the liquidity necessary for operations.
- **Asset segregation:** client wallets are segregated from proprietary and treasury wallets, and the control instruments of proprietary wallets are incapable of producing any effect on client wallets, in accordance with articles 29, 30 and 78 of BCB Resolution No. 520/2025.
- **Traceability:** every access, approval, signature and ceremony is recorded in a complete and auditable manner.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

4.2. Company control and provider support

The Company may use custody technology, security modules, multi-party computation platforms and operational services contracted from third parties or from members of its economic group, in accordance with the Supplier Management Procedure (KYP). The contracting of a technological mechanism or service for custody is only permitted if the provider attests, in a specific document, that the mechanism or service does not allow it to affect, in any way, the custody and control of the control instruments, the description and reconciliation of positions, the execution of movement instructions and the handling of events affecting the assets, or the exercise of the rights related to them, in accordance with article 9, paragraph 6, of BCB Resolution No. 520/2025. The declaration covers the smart contracts supplied by the provider to which client wallets delegate code.

These mechanisms and services are considered relevant for the purposes of BCB Resolution No. 520/2025 and are subject to the regulation on the contracting of data processing and storage and cloud computing services, in accordance with article 9, paragraph 7, of the same Resolution. The contracts ensure the Company full and timely access to the data, records and evidence necessary for reconciliation, audit, supervision and compliance with court orders, as well as an exit plan that allows the migration of the control instruments without interruption of custody, including through the recovery of the shares from backups under the Company's control.

The contracted support is auxiliary. The quorum configuration ensures that every movement depends on the approval of an authorized person of the Company. Decisions on movements, parameters, exceptions and the response to compromises remain with the Company.

If the Company engages another entity, including a member of the group or an entity incorporated abroad, to provide the custody service itself, and not merely supporting technology, it additionally observes articles 74, 75, 83 and 84 of BCB Resolution No. 520/2025. In that case, the Company continuously assesses and monitors the custodian's custody policy, which must be compatible with this Policy and with the Company's cybersecurity policy and kept in Portuguese at the disposal of the Central Bank of Brazil; receives and assesses its stress tests and its security and AML plans; verifies the conditions of the sole paragraph of article 83, including authorization and supervision in the country of incorporation, the legal representative in Brazil and the guarantees; and ensures clauses on monitoring of positions, access by the Central Bank of Brazil, segregation with full legal effect and specific wallets for clients in Brazil. The Company is liable to clients on the same terms as the contracted custodian, in accordance with articles 73, paragraph 6, item III, and 81, sole paragraph, of the same Resolution.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

5. Architecture and Custody of Control Instruments

5.1. Wallet architecture and distribution of assets

Each client account has its own associated wallet, without the use of a collective (omnibus) wallet. Client wallets are operated through multi-party computation in a connected environment and are classified as hot wallets, under article 2, item VI, of BCB Resolution No. 520/2025. As of this date, the Company does not maintain warm or cold wallets. Any distribution of assets among hot, warm and cold wallets, as referred to in article 49, item II, of the same Resolution, depends on approval by the Board of Executive Officers and on the revision of this Policy and of the custody agreement. The balance of proprietary and treasury wallets held in a connected environment observes the limit. The Company does not hold virtual assets of its own in client wallets, except for the minimum deposits required by the network for the existence of token accounts, which observe article 30, paragraphs 2 to 4, of BCB Resolution No. 520/2025. Network fees for client movements are paid by a fee sponsor wallet owned by the Company, segregated from client wallets and subject to the limits and quorums applicable to treasury wallets and to monitored consumption limits.

Movements of proprietary and treasury wallets depend on quorum approval and are made only to previously registered addresses controlled by the Company. Hot wallets are subject to continuous monitoring and automatic blocking in the face of anomalous movement patterns.

The description of the wallets, the custody methods and the distribution of assets among them forms part of the custody agreement and of the terms of use offered to clients, in accordance with article 73, items III and V, of BCB Resolution No. 520/2025, in terms consistent with this Policy. These documents disclose the risks of each custody method and of each distribution strategy and obtain, in a documented manner, the client's decision or consent, in accordance with paragraph 1 of the same article.

The admission of a new virtual asset or new network depends on a prior assessment, by Custody and Information Security, of the capacity for secure custody of the respective control instruments, within the scope of the Virtual Asset Eligibility Policy.

5.2. Key generation and ceremonies

Control instruments are generated exclusively in a security module or in an approved multi-party computation protocol, in a controlled environment, with a validated entropy source and without exposure of the full key in clear text outside the secure environment. Generation on personal devices, in non-approved environments or with non-approved tools is prohibited.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

The generation of control instruments for proprietary and treasury wallets, as well as their backups, recoveries, rotations and destructions, takes place in a key ceremony, conducted according to an approved script, in the presence of at least two authorized participants and an independent witness to the operation, recorded in minutes and, where appropriate, on video, with validation of the resulting public addresses before use. Client wallets are generated by the custody platform, through an application programming interface, according to approved rules and with each generation recorded.

5.3. Security modules and cryptographic techniques

The Company uses cryptographic techniques compatible with the value held in custody and with the state of the art, documented in the Procedure, in accordance with article 49, item III, of BCB Resolution No. 520/2025. The custody of control instruments is carried out by multi-party computation (MPC), without the use of a hardware security module (HSM). Should the Company adopt HSMs, the modules will have a current validation under the FIPS 140-3 standard, level 3 or higher, or an equivalent recognized certification. Modules whose FIPS 140-2 validation has been moved to the historical list are not adopted in new contracts and are subject to a replacement plan.

The multi-party computation solution adopted, and any multi-signature solution, must offer a security guarantee at least equivalent to that standard, with the protocol and implementation assessed by an independent third party. Firmware, software and configuration updates to the modules follow the change management process, with prior approval and testing.

5.4. Storage, sharding and redundancy

Control instruments are stored according to documented access, storage and protection protocols, using cryptography and other information security techniques, in accordance with article 49, paragraph 2, of BCB Resolution No. 520/2025.

Multiple or sharded keys are stored in different locations, in accordance with article 49, paragraph 3, of BCB Resolution No. 520/2025, in a number and distribution that ensure, at the same time, that no location or custodian alone allows the movement of the assets and that the loss of a location or custodian does not prevent their recovery. Backups of the shares are encrypted with a key under the Company's exclusive control and kept in at least two geographically distinct locations, so as to allow the recovery of the control instruments independently of the provider.

The Company also maintains the redundancy mechanism provided for in article 76, item XII and paragraph 1, of BCB Resolution No. 520/2025, which contains all client data and information and the control instruments over the virtual assets, accompanied by recovery procedures. The mechanism is subject to Brazilian law, administered by an institution or entity

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

incorporated in Brazil, or by a technological repository of the Company itself once authorized, in accordance with paragraph 2 of the same article, accessible to the Central Bank of Brazil and compatible with the cybersecurity policy, including when the main custody infrastructure is operated by a provider abroad. The entity that administers it is considered a relevant engagement, in accordance with paragraph 3 of the same article. When hosted in the cloud abroad, the mechanism observes the conditions of BCB Resolution No. 85/2021 for data processing and storage abroad. The recovery procedure is tested every six months.

Seed phrases, shares and credentials are not recorded in e-mail, messaging applications, general-purpose cloud storage, photographs or any other non-approved medium. Custody maintains an up-to-date inventory of the control instruments, with their location, their custodians and the networks and wallets to which they refer.

6. Access and Transaction Authorization

6.1. Granting, approval authorities and deactivation of access

Access to control instruments and custody systems is granted formally, according to rules and approval authorities compatible with the level of access and with the limits of responsibility of each role, in accordance with article 49, items IV and VI, and article 48, items I and IV, of BCB Resolution No. 520/2025. Access requires multi-factor authentication with a physical device and is preceded, for custodians and for roles with access to control instruments, by a background check justified by the nature of the role, based on article 7, item IX, of Law No. 13,709/2018, according to criteria defined in the Know Your Employee (KYE) Procedure, and by the signing of a specific confidentiality agreement.

Access rights are reviewed every six months by an area other than the one that granted them, and revoked immediately in the event of termination, change of role or suspected compromise. The termination or replacement of a custodian triggers the reissuance or redistribution of the shares under their custody or, when the custodian holds only approval credentials, the revocation of those credentials, so that the former custodian retains no ability to contribute to the quorum.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

6.2. Transaction authorization and signing

Every movement of client assets takes place only upon instruction from the holder, or from whoever the holder authorizes, or, regardless of instruction, in cases of movement between wallets controlled by the Company without change in the ownership of the assets, compliance with a court order or a demand from a competent authority, and transfer provided for in the asset segregation policy in the event of interruption or discontinuation of services, and is authorized according to signing rules configured in the custody system, which apply limits, approval authorities, quorums, execution windows and address lists. Movements of proprietary and treasury wallets and changes to signing rules, permissions and address lists on the custody platform require the approval of at least two authorized persons other than the requester. Code delegation in client wallets, such as under the EIP-7702 standard, is restricted to contracts previously approved by Custody and Information Security, and any change to it depends on the quorum.

The signing system is integrated with the AML, sanctions and fraud prevention controls. No transaction is signed before the screening of the origin and destination addresses, in accordance with the Sanctions and Asset Freezing Policy, and the application of the limits and temporary blocks referred to in article 43, paragraph 2, item VI, of BCB Resolution No. 520/2025 and, as from January 1, 2027, of the precautionary hold provided for in BCB Resolution No. 584/2026. Transfers to or from self-hosted wallets that reach the Coaf reporting threshold provided for in article 49 of BCB Circular No. 3,978/2020, as amended by BCB Resolution No. 591/2026, are identified in the signing flow and forwarded to the AML function, and originator and beneficiary information is handled in accordance with the applicable regulation.

7. Life Cycle, Reconciliation and Orders from Authorities

7.1. Rotation, reissuance and destruction

Custody platform access credentials and service account keys have validity periods defined based on the recommendations of NIST SP 800-57. Control instruments generated by multi-party computation have no fixed validity period and are rotated, with a sweep of the assets to new addresses, upon suspected compromise, upon the termination of a custodian whose participation cannot be neutralized by redistribution, upon the replacement of a security module or provider, and whenever the risk assessment so recommends.

Control instruments are destroyed only after confirmation of a zero balance and of the absence of pending operations at the associated addresses, in a ceremony, by a method that prevents their recovery, with a record in minutes.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

7.2. Reconciliation and demonstration of control

The Company reconciles, daily and through an area other than the one that executes the movements, the recorded positions of each client with the balances of the addresses on the respective networks, obtained from a source independent of the custody technology provider, in accordance with article 9, item II, and article 76, item III, of BCB Resolution No. 520/2025, and treats discrepancies as incidents. Custody maintains the ability to demonstrate, by verifiable cryptographic means, control of the addresses that the Company declares it holds, for the purposes of audit and proof of reserves, according to the methods defined in the asset segregation policy referred to in article 30, item II, of the same Resolution, and of providing information to the Central Bank of Brazil, including that provided for in article 88, item III, of BCB Resolution No. 520/2025, as amended by BCB Resolution No. 589/2026, and, where applicable, in BCB Normative Instruction No. 713/2026.

7.3. Court orders and asset freezing measures

The Company does not adopt control instruments or custody mechanisms that impose obstacles to the performance of its duties under the custody agreement or to the immediate compliance with court orders or demands from competent authorities applicable to the assets held in custody, in accordance with article 73, paragraph 3, of BCB Resolution No. 520/2025, or to the immediate compliance with asset freezing measures. The Procedure provides for a specific process for executing blocks and transfers ordered by a competent authority, with quorums and custodians available within a timeframe compatible with that set in the order, in accordance with the Sanctions and Asset Freezing Policy.

8. Monitoring, Incidents and People

8.1. Monitoring, records and testing

The Company maintains continuous monitoring of the security of the custody and risk assessment environments, with threat detection and response, in accordance with articles 48, item II, and 50 of BCB Resolution No. 520/2025. Records of generation, access, approval, signing, ceremonies and configuration changes are immutable, time-synchronized and kept for at least five years, or for the longer period required by anti-money laundering and counter-terrorist financing regulation.

The systems, programs and smart contracts used in custody are subject to vulnerability analyses, review by independent analysts and robustness and security testing, in accordance with article 48, item VIII, of BCB Resolution No. 520/2025, including an annual penetration test. Backup and recovery procedures are tested every six months, with verification of the integrity of the shares, and the results are reported to the Board of Executive Officers.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

The Company carries out, at least annually, stress tests to assess the ability of its systems to ensure the security of the assets held in custody, with the method and results documented and kept for at least five years, in accordance with article 82 of BCB Resolution No. 520/2025, and may engage an entity of recognized technical capacity for this purpose.

8.2. Response to compromise and continuity

The Company maintains a control instrument compromise response plan, integrated into the Incident Action and Response Plan provided for in the Cybersecurity Policy, in accordance with article 49, item V, of BCB Resolution No. 520/2025. In the event of a compromise or well-founded suspicion thereof, the Company immediately suspends the use of the affected instruments, assesses the exposure and, where necessary, carries out an emergency sweep of the assets to unaffected wallets.

The business continuity plan, together with the Plan for the Recovery of Positions and Control of Virtual Assets and Client Funds, sets the estimated timeframes for the resumption and recovery of custody and for communication actions, in accordance with article 43, paragraph 4, of BCB Resolution No. 520/2025. Incidents are recorded and reported to the Central Bank of Brazil, to affected clients and to the other competent authorities in accordance with cybersecurity and personal data protection regulation, and to Coaf when there is an indication of money laundering or of the financing of terrorism or proliferation.

8.3. People, training and confidentiality

Employees and custodians with access to control instruments receive specific training, at least annually, within the training program of the Know Your Employee (KYE) Procedure, in accordance with article 43, paragraph 2, item II, and article 48, items V and VII, of BCB Resolution No. 520/2025, sign a specific confidentiality agreement and are subject to background checks upon hiring and periodically, in accordance with item 6.1 and the Know Your Employee (KYE) Procedure. Critical functions are distributed so as to avoid conflicts of interest and concentration of knowledge, with designated and trained substitutes.

8.4. Prohibitions

- Generating, storing or using a control instrument outside an approved environment and tool.
- Recording a seed phrase, share or credential in a non-approved medium, including e-mail, messaging applications, general-purpose cloud storage or photographs.
- Allowing a single person, location, device or provider to be sufficient to move client assets outside the approved signing rules or to change those rules.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

- Allowing a provider, even one belonging to the group, to reach the movement quorum or to change signing and authentication rules without the approval of an authorized person of the Company.
- Sharing credentials or authentication devices, or concentrating in the same person the functions of requesting, approving and executing a movement.
- Signing a transaction before the completion of screening and the other applicable AML, sanctions and fraud prevention controls.
- Holding a balance in a proprietary or treasury wallet above the approved limit, except for a documented and temporary exception.
- Maintaining a custody or control mechanism that prevents or delays compliance with an authentic court order, a demand from a competent authority or an asset freezing measure.
- Contracting, adopting or using a mechanism that hinders the work of the authorities or the detection of crimes, such as mixers or tumblers, in accordance with article 90 of BCB Resolution No. 520/2025.
- Destroying a control instrument without confirmation of a zero balance and without a recorded ceremony.

9. Review

This Policy is reviewed annually, and on an extraordinary basis upon relevant changes in the regulation of the Central Bank of Brazil, in the custody architecture, in the security modules or in the contracted providers, in the networks and assets held in custody, after a compromise incident or upon an audit or supervisory finding, with approval by the Board of Executive Officers, formalized in minutes, following prior deliberation by the Compliance Committee.

10. Reference Standards

- Law No. 14,478 of December 21, 2022, and Decree No. 11,563 of June 13, 2023.
- BCB Resolution No. 520 of November 10, 2025, in particular articles 9, 29, 30, 43, 48 to 50, 73 to 84 and 90, and article 88, as amended by BCB Resolution No. 589/2026.
- BCB Resolution No. 85 of April 8, 2021 (cybersecurity and contracting of data processing and storage and cloud computing services), BCB Resolution No. 260/2022 (internal controls) and BCB Resolution No. 93/2021 (internal audit), applicable by virtue of BCB Resolution No. 552/2026.

	Private Key Custody And Protection Policy	SEG-POL-011-FIN
Publication Date: 10/15/2026	Information Security	Public

- BCB Circular No. 3,978 of January 23, 2020, as amended by BCB Resolution No. 591/2026, and BCB Resolution No. 584/2026 (fraud prevention).
- Law No. 13,810 of March 8, 2019 (enforcement of United Nations Security Council sanctions and asset freezing).
- BCB Resolution No. 44 of November 24, 2020 (procedures for the execution, by institutions authorized to operate by the Central Bank of Brazil, of the measures determined by Law No. 13,810/2019).
- BCB Normative Instruction No. 713/2026, where applicable.
- CMN Resolution No. 5,280/2026 (banking secrecy) and Law No. 13,709 of August 14, 2018 (General Personal Data Protection Law).

11. Effectiveness

This Policy is permanent in nature and enters into force on the date of its approval by the Board of Executive Officers, formalized in minutes, following prior deliberation by the Compliance Committee. Its content may be modified at any time according to current needs. The Company's employees and service providers must always consult the latest available version.

12. Version Control and History

Version	Date	Change/Addition History	Approved by
1.0	10/15/2026	Initial issue	Board of Executive Officers, following deliberation by the Compliance Committee