# Cybersecurity Policy

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

## Contents


**1. Purpose** **3**

**2. Scope** **3**

**3. Terms and Definitions** **5**

**4. Cybersecurity Objectives** **6**

**5. Minimum Procedures and Controls** **6**

5.1. Authentication and access controls 7

5.2. Cryptography, certificates and keys 7

5.3. Network protection and secure configuration 7

5.4. Prevention and detection of intrusion, malicious software and data leakage 8

5.5. Traceability 8

5.6. Backups 8

5.7. Vulnerability management and penetration testing 8

5.8. Security in development and in the adoption of new technologies 9

5.9. Integration through electronic interfaces 9

5.10. Cyber threat intelligence 9

**6. Security Measures Specific to the Activity** **10**

6.1. Computing environment 10

6.2. Custody and protection of virtual asset control instruments 10

6.3. Institutional security 11

**7. Data Classification and Incident Relevance** **11**

7.1. Classification of data and information 11

7.2. Incident relevance parameters 11

**8. Incident Action and Response Plan** **12**

**9. Contracting of Data Processing, Data Storage and Cloud Computing Services** **12**

**10. Relevant Services** **13**

10.1. Relevance criterion 13

10.2. Register of relevant services 13

10.3. Cloud computing modalities 14

**11. Pre-Contracting Procedures 14**

11.1. Proportionate governance 14

11.2. Verification of the provider's capacity 14

11.3. Documentation 15

11.4. Internal competencies 15

**12. Contracting Abroad 15**

12.1. Requirements 15

12.2. Absence of a cooperation agreement 16

12.3. Change of countries and regions 16

**13. Mandatory Contractual Clauses 16**

13.1. General clauses 16

13.2. Resolution regime 17

13.3. Supervisor access and information to clients 18

**14. Communication to the Central Bank of Brazil 18**

**15. Subcontracting 18**

**16. Monitoring, Continuity and Termination 19**

16.1. Continuous monitoring 19

16.2. Continuity and replacement 19

16.3. Termination and return of data 19

**17. Recovery of Positions and the National Financial System Network 19**

**18. Prohibitions 20**

**19. Business Continuity at the Cyber Interface 20**

19.1. Guidelines 20

19.2. Timeframes 21

19.3. Crisis situation and communication to the Central Bank of Brazil 21

**20. Disclosure and Security Culture 21**

**21. Monitoring, Effectiveness and Annual Report 22**

21.1. Mechanisms 22

21.2. Internal audit 22

21.3. Annual report 22

21.4. Exceptions 22

**22. Review** **23**

**23. Reference Standards** **23**

**24. Effectiveness** **23**

**25. Version Control and History** **23**


# 1. Purpose

This Policy sets out the cybersecurity principles, guidelines, procedures and controls of Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. (the PSAV company), referred to in this document as the Organization, with the aim of ensuring the confidentiality, integrity and availability of the data and information systems used in the provision of virtual asset services.

The Organization provides services that involve the custody and movement of third parties' virtual asset control instruments, through wallet infrastructure contracted from a specialized provider, under its responsibility and governance. In this context, the compromise of a single cryptographic signing mechanism causes a direct, immediate and, as a rule, irreversible loss to the client. Cybersecurity is not a support function here: it is a condition for carrying out the activity.

It is grounded in BCB Resolution No. 85 of April 8, 2021, the scope of which was extended to virtual asset service provider companies by BCB Resolution No. 552 of March 3, 2026, and in articles 14, 32 to 43, 45, 48, 49, 50 and 51 of BCB Resolution No. 520 of November 10, 2025.

This Policy incorporates, in Sections 9 to 18 (the "Cloud Chapter"), the policy on the contracting of data processing and storage and cloud computing services required by Chapter III of BCB Resolution No. 85/2021, previously addressed in a separate document, so that a single instrument meets both regulatory requirements.

# 2. Scope

This Policy applies to all data, information systems, technology assets, networks, cloud environments and cryptographic instruments under the Organization's responsibility, whether its own or operated by third parties on its behalf, and to all officers, employees, interns, service providers and other related parties who access them.

It also applies to relevant services contracted from third parties, in accordance with article 33 of BCB Resolution No. 520/2025, in which case responsibility for compliance with this Policy remains entirely with the Organization, under articles 36 and 51 of the same Resolution.

The Organization is not part of a prudential conglomerate. Therefore, the option of adopting a single cybersecurity policy provided for in article 2, paragraph 2, of BCB Resolution No. 85/2021 does not apply to it. Technical standards of other group companies may be adopted as a reference, but do not replace this Policy or its approval by the Organization's management body.

# 3. Terms and Definitions

| Term | Definition |
|---|---|
| Senior Management | The Organization's Board of Executive Officers. |
| Incident | Event that compromises or may compromise the confidentiality, integrity or availability of the Organization's data or information systems. |
| Relevant incident | Incident that meets at least one of the parameters of Section 7.2, requiring recording, cause and impact analysis, control of effects and the applicable communications. |
| Sensitive information | Data or information classified as Restricted or Confidential under Section 7.1, including personal data, information subject to secrecy and virtual asset control instruments. |
| Virtual asset control instrument | Cryptographic signing mechanism that authenticates virtual asset transactions, notably the private key, under article 2, VIII, of BCB Resolution No. 520/2025. |
| Relevant service | Service whose failure affects the performance of the Organization's activities or the full exercise of the rights of a client or user, under article 33 of BCB Resolution No. 520/2025, including technology services related to the provision of virtual asset services. |
| Cloud computing | Availability to the Organization, on demand and virtually, of computing resources for deploying or running software; of resources for running its own applications; or of the provider's own applications run over the internet, under article 13 of BCB Resolution No. 85/2021. |
| Cooperation agreement | Agreement for the exchange of information between the Central Bank of Brazil and the supervisory authority of the country where the service is provided, required by article 16, I, of BCB Resolution No. 85/2021. |
| Contracting file | Set of documents that brings together the prior due diligence, the contract, the communications to the Central Bank of Brazil and the monitoring records of each relevant service provider. |
| Provider | Institution or entity engaged to provide a relevant service, in Brazil or abroad. |
| Subcontracting | Engagement, by the provider, of a third party to perform part of the relevant service provided to the Organization. |
| Crisis situation | Relevant incident or interruption of a relevant service that meets the criteria of Section 19.3, requiring timely communication to the Central Bank of Brazil. |

| Term | Definition |
|---|---|
| Penetration test | Controlled vulnerability exploitation exercise, carried out with independence and impartiality, under article 22-A of BCB Resolution No. 85/2021. |

# 4. Cybersecurity Objectives

The Organization's cybersecurity objectives, under article 3, I and paragraph 1, of BCB Resolution No. 85/2021, are to:

- prevent incidents, through controls proportionate to the Organization's size, risk profile and business model, the nature of its activities and the sensitivity of the data under its responsibility;
- detect incidents and atypical behavior in a timely manner, through continuous monitoring and traceability of processing;
- reduce the Organization's vulnerability to incidents related to the cyber environment, through a permanent vulnerability assessment and remediation program;
- respond to incidents in a structured manner, preserving the integrity of clients' and users' virtual assets and financial resources and the continuity of critical business processes; and
- ensure that the compromise of any single component is not sufficient to allow the unauthorized movement of clients' and users' virtual assets.

The last objective is specific to the Organization's activity and prevails, in the event of conflicting priorities in incident response, over availability objectives.

# 5. Minimum Procedures and Controls

The procedures and controls adopted to reduce the Organization's vulnerability to incidents cover, at a minimum, the families listed in article 3, paragraph 2, of BCB Resolution No. 85/2021, detailed in this Section. They also apply to the development of secure information systems and to the adoption of new technologies, under article 3, paragraph 3, and extend, where applicable, to systems acquired or developed by third parties and run on the Organization's computing resources.

## 5.1. Authentication and access controls

Access to the corporate network is limited to credentialed users and authorized devices. Access from environments external to the Organization requires multi-factor authentication, without exception.

Access permissions are reviewed periodically and in a timely manner, with specific attention to outsourced personnel who access the Organization's computing resources. The review takes place at least every six months for privileged access and critical systems and annually for the others, in accordance with the Access Management Standard, and is recorded with the date, responsible person and result.

The granting of authorizations, the creation of passwords and access controls observe approval authorities compatible with the responsibilities of each role and are subject to a preventive deactivation mechanism in suspicious situations, under article 48, IV, of BCB Resolution No. 520/2025.

## 5.2. Cryptography, certificates and keys

The Organization uses cryptography in the transmission and storage of sensitive information, in accordance with the algorithms and parameters defined in the Cryptography and Key Management Policy and in the Cryptography Technical Standard.

Digital certificate management comprises monitoring the use of certificates and digital signatures with the traceability mechanisms of Section 5.5; safekeeping procedures, with physical and logical access control to the private keys under the Organization's responsibility; measures to prevent the improper sharing of such keys; and timely validation of revoked certificates with the certification authorities.

The private keys of clients' and users' virtual assets are additionally, and with precedence, subject to the regime of Section 6.2.

## 5.3. Network protection and secure configuration

The network is segmented so as to protect the production environment and the computing resources that support critical business processes. Firewall rules and connection monitoring are maintained, along with defined criteria for establishing and monitoring connections with external environments, with reinforced attention at night and on non-business days, and measures to identify and prevent improper connections originating from the Organization's technology resources, in accordance with the Secure Configuration and Network Security Standard.

Processes and tools are maintained for the identification, analysis, handling and control of atypical events in the production environment, including the establishment of virtual private networks and privileged access attempts.

Technology assets follow secure configuration profiles, defined in the Secure Configuration and Network Security Standard, which provide for the life cycle management of computing resources, the regular application of security patches, the proper configuration of supported services and the changing of passwords and other factory defaults.

## 5.4. Prevention and detection of intrusion, malicious software and data leakage

The Organization maintains intrusion prevention and detection, malware protection and data leakage prevention mechanisms, covering production environments, cloud environments and corporate workstations, with recorded handling of the events identified, in accordance with the Event Logging and Monitoring Standard.

## 5.5. Traceability

Traceability covers transactions and operations and includes, at a minimum, audit trails of the end-to-end processing of data and information, including the definition and generation of logs that make it possible to identify processing failures or atypical behavior and to support analyses; the definition of retention periods according to the type of processing performed; and the secure retention of audit trails, in accordance with the Event Logging and Monitoring Standard.

The movement trail of clients' and users' virtual assets is retained for no less than five years, in compliance with article 45, II, of BCB Resolution No. 520/2025.

## 5.6. Backups

Backups of data and information follow the frequency, retention and storage location defined in the Backup Policy and in the Backup Restoration Testing Process, and are subject to restoration tests at least every six months. The result of each test is recorded, and a restoration failure is treated as a relevant incident.

## 5.7. Vulnerability management and penetration testing

The vulnerability management program comprises periodic tests and analyses to detect vulnerabilities in information systems; periodic scans of technology resources to identify devices improperly connected to the corporate network; periodic analyses of technology resources; penetration tests; and the timely remediation of the vulnerabilities identified.

Penetration tests are carried out at least annually, with independence and impartiality, by an individual or specialized firm engaged specifically for this purpose, without prejudice to tests performed by the Organization's own teams. The results are documented, identifying the vulnerabilities and the action plans established for their remediation.

**Prohibition on accumulation.** The provider engaged to design or implement the controls of this Policy may not be the same provider engaged to perform the penetration test referred to above, as this would compromise the independence and impartiality required by article 22-A of BCB Resolution No. 85/2021.

## 5.8. Security in development and in the adoption of new technologies

The systems development cycle includes security verification stages before promotion to the production environment. The adoption of a new technology is preceded by a documented security assessment, and the same verification applies, where applicable, to systems acquired or developed by third parties and run on the Organization's computing resources.

Smart contracts that affect the performance of the Organization's activities are subject to vulnerability analysis, performance review by independent analysts and robustness and security testing, under article 48, VIII, of BCB Resolution No. 520/2025, before their use and upon each relevant change.

## 5.9. Integration through electronic interfaces

The integration of information systems through electronic interfaces observes security requirements defined in the Secure Configuration and Network Security Standard, applicable to authentication, authorization, rate limiting, logging and error handling. An inventory of integrations is maintained, indicating the controls applied to each interface.

## 5.10. Cyber threat intelligence

The Organization maintains cyber threat intelligence activities, including monitoring of information of interest to it on the internet, the Deep Web and the Dark Web and in private communication groups, with specific attention to the exposure of credentials, wallet addresses and the Organization's brand. Findings are handled and, where appropriate, classified as an incident under Section 7.2.

# 6. Security Measures Specific to the Activity

## 6.1. Computing environment

The measures and procedures intended to ensure the security, resilience and proper functioning of the computing environment that supports the provision of virtual asset services, required by article 48 of BCB Resolution No. 520/2025, form part of this Policy and observe Sections 5.1 to 5.10.

Specific preventive measures are adopted to mitigate cyber incidents in transactions involving operators in the decentralized finance segment, including a prior assessment of the protocol, of the smart contracts involved and of the network's history of compromise.

## 6.2. Custody and protection of virtual asset control instruments

The generation, custody and management of the control instruments of clients' and users' virtual assets follow documented procedures, specifying the methods and techniques used in the execution of transactions, under article 49 of BCB Resolution No. 520/2025.

The infrastructure for generating, safeguarding and using the keys of clients' and users' virtual assets is contracted from a specialized relevant service provider, subject to the Cloud Chapter (Sections 9 to 18). Signing policies, approval authorities, quorum and the granting and deactivation of control instruments remain under the Organization's definition and governance, and responsibility before clients, users and the Central Bank of Brazil is not transferred to the provider.

Clients' and users' virtual assets are held in wallets segregated from the Organization's own assets, with individualized identification and periodic reconciliation between internal records and on-chain balances, in accordance with BCB Resolution No. 520/2025.

The procedures for the generation, safeguarding, access, transaction authorization, rotation and destruction of control instruments, the wallet architecture and the distribution of assets among wallets, quorums and compromise mitigation measures are set out in the Private Key Custody and Protection Policy, which forms part of this Policy under article 49, paragraph 4, of BCB Resolution No. 520/2025.

Where multiple or sharded private keys are adopted, the shares are stored in different locations. No individual, alone, has the ability to move clients' and users' virtual assets.

Each exercise of signing power is recorded with the date, time, reason, participating holders and quorum observed, and the corresponding trail is retained in accordance with Section 5.5.

### 6.3. Institutional security

The Organization maintains continuous monitoring of institutional security and risk assessment mechanisms, with the aim of detecting, preventing and responding to threats and incidents, under article 50 of BCB Resolution No. 520/2025. Institutional security comprises, in addition to the cyber environment, the physical security of facilities and personnel, and is the subject of a separate policy with which this Policy is aligned (Physical Security Policy).

## 7. Data Classification and Incident Relevance

### 7.1. Classification of data and information

Data and information are classified by relevance into the categories Public, Internal Use, Confidential and Restricted, in accordance with the Information Management Standard. The classification determines the applicable access, transmission, storage and disposal controls and guides the assessment of the relevance of the services to be contracted, under article 12, paragraph 1, of BCB Resolution No. 85/2021.

Virtual asset control instruments are classified, in all cases, as Restricted; data subject to secrecy is classified, at a minimum, as Confidential, in accordance with the Information Management Standard.

### 7.2. Incident relevance parameters

An incident is relevant if it meets at least one of the following parameters:

- actual or potential compromise of a virtual asset control instrument, regardless of the amount involved;
- unauthorized access to, exfiltration or alteration of information classified as Restricted or Confidential;
- unavailability of a critical business process for a period longer than the timeframe set for its resumption (RTO), approved in accordance with the Business Continuity Policy;
- movement of a client's or user's virtual asset or financial resource without a valid instruction;
- compromise of a relevant service provider with an effect on the Organization's data, assets or services; and
- any event requiring communication to an authority, client or user by force of law or regulation.

A relevant incident is recorded, its cause and impact are analyzed and its effects are controlled, including information received from companies providing services to third parties,

under article 3, IV and paragraph 4, of BCB Resolution No. 85/2021.

# 8. Incident Action and Response Plan

The implementation of this Policy is operationalized by the Incident Action and Response Plan, a separate document approved by the Board of Executive Officers, formalized in minutes, following prior deliberation by the Compliance Committee, which covers, at a minimum, the actions intended to adapt the Organization's organizational and operational structures to the principles and guidelines of this Policy; the routines, procedures, controls and technologies to be used in incident prevention and response; and the area responsible for recording and controlling the effects of relevant incidents.

The Plan includes response playbooks by type of incident and is compatible with the plans for the recovery of positions and control of clients' and users' virtual assets and financial resources required by article 34, II, of BCB Resolution No. 520/2025.

# 9. Contracting of Data Processing, Data Storage and Cloud Computing Services

Companies providing services to third parties that handle sensitive data or information, or that are relevant to the conduct of the Organization's operational activities, observe incident prevention and handling procedures and controls at levels of complexity, scope and precision compatible with those used by the Organization itself.

Sections 9 to 18 set out the criteria, procedures and contractual conditions that the Organization observes when contracting relevant data processing and storage and cloud computing services, in Brazil or abroad, based on Chapter III and article 22-B of BCB Resolution No. 85/2021 and on articles 32 to 42 and 51 of BCB Resolution No. 520/2025.

The Organization operates on third-party infrastructure. The regulatory consequence is that a substantial part of its controls is exercised through contracts rather than through its own configuration. A missing or poorly drafted clause is, here, a control deficiency and not a commercial matter.

The Organization's responsibility for the reliability, integrity, availability, security and confidentiality of the contracted services, as well as for compliance with legislation and regulation, is not transferred to the contractor under any circumstances.

The Cloud Chapter applies to the contracting, amendment, monitoring and termination of contracts for relevant data processing and storage and cloud computing services, entered into in Brazil or abroad, with providers whether or not they belong to the Organization's

economic group.

The contracting of a relevant service from a group company does not waive any requirement of this Chapter. The intragroup contract observes the same mandatory clauses of Section 13 and the same prior due diligence of Section 11.

The Chapter does not apply to the contracting of systems operated by clearing houses, by clearing and settlement service providers or by entities that perform registration or central depository activities, under article 18 of BCB Resolution No. 85/2021.

Suppliers that do not qualify as relevant service providers observe the Supplier Security Standard.

# 10. Relevant Services

## 10.1. Relevance criterion

A service is relevant if it affects the performance of the Organization's activities or affects, or may affect, the full exercise of the rights of a client or user. In assessing relevance, the criticality of the service and the sensitivity of the data and information to be processed, stored and managed by the contractor are considered, taking into account the data classification of Section 7.1 of this Policy.

Relevant services include, among others, wallet infrastructure and virtual asset custody services; liquidity provision for transactions in the virtual asset market; market making; issuance of electronic money and provision of payment or deposit accounts; and technology services specifically related to the provision of virtual asset services.

The technology services referred to above are also considered relevant for the purposes of the regulation on the contracting of data processing and storage and cloud computing services, under article 33, paragraph 2, of BCB Resolution No. 520/2025. The qualification is not discretionary: once the criteria are met, the service is fully subject to this Policy.

## 10.2. Register of relevant services

The Organization maintains a named and versioned register of contracts qualified as relevant, indicating the provider, the purpose, the applicable cloud computing modality under Section 10.3, the countries and regions of processing and storage, the date of communication to the Central Bank of Brazil and the existence of notified subcontracting.

The current register is kept as a record of this Policy, in Compliance's regulatory evidence index, and does not form part of the text of this Policy.

The register is maintained by Compliance, with the support of Information Security and Technology, and updated upon each contracting, amendment or termination. Operating a relevant service not included in the register is a reportable event.

### 10.3. Cloud computing modalities

Each contract is classified into one of the following modalities: provision of data processing, data storage, network infrastructure and other computing resources that allow the Organization to deploy or run software; deployment or execution of applications developed or acquired by the Organization on the provider's computing resources; or execution, over the internet, of applications deployed or developed by the provider on its own computing resources.

In the third modality, the Organization ensures that the provider adopts controls that mitigate the effects of any vulnerabilities when releasing new versions of the application.

## 11. Pre-Contracting Procedures

### 11.1. Proportionate governance

The contracting of a relevant service is preceded by the adoption of corporate governance and management practices proportionate to the relevance of the service to be contracted and to the risks to which the Organization is exposed. Outsourcing decision criteria form part of the Organization's risk management policies, strategies and structures and expressly cover the contracting of data processing and storage and cloud computing services, in Brazil and abroad.

### 11.2. Verification of the provider's capacity

Before contracting, the Organization verifies the potential provider's capacity to ensure:

- compliance with the legislation and regulation in force;
- the Organization's access to the data and information to be processed or stored;
- the confidentiality, integrity, availability and recovery of the data and information processed or stored;
- its adherence to the certifications required by the Organization for the provision of the service;
- the Organization's access to the reports prepared by an independent specialized audit firm engaged by the provider, relating to the procedures and controls used in providing the services;

- the provision of information and management resources appropriate for monitoring the services;
- the identification and segregation of the data of the Organization's clients and end users through physical or logical controls; and
- the quality of the access controls aimed at protecting the data and information of clients and end users.

The verification additionally covers the provider's technical and operational capacity and its regulatory compliance history, under article 34, I, of BCB Resolution No. 520/2025, and the establishment, jointly with the provider, of internal controls that allow the monitoring and identification of sanctions lists and of sanctioned virtual asset wallet addresses, in Brazil or abroad.

### 11.3. Documentation

The procedures of this Section, including the information relating to the verification under Section 11.2, are documented and gathered in the provider's contracting file, which remains at the disposal of the Central Bank of Brazil.

### 11.4. Internal competencies

The Organization maintains the resources and competencies necessary for the proper management of the contracted services, including for analyzing the information and using the monitoring resources provided by the provider. The lack of internal competence to interpret the reports and management resources made available is equivalent, for the purposes of this Policy, to the absence of monitoring.

## 12. Contracting Abroad

### 12.1. Requirements

The contracting of relevant services provided abroad requires the existence of a cooperation agreement for the exchange of information between the Central Bank of Brazil and the supervisory authorities of the countries where the services may be provided; assurance that the provision will not harm the regular functioning of the Organization or hinder the work of the Central Bank of Brazil; prior definition of the countries, and the regions in each country, where the services may be provided and the data may be stored, processed and managed; and provision for business continuity alternatives in the event that the contract cannot be maintained or is terminated.

The Organization ensures that the legislation and regulation of the countries and regions indicated do not restrict or prevent access by the Organization and by the Central Bank of Brazil to the data and information. Evidence of compliance with these requirements is documented.

The existence of a cooperation agreement and compliance with the other requirements of this Section for each jurisdiction included in the register of relevant services are verified and documented in each provider's contracting file, before the filing of the authorization request and upon each change of provider, service or region.

### 12.2. Absence of a cooperation agreement

In the absence of a cooperation agreement, the contracting depends on prior authorization from the Central Bank of Brazil, requested at least sixty days before the intended contracting date. The same minimum period applies to contractual amendments that change the name of the contractor, the relevant services contracted or the countries and regions indicated.

**Effect on the timeline.** The sixty-day period precedes the contracting, not the other way round. Every relevant engagement in a jurisdiction without a cooperation agreement, including the migration of an existing contract to a new region, must be identified in planning sufficiently in advance. The jurisdiction mapping of Section 10.2 is therefore a condition for the feasibility of this Policy, and not an ancillary document.

### 12.3. Change of countries and regions

A change in the countries or regions of data processing, storage and management, even if made unilaterally by the provider, is subject to the requirements of this Section. The contract provides for the provider's obligation to give prior notice of the change, within a timeframe compatible with the Organization's compliance with regulatory requirements.

## 13. Mandatory Contractual Clauses

### 13.1. General clauses

Contracts for the provision of relevant data processing, data storage and cloud computing services contain clauses providing for:

- the indication of the countries, and the region in each country, where the services may be provided and the data may be stored, processed and managed;
- the adoption of security measures for the transmission and storage of such data;
- the maintenance, while the contract is in force, of data segregation and access controls to protect the information of clients and end users;

- the obligation, upon termination of the contract, to transfer the data to the new provider or to the Organization and to delete the data by the replaced contractor, after the transfer and confirmation of the integrity and availability of the data received;
- the Organization's access to the information provided by the provider to verify compliance with the preceding items, to information on certifications and specialized audit reports, and to information and management resources appropriate for monitoring the services;
- the provider's obligation to notify the Organization of the subcontracting of relevant services;
- permission for the Central Bank of Brazil to access the contracts and agreements entered into, the documentation and information on the services provided, the data stored and information on its processing, backups of data and information, and access codes;
- the adoption of measures by the Organization as a result of a determination by the Central Bank of Brazil; and
- the provider's obligation to keep the Organization permanently informed of any limitations that may affect the provision of the services or compliance with the legislation and regulation in force.

Contracts also provide that the provider acts on behalf of and under the guidelines of the Organization, and that the Organization remains responsible for the services provided to clients, users and other institutions in the virtual asset market through the contracted entity.

## 13.2. Resolution regime

In the event that the Central Bank of Brazil places the Organization under a resolution regime, contracts provide for the provider's obligation to grant the person responsible for the resolution regime full and unrestricted access to the contracts, agreements, documentation and information on the services provided, the data stored and information on its processing, backups and access codes in its possession.

They also provide for the obligation to give the person responsible for the resolution regime prior notice of the intention to interrupt the provision of services, at least thirty days in advance, the provider undertaking to accept any request for an additional thirty-day period made by that person, including when the interruption is due to the Organization's default.

### 13.3. Supervisor access and information to clients

Contracts for the provision of relevant services provide that the provider supplies the information and documents necessary for the Central Bank of Brazil to perform its supervisory duties and allows it access to the documentation, to information on the products and services provided and to its premises, under article 40 of BCB Resolution No. 520/2025.

The Organization provides clients, users and other business counterparties with clear and transparent information on the involvement of other contracted institutions or entities in the provision of relevant services, highlighting the engagements that may represent risks and indicating the forms of mitigation, while safeguarding the confidentiality of confidential information and commercially sensitive data.

## 14. Communication to the Central Bank of Brazil

The contracting of relevant data processing, data storage and cloud computing services is communicated to the Central Bank of Brazil within ten days of contracting, indicating the name of the contracted company, the relevant services contracted and, in the case of contracting abroad, the countries and the regions in each country where the services may be provided and the data stored, processed and managed.

Contractual amendments that change this information are communicated within ten days of the amendment.

Compliance controls the deadlines for the communications of this Section. Failure to meet the deadline is an event reportable to the Board of Executive Officers, regardless of whether the service remains in regular operation.

## 15. Subcontracting

Notice of the subcontracting of relevant services received from the provider is recorded in the contracting file and taken into account in defining the Organization's monitoring and control mechanisms.

Subcontracting does not change the provider's responsibility to the Organization or the Organization's responsibility to its clients, users and the Central Bank of Brazil.

If the subcontracting entails the processing or storage of data in a country or region not indicated in the contract, Section 12.3 applies.

# 16. Monitoring, Continuity and Termination

## 16.1. Continuous monitoring

The Organization continuously verifies the provider's technical and operational capacities and continuously monitors its performance, based on the information and management resources made available, on independent specialized audit reports and on the certifications held.

Monitoring takes place at least annually and, for providers that support the custody of virtual assets or the production environment, every six months, and is recorded with the date, responsible person, information analyzed and conclusion.

## 16.2. Continuity and replacement

For each relevant service, the Organization maintains a continuity alternative that covers the replacement of the provider and the restoration of normal operations, with an estimated resumption timeframe compatible with the timeframes defined in the Business Impact Analysis (BIA), in accordance with the Business Continuity Policy and Section 19 of this Policy.

The interruption of a relevant service is treated as an incident and, where the applicable criteria are met, as a crisis situation, with timely communication to the Central Bank of Brazil.

## 16.3. Termination and return of data

Upon termination of the contract, the Organization ensures the transfer of the data to the new provider or to itself and the deletion of the data by the replaced contractor, after the transfer and confirmation of the integrity and availability of the data received. The confirmation is documented and forms part of the contracting file.

# 17. Recovery of Positions and the National Financial System Network

The Organization prepares and keeps up to date robust plans for the recovery of positions and control of clients' and users' virtual assets and financial resources, applicable to incidents that affect such assets and resources and that involve the contracted institution or entity.

These plans are compatible with the Incident Action and Response Plan and with the other Sections of this Policy, and are subject to testing that includes a scenario of unavailability of a relevant service provider.

The service provided for the electronic communication of data on the National Financial System Network, where applicable to the Organization, is considered relevant for the purposes

of this Policy, regardless of the form of connection, including where the provider supplies message processing services within the National Financial System and the Brazilian Payment System.

# 18. Prohibitions

The Organization is prohibited from:

- starting the operation of a relevant service before the prior due diligence of Section 11 has been completed and the contract has been formalized with the clauses of Section 13;
- contracting a relevant service provided abroad in a jurisdiction without a cooperation agreement without the prior authorization of Section 12.2;
- entering into a relevant service contract that does not contain a clause prohibiting the contracted institution or entity from charging the Organization's clients and users, in the form of fees, commissions or reimbursement amounts, for services rendered in supplying products or services that are the contractor's own responsibility, under article 37 of BCB Resolution No. 520/2025;
- accepting a clause that restricts access by the Organization or by the Central Bank of Brazil to data, information, backups or access codes; and
- maintaining a relevant contract whose termination does not ensure the transfer and subsequent deletion of the data in accordance with Section 16.3.

# 19. Business Continuity at the Cyber Interface

## 19.1. Guidelines

The Business Continuity Policy establishes the method, approval authorities, minimum scenarios and continuity testing program. The Risk Management Policy provides, with regard to business continuity and under articles 19 and 20 of BCB Resolution No. 85/2021, for the handling of relevant incidents; for the procedures to be followed in the event of interruption of contracted relevant data processing and storage and cloud computing services, including scenarios that consider the replacement of the contracted company and the restoration of normal operations; and for the incident scenarios considered in continuity tests.

### 19.2. Timeframes

The Risk Management Policy and its procedures specify the treatment provided to mitigate the effects of relevant incidents and of the interruption of relevant services, and the timeframe set for the resumption or normalization of the interrupted activities or services, in accordance with article 43, paragraph 4, of BCB Resolution No. 520/2025, which also covers the internal and external communication actions necessary to guide the restoration of activities. The timeframes per critical process are set out in the Business Impact Analysis (BIA), an annex to the Business Continuity Policy.

### 19.3. Crisis situation and communication to the Central Bank of Brazil

A crisis situation is a relevant incident or interruption of a relevant service that meets at least one of the following criteria: unavailability of a critical business process for a period longer than the maximum tolerable period of disruption (MTPD) defined in the Business Impact Analysis; compromise of a virtual asset control instrument of a client or user; or inability to restore through the ordinary procedures provided for in the Incident Action and Response Plan.

The Organization promptly informs the Central Bank of Brazil of the occurrence of relevant incidents and of interruptions of relevant services that constitute a crisis situation, as well as of the measures taken to resume activities, in the form and through the channels defined in regulation. The decision to report, or not to report, is reasoned by the responsible Officer and recorded, in accordance with the Incident Action and Response Plan.

## 20. Disclosure and Security Culture

This Policy is disclosed to the Organization's employees and to companies providing services to third parties, in clear and accessible language and at a level of detail compatible with the functions performed and the sensitivity of the information. A summary containing its general outlines is disclosed to the public on the Organization's website.

The dissemination of the cybersecurity culture comprises training and periodic assessment programs for personnel; the provision of information to clients and end users on precautions in using the products and services offered, including recommended security measures and the risks of self-custody; and Senior Management's commitment to the continuous improvement of procedures.

The Organization develops initiatives to share information on relevant incidents with other institutions authorized to operate by the Central Bank of Brazil, without prejudice to the duty of confidentiality and to free competition, including information received from service providers and keeping it available to the Central Bank of Brazil.

# 21. Monitoring, Effectiveness and Annual Report

## 21.1. Mechanisms

The Organization establishes monitoring and control mechanisms to ensure the implementation and effectiveness of this Policy, of the Incident Action and Response Plan and of the requirements for contracting data processing and storage and cloud computing services, including the definition of processes, tests and audit trails; the definition of appropriate metrics and indicators; and the identification and correction of any deficiencies. Notices received on the subcontracting of relevant services are taken into account in defining these mechanisms.

## 21.2. Internal audit

The mechanisms of Section 21.1 are tested annually by internal audit, performed by an independent contracted firm, within the ISMS internal audit program, with the support of Compliance when necessary, and reported to the Compliance Committee.

## 21.3. Annual report

An annual report on the implementation of the Incident Action and Response Plan is prepared, with a base date of December 31, addressing, at a minimum, the effectiveness of the implementation of the adaptation actions; a summary of the results obtained in implementing the prevention and response routines, procedures, controls and technologies; the relevant incidents that occurred in the period; the results of business continuity tests, considering unavailability scenarios caused by incidents; and the results of penetration tests and of periodic vulnerability scans and analyses, with the action plans established for their remediation.

The report is submitted to the Compliance Committee and presented to the Board of Executive Officers by March 31 of the year following the base date.

## 21.4. Exceptions

Exceptions to this Policy are recorded, assessed for residual risk by Information Security and approved under the single exception approval authority of the Information Security Policy, with a defined deadline, compensating controls and responsible person. No exceptions are permitted to the controls of Section 6.2 or to the requirement of multi-factor authentication for access from external environments.

## 22. Review

This Policy and the Incident Action and Response Plan are documented and reviewed at least annually, and on an extraordinary basis upon a regulatory change, a relevant incident, including one involving a provider, the contracting or termination of a relevant service, a change in the jurisdiction of processing or storage, a material change in the technology architecture or in the service perimeter, a penetration test result that reveals a structural deficiency, or an audit or supervisory finding.

## 23. Reference Standards

- BCB Resolution No. 85 of April 8, 2021, as currently in force, in particular Chapter III and articles 21, 22-A, 22-B and 23.
- BCB Resolution No. 552 of March 3, 2026, which extended the scope of BCB Resolution No. 85/2021 to virtual asset service provider companies.
- BCB Resolutions No. 519 and No. 520 of November 10, 2025, in particular articles 14, 32 to 43, 45, 48, 49, 50 and 51 of Resolution No. 520.
- Law No. 14,478 of December 21, 2022.
- Law No. 13,709 of August 14, 2018, with regard to personal data protection.

## 24. Effectiveness

This Policy enters into force on the date of its publication, after approval by the Organization's Board of Executive Officers, formalized in minutes, following prior deliberation by the Compliance Committee, and remains in force until its review or express revocation. The approval of this Policy and of the Incident Action and Response Plan by the Board of Executive Officers complies with article 9 of BCB Resolution No. 85/2021, applicable to the Organization by virtue of BCB Resolution No. 552/2026; in the absence of a board of directors, approval rests with the Board of Executive Officers and is not replaced by the ratification of a committee resolution.

## 25. 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 |