

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

Information Security Policy

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Contents

1. Purpose	2
2. Scope	2
3. Terms and Definitions	4
4. Information Security Principles	4
5. General Guidelines	5
5.1. Information Security Objectives	5
5.2. Organizational Commitment	5
5.3. Compliance	5
5.4. Risk Management	6
5.5. Human Resources Security	6
5.6. Awareness and Training	6
5.7. Asset Management	6
5.8. Acceptable Use of Assets and Technology Resources	7
5.9. Information Classification and Labeling	7
5.10. Information Transfer	8
5.11. Information Retention and Disposal	8
5.12. Privacy and Personal Data Protection	8
5.13. Intellectual Property	9
5.14. Identity and Access Management	9
5.15. Segregation of Duties	9
5.16. Physical and Environmental Security	9
5.17. Remote Work and Remote Access	10
5.18. Network and Communications Security	10
5.19. Protection against Malicious Code	10
5.20. Vulnerability Management	11
5.21. Change Management	11

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

5.22. Event Monitoring and Logging	11
5.23. Cryptography	12
5.24. Backup	12
5.25. Use of Cloud Services	12
5.26. Secure Development	13
5.27. Supplier and Supply Chain Management	13
5.28. Business Continuity	13
5.29. Incident Management	14
5.30. Use of Artificial Intelligence	14
5.31. Changes to the ISMS	14
5.32. Monitoring, Measurement and Audit	15
6. Exceptions	15
7. Violations and Penalties	15
8. Review	15
9. Reference Standards	16
10. Effectiveness	16
11. Version Control and History	16

1. Purpose

The purpose of this Policy is to establish the Organization's Information Security principles and guidelines, with a view to protecting its information and assets and ensuring their confidentiality, integrity and availability.

In addition, this Policy seeks to guide the adoption of Information Security practices, promote compliance with legal, regulatory, contractual and other applicable requirements, and establish the responsibilities related to the protection of information within the Organization.

2. Scope

This Policy applies to all employees, third parties and suppliers who have access to the Organization's information, assets, systems, services or environments, regardless of their location or form of access.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

The guidelines set out in this Policy cover information, regardless of its physical or digital format, as well as the assets, technology resources, processes and environments used for its storage, processing or transmission.

Information Security is not limited to systems and technology resources; it also encompasses people, processes and other means involved in protecting the Organization's information.

This document applies to Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda. (the PSAV company), referred to in this document as the Organization.

For the PSAV company, the cybersecurity requirements of BCB Resolution No. 85/2021 are detailed in the Cybersecurity Policy, including those on the contracting of data processing, data storage and cloud computing services, addressed in its Cloud Chapter, with which this Policy is aligned.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

3. Terms and Definitions

Term	Definition
Asset	Any element that has value to the Organization, including information, systems, applications, services, infrastructure, devices, people and processes.
Information	A set of organized and ordered data that makes it possible to understand a given subject in a context.
Vulnerability	Weakness or deficiency in an asset, process, system or control that can be exploited by a threat, potentially resulting in an information security incident.
Threat	Event, action or agent with the potential to exploit a vulnerability and cause damage to an asset or to information security.
Incident	Event that compromises or may compromise the confidentiality, integrity or availability of the Organization's information, systems or services.
Risk	Possibility of a threat exploiting a vulnerability and causing a negative impact on the organization, considering the probability of occurrence and its consequences.
Cryptography	Technique used to encipher information or a set of data so that it is inaccessible to those who do not have the access key.
Backup	Copy of files, folders, databases or even entire disks to secondary storage systems, in order to preserve data in the event of incidents or problems and enable its recovery.
ISMS Owner	Officer responsible for the Information Security Management System and for the cybersecurity policy before the Central Bank of Brazil (BCB Res. 85/2021).
Information Security Manager	Person responsible for managing information security and cybersecurity, including coordinating incident response.
Senior Management	The Organization's Board of Executive Officers.

4. Information Security Principles

Information Security at the Organization is guided by preserving the confidentiality, integrity and availability of information and associated assets, considering the risks and the requirements applicable to its activities.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

For the purposes of this Policy, the following principles must be observed:

- a. Confidentiality:** ensuring that information is accessed and used only by duly authorized persons, entities or processes;
- b. Integrity:** ensuring the accuracy, completeness and protection of information against unauthorized alteration or destruction;
- c. Availability:** ensuring that the necessary information, systems and resources are accessible and available to authorized parties, according to the Organization's needs.

The application of these principles must take into account the criticality of the information and assets, the identified risks and the applicable legal, regulatory and contractual requirements.

5. General Guidelines

The guidelines set out in this Policy aim to guide the protection of the Organization's information and assets against internal and external threats, reduce the risks arising from Information Security failures, and promote the adoption and maintenance of controls appropriate to the Organization's needs.

5.1. Information Security Objectives

The Organization sets measurable information security objectives, consistent with this Policy and with the approved risk appetite, defined and reviewed annually in the Annual ISMS Plan, with an indicator, target, measurement method, responsible person and deadline. Progress is reported quarterly to the Compliance Committee and consolidated in the management review.

5.2. Organizational Commitment

The Organization is committed to protecting its information and assets, to maintaining and continually improving Information Security and to meeting legal, regulatory, contractual and other applicable requirements.

To this end, the Organization must promote the adoption of Information Security controls proportionate to the identified risks, provide the necessary resources and foster a security culture consistent with its objectives and activities.

5.3. Compliance

The Organization must identify and observe the legal, regulatory, contractual and other requirements applicable to Information Security, adopting the measures necessary to ensure compliance.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

Adherence to the applicable requirements must be monitored and assessed periodically, and any deviations or non-conformities identified must be recorded and addressed in a timely manner, in accordance with the processes established by the Organization.

5.4. Risk Management

The Organization must manage Information Security risks in a structured manner proportionate to its context, considering the potential impacts on its information, assets, processes and services.

Identified risks must be assessed, treated and monitored in accordance with the criteria and guidelines established by the Organization, so as to support decision-making and maintain risk levels compatible with its objectives.

5.5. Human Resources Security

The Organization must adopt Information Security controls throughout the employment life cycle, from selection and hiring to termination, considering the responsibilities, risks and requirements applicable to the roles performed.

Processes related to people management must include, where applicable, screening of candidates, formalization of Information Security responsibilities and obligations, and the adoption of appropriate measures in hiring, transfer and termination processes.

Information Security responsibilities must be communicated to employees and formalized through appropriate and auditable means.

5.6. Awareness and Training

The Organization must promote Information Security awareness and training actions, so as to ensure that employees know their responsibilities and are able to comply with the guidelines and controls applicable to their activities.

Actions must take into account the Organization's needs and, where applicable, the responsibilities and risks associated with the roles performed, including general and specific training.

Participation, completion and, where applicable, the effectiveness of awareness and training actions must be monitored and recorded through appropriate and auditable means.

5.7. Asset Management

The Organization must identify, record and keep up to date the assets relevant to its activities and to Information Security, considering information, technology resources, systems, applications, services and other assets that support its processes and operations.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

Assets must have defined owners and be managed according to their importance, criticality and associated risks, considering their entire life cycle, from acquisition, creation or provision to return, replacement or disposal.

Asset records must be periodically reviewed and updated whenever there are relevant changes in their status, use or ownership.

5.8. Acceptable Use of Assets and Technology Resources

The Organization must establish guidelines for the appropriate and secure use of its assets and technology resources, which must be used primarily for the performance of professional activities and in compliance with internal, legal, regulatory and contractual requirements.

Employees and other authorized users must use assets, systems, applications, services and technology resources responsibly, ethically and securely, taking the necessary care to prevent unauthorized access, loss, alteration, improper disclosure or compromise of the Organization's information and resources.

Only assets, software, services and technology resources duly authorized by the Organization may be used to store, process or transmit corporate information, subject to formally approved exceptions.

5.9. Information Classification and Labeling

The Organization's information must be classified according to its sensitivity, criticality and protection requirements, so as to ensure the application of controls commensurate with the risks associated with its access, use or disclosure.

The assigned classification must guide the handling and protection of information throughout its life cycle and be reviewed whenever there are relevant changes in its nature, value, sensitivity or applicable requirements.

Information must be labeled, where applicable, so as to allow its classification to be identified and to guide users on the care required for its proper handling.

Information is classified into the levels Public, Internal Use, Confidential and Restricted, in accordance with the Information Management Standard. Transaction and client data protected by secrecy (Complementary Law No. 105/2001, extended to PSAV companies by CMN Resolution No. 5,280/2026) are classified, at a minimum, as Confidential, and virtual asset control instruments are classified, in all cases, as Restricted; external sharing of data under secrecy requires a legal basis, an order from a competent authority or the data subject's consent.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

5.10. Information Transfer

The transfer of the Organization's information, by physical, digital or other means of communication, must be carried out securely and in a manner consistent with the classification and sensitivity of the information involved.

Appropriate controls must be adopted to protect information during transfer against unauthorized access, loss, alteration, improper disclosure or compromise, considering the means used and the associated risks.

When the transfer involves third parties or other organizations, protection requirements commensurate with the information shared and the nature of the relationship must be established.

5.11. Information Retention and Disposal

The Organization's information must be retained for the period necessary to meet business needs and legal, regulatory, contractual and other applicable requirements.

Information retention must take into account its nature, classification and purpose, ensuring its protection throughout the period during which it is kept by the Organization.

Information and the media that store it must be disposed of securely when no longer needed or when the applicable retention period ends, using methods consistent with its classification and sensitivity, so as to prevent its recovery or unauthorized access.

When disposal is carried out by third parties, evidence of its execution must be kept, where applicable.

5.12. Privacy and Personal Data Protection

The Organization must ensure the protection of the personal data processed in the course of its activities, observing the principles, data subject rights and other requirements established by the legislation and regulation applicable to personal data protection.

Personal data must be processed for legitimate purposes compatible with the Organization's activities, limited to what is necessary to achieve the established purposes, and protected against unauthorized access, loss, alteration, disclosure or improper processing.

Security and protection measures appropriate to the risks associated with the processing of personal data must be adopted throughout its life cycle.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

5.13. Intellectual Property

The Organization must protect the intellectual property rights related to the information, systems, applications, source code, documentation, trademarks and other intellectual assets used, developed or maintained in the course of its activities.

The use, reproduction, alteration, distribution or sharing of materials protected by intellectual property rights must observe the applicable authorizations, licenses, contracts and other legal requirements.

Employees and other authorized users must use third-party software, content and other materials in accordance with the respective rights of use and licensing.

5.14. Identity and Access Management

Access to the Organization's information, systems, applications, services and technology resources must be granted according to the needs of the activities performed, observing the principles of least privilege, need-to-know and segregation of duties.

Identities and access must be managed throughout their life cycle, including granting, modification, review and revocation, with appropriate authorization and maintenance of the applicable records and evidence.

Authentication mechanisms commensurate with the risks and criticality of the resources accessed must be adopted, including multi-factor authentication, where applicable.

5.15. Segregation of Duties

Conflicting duties and responsibilities must be segregated so as to reduce the risks of fraud, error, misuse of information or performance of unauthorized activities.

The definition of responsibilities, duties and access must take into account potential conflicts of interest and incompatibilities between activities, observing the risks associated with the processes and roles performed.

Where segregation of duties is not feasible, compensating controls appropriate to the identified risks must be adopted.

5.16. Physical and Environmental Security

The Organization must adopt appropriate physical and environmental security measures to protect its information, assets and technology resources against unauthorized physical access, damage, interference and other threats that may compromise their security.

Access to facilities and areas that house relevant information or assets must be controlled according to the Organization's risks and needs, and restricted to duly authorized persons.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

Assets and information must be protected in the environments in which they are used or stored, including the adoption of practices to prevent exposure, improper access, loss or damage.

5.17. Remote Work and Remote Access

Remote work and remote access to the Organization's information, systems, applications and technology resources must be carried out securely, observing the established protection requirements and the risks associated with the environment and form of access.

Users must adopt appropriate measures to prevent unauthorized access, exposure or compromise of the Organization's information and assets when carrying out activities outside the corporate environments.

Remote access to the Organization's resources must be carried out through authorized means and devices, using the security and authentication mechanisms established by the Organization.

5.18. Network and Communications Security

The Organization must protect its networks, communication services and other connectivity resources against unauthorized access, interception, unavailability and other threats that may compromise the confidentiality, integrity or availability of information and services.

Network and communication resources must be managed and protected through controls commensurate with the risks and criticality of the environments and services supported, considering the segregation of environments and the restriction of communications, where applicable.

The architecture, configurations and protection mechanisms of networks and communications must be periodically assessed and updated according to the Organization's needs and the identified risks.

5.19. Protection against Malicious Code

The Organization must adopt measures to prevent, detect and address threats related to malicious code that may compromise the confidentiality, integrity or availability of information or the operation of its assets and technology resources.

The Organization's assets must be protected by security mechanisms commensurate with the identified risks, including preventive, detective and corrective measures against malicious code.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

Users must immediately report to the responsible areas any suspicion or evidence of malicious code, anomalous behavior or compromise of the Organization's assets and technology resources.

5.20. Vulnerability Management

The Organization must identify, assess, prioritize and address vulnerabilities that may compromise the security of its information, assets, systems, applications and services, in a manner commensurate with the identified risks.

Identified vulnerabilities must be addressed within a timeframe consistent with their criticality and potential impact, adopting mitigation measures, corrections or compensating controls, where applicable.

The effectiveness of the actions implemented must be monitored periodically, so as to support the continuous reduction of exposure to Information Security risks.

5.21. Change Management

The Organization must ensure that changes related to information, assets, systems, applications, infrastructure and services are assessed, approved, implemented and recorded in a controlled manner, considering the associated Information Security risks.

Changes that may affect the confidentiality, integrity, availability or compliance of the Organization's information and services must be subject to risk analysis and to the adoption of the applicable security controls before implementation.

Implemented changes must be recorded and, where applicable, subsequently assessed in order to verify their effectiveness and identify the need for corrective or improvement actions.

5.22. Event Monitoring and Logging

The Organization must monitor its assets, systems, applications, services and technology environments in order to identify events that may affect Information Security and to support the prevention, detection, investigation and handling of incidents.

Logs of events relevant to Information Security must be generated, protected, stored and retained for the period defined by the Organization, so as to preserve their integrity, availability and traceability.

Information obtained through monitoring and event logs must be used to support Information Security management, incident investigation, compliance with legal, regulatory and contractual requirements and the continuous improvement of the controls implemented.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

5.23. Cryptography

The Organization must adopt appropriate cryptographic mechanisms to protect the confidentiality, integrity and authenticity of information, considering its classification, sensitivity, the identified risks and the applicable legal, regulatory and contractual requirements.

The use of cryptographic controls must observe criteria defined by the Organization for the protection of information in storage, processing and transmission, as well as for the proper management of cryptographic keys, where applicable.

The cryptographic mechanisms adopted must be periodically assessed to ensure their effectiveness and suitability to the Organization's needs.

5.24. Backup

The Organization must ensure that backup copies of the information and assets necessary for the continuity of its operations are made and maintained, according to business requirements and the identified risks.

Backup copies must be protected against unauthorized access, alteration, loss or destruction and remain available for use when necessary, observing the retention, storage and recovery requirements established by the Organization.

The effectiveness of backup and recovery processes must be periodically verified to ensure their ability to meet the Organization's needs.

5.25. Use of Cloud Services

The use of cloud services must observe the Information Security, privacy, compliance and risk management requirements established by the Organization, considering the criticality of the information and services involved.

The contracting, use and management of cloud services must ensure the adoption of controls commensurate with the identified risks, as well as the protection of information throughout its life cycle.

The cloud services used by the Organization must be periodically assessed for security, compliance and adherence to the requirements established by the Organization.

The contracting of relevant data processing, data storage and cloud computing services follows the Cloud Chapter of the Cybersecurity Policy.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

5.26. Secure Development

The Organization must incorporate Information Security requirements into all stages of the life cycle of development, acquisition, maintenance and modification of systems, applications and other technology solutions, in a manner commensurate with the identified risks.

Systems and applications must be developed, tested, implemented and maintained in accordance with secure development practices, observing applicable security, privacy, quality and compliance requirements.

Changes to systems, components and technology environments must be made in a controlled manner, preserving the integrity, availability and security of the Organization's information and services.

5.27. Supplier and Supply Chain Management

The Organization must manage the Information Security risks related to suppliers, partners and other third parties that have access to its information, assets, systems or services, throughout the life cycle of the relationship.

Suppliers, partners and third parties must meet the Information Security, privacy, compliance and other obligations established by the Organization, according to the nature of the services provided, the information handled and the risks involved.

The contracting, monitoring and reassessment of suppliers, partners and third parties must take into account security criteria commensurate with the identified risks, as well as the applicable legal, regulatory and contractual requirements.

5.28. Business Continuity

The Organization must establish and maintain processes that ensure the continuity of its activities and the recovery of its critical processes, information, systems and services in the face of incidents, interruptions or events that may compromise its business objectives.

Continuity requirements must take into account the identified risks, the impacts on the business and the criticality of the processes and assets involved, including prevention, response and recovery measures appropriate to the Organization's needs.

Business continuity plans and processes must be periodically assessed, tested and updated to ensure their effectiveness and adherence to the Organization's needs.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

5.29. Incident Management

The Organization must establish and maintain processes for the identification, recording, reporting, assessment, handling and response to Information Security incidents, so as to minimize their impacts and restore the affected operations as quickly as possible.

Information Security incidents must be reported promptly to the responsible areas, recorded through appropriate means and handled according to their nature, criticality and potential impacts.

The causes of incidents and lessons learned must be analyzed, where applicable, with a view to implementing corrective, preventive and continuous improvement actions for Information Security controls.

Incident handling follows the Incident Management Standard and the Incident Action and Response Plan. The relevance parameters for incidents and the communication of crisis situations to the Central Bank of Brazil follow the Cybersecurity Policy.

5.30. Use of Artificial Intelligence

The use of Artificial Intelligence solutions within the Organization must observe the applicable Information Security, privacy, intellectual property, compliance and risk management requirements.

The Organization's information may only be used in Artificial Intelligence solutions in accordance with its classification, sensitivity and the authorizations established by the Organization, and the sharing of information whose use may compromise the confidentiality, integrity, availability or interests of the Organization is prohibited.

The adoption and use of Artificial Intelligence solutions must be commensurate with the associated risks, observing the controls, restrictions and guidelines established by the Organization.

5.31. Changes to the ISMS

Changes to the ISMS, its scope, document structure, roles, control tools and processes are planned, assessed for risk and approved by the Compliance Committee, recorded in minutes and reflected in the Annual ISMS Plan.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

5.32. Monitoring, Measurement and Audit

The information security indicators defined in the policies and standards are consolidated in the Annual ISMS Plan, measured monthly by Information Security and reported quarterly to the Compliance Committee. The ISMS is audited annually by internal audit, performed by an independent contracted firm, with the support of Compliance when necessary, and submitted to management review in accordance with the Internal Rules of the Compliance Committee and the ISMS Manual.

6. Exceptions

Exceptions to this Policy and to the regulations derived from it are recorded, assessed for residual risk by Information Security and approved. Every exception has a defined deadline, compensating controls and responsible person, and is recorded in a controlled system that ensures traceability, integrity and change history.

Exceptions granted do not exempt those responsible from adopting the measures necessary to reduce the risks arising from their treatment.

7. Violations and Penalties

Non-compliance with the guidelines set out in this Policy, as well as with the standards, procedures and other documents derived from it, may subject those responsible to the applicable administrative, disciplinary, contractual and legal measures, according to the nature, severity and impacts of the occurrence.

Any suspicion or evidence of a violation must be reported to the responsible areas for analysis, handling and adoption of the applicable measures, observing the Organization's internal processes and the legislation in force.

Violations may result, where applicable, in corrective actions, disciplinary measures, civil, administrative or criminal liability, as well as termination of contracts or other measures provided for in the legislation and in the instruments executed with the Organization.

8. Review

This document must be reviewed at least annually or whenever there are relevant changes in the structure, processes, legal, regulatory, contractual or other requirements applicable to the Organization, or when the need for an update is identified.

	Information Security Policy	SEG-POL-001-FIN
Publication Date: 10/15/2026	Information Security	Public

9. Reference Standards

ISO/IEC 27001:2022: Information security, cybersecurity and privacy protection, Information security management systems, Requirements.

ISO/IEC 27002:2022: Information security, cybersecurity and privacy protection, Information security controls.

Law No. 13,709 of August 14, 2018: General Personal Data Protection Law (LGPD).

BCB Resolution No. 520/2025: Provision of virtual asset services and operation of virtual asset service provider companies.

BCB Resolution No. 85/2021: Cybersecurity policy and contracting of data processing, data storage and cloud computing services, applicable to virtual asset service provider companies under BCB Resolution No. 552/2026, as amended by BCB Resolution No. 538/2025.

10. Effectiveness

This document enters into force on the date of its publication, after approval by the Board of Executive Officers, formalized in minutes, following prior deliberation by the Compliance Committee, and remains in force until its review or express revocation.

11. 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