

	Physical Security Policy	SEG-POL-008-FIN
Publication Date: 10/15/2026	Information Security	Public

Physical Security Policy

Trace Finance Sociedade Prestadora de Serviços de Ativos Virtuais Ltda.

Contents

1. Purpose	1
2. Scope	2
3. Terms and Definitions	2
4. Principles for the Protection of the Physical Environment	3
5. Physical Access Control	3
5.1. Access Management	3
5.2. Restricted Areas	4
5.3. Recording and Monitoring	4
6. Protection of the Environment and Physical Infrastructure	5
7. Monitoring	6
8. Incident Reporting	6
9. Third-Party and Cloud Environments	6
10. Remote Work, Clear Desk and Off-Premises Equipment	7
11. Review	7
12. Reference Standards	7
13. Effectiveness	7
14. Version Control and History	8

1. Purpose

This Policy sets out guidelines for physical access control and for the protection of the Organization's work environment, with the aim of protecting people, assets and information, ensuring the confidentiality, integrity and availability of information, and meeting the applicable legal, regulatory, contractual and business requirements.

	Physical Security Policy	SEG-POL-008-FIN
Publication Date: 10/15/2026	Information Security	Public

2. Scope

This Policy applies to the Organization's physical facilities and to all persons who use or access them, including employees, third parties, service providers, partners and visitors, as well as to the physical assets and information under its responsibility.

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.

3. Terms and Definitions

Term	Definition
Asset	Any physical or logical resource that has value to the Organization and requires protection, including equipment, documents, information and infrastructure.
Physical Environment	Facilities, premises and areas used by the Organization to carry out its activities, including offices, rooms, restricted areas and other locations under its responsibility.
Restricted Area	Environment to which access is controlled because of the criticality of the assets, information or services it contains, and which may be accessed only by duly authorized persons.
Physical Access Control	Set of measures intended to control and record the access of persons to the Organization's facilities or areas, in a manner commensurate with the identified risks.
Visitor	Person who is not part of the Organization's workforce and who accesses its facilities temporarily, upon authorization.
Third Party	Individual or legal entity that provides services or performs activities for the Organization without a direct employment relationship.
Security Perimeter	Physical boundary defined to protect the Organization's facilities, areas or assets against unauthorized access.
Physical Infrastructure	Set of facilities, equipment and physical resources that support the Organization's operations, including power, air-conditioning, cabling and monitoring systems and other elements related to the physical environment.
Monitoring	Continuous or periodic oversight of physical and environmental security controls, with the aim of identifying events, failures or situations that may compromise information security.

	Physical Security Policy	SEG-POL-008-FIN
Publication Date: 10/15/2026	Information Security	Public

4. Principles for the Protection of the Physical Environment

The Organization's physical environment is an integral part of the Information Security Management System (ISMS) and must be protected so as to preserve people, information assets, infrastructure and the services essential to the business.

The protection of the physical environment must observe, at a minimum, the following principles:

- a.** Classification by criticality and risk, considering the type of information processed, stored and accessed at the location;
- b.** Defense in depth, combining physical, administrative and technological controls of a preventive, detective and corrective nature;
- c.** Minimum necessary access, aligned with roles and responsibilities;
- d.** Proportionality, ensuring that controls are appropriate to the identified level of risk;
- e.** Integration with the ISMS and with the risk management, business continuity and incident response processes.

Areas that store information assets, handle classified information or support critical services must have physical controls commensurate with their criticality and with the identified risks.

5. Physical Access Control

Physical access to the corporate facilities must be controlled so as to prevent unauthorized access, protect people, assets and information, and reduce information security risks. To this end, the Organization must:

- a.** Define and maintain the physical perimeter of the facilities under its responsibility;
- b.** Control the entry and exit points of the facilities according to their criticality and the identified risks;
- c.** Apply physical access control mechanisms appropriate to the risk.

5.1. Access Management

Access to the Organization's facilities must be granted exclusively to authorized persons, based on the principle of least privilege and on the need for access to perform their activities.

The Organization must implement physical access control mechanisms commensurate with the criticality of the areas and the identified risks, including, where applicable:

	Physical Security Policy	SEG-POL-008-FIN
Publication Date: 10/15/2026	Information Security	Public

- a.** Controlled reception, turnstiles or equivalent systems;
- b.** Physical credentials, biometric identification, proximity cards (RFID) or equivalent mechanisms;
- c.** Physical or electronic locks to protect restricted areas;
- d.** Physical barriers to protect alternative entry points, such as doors, windows and service entrances.

Access by third parties, visitors and service providers must be authorized in advance and granted only when necessary, preferably for a fixed period. Such access must be recorded and, where applicable, supervised while they remain on the premises, and must be terminated or revoked when the need for access ends.

Physical access rights granted are reviewed every six months by Management, with the support of Information Security, and revoked when no longer necessary.

5.2. Restricted Areas

Areas classified as restricted or critical must have physical controls commensurate with their criticality and with the identified risks, so as to prevent unauthorized access and protect the assets and information they contain.

Access to these areas must be granted exclusively to persons authorized to perform their activities there and, where applicable, recorded and supervised in accordance with the procedures established by the Organization.

5.3. Recording and Monitoring

The Organization must keep records of access to areas that have physical access control mechanisms, manually or electronically, containing, whenever applicable, sufficient information to ensure traceability, including:

- a.** Identification of the person;
- b.** Date and time of entry and exit;
- c.** Area or location accessed.

Access records must be protected against unauthorized access, alteration or deletion, observing a 12-month retention period in accordance with Annex B of the Document Management Standard, and must be available for use in audits, investigations or other verification activities when necessary.

Physical access control and the related recording mechanisms must be periodically assessed for effectiveness and reviewed whenever there are relevant changes to the infrastructure, the

	Physical Security Policy	SEG-POL-008-FIN
Publication Date: 10/15/2026	Information Security	Public

working model or the identified risks, or after information security incidents related to the physical environment.

6. Protection of the Environment and Physical Infrastructure

The Organization must implement controls to protect the physical environment and infrastructure against physical and environmental threats that may compromise information security, the Organization's assets or the continuity of operations.

The measures must be implemented based on the assessment of risks related to the physical environment, taking into account the criticality of the assets present, the type of operation carried out at the location and the possibility of events that may cause interruptions, damage or loss of information, such as:

- a.** Electrical failures;
- b.** Fires;
- c.** Flooding;
- d.** Structural and environmental conditions.

The Organization must adopt physical and environmental controls commensurate with the identified risks, which may include, where applicable:

- a.** Controls to mitigate failures in the electricity supply;
- b.** Appropriate fire detection, firefighting and suppression systems;
- c.** Measures to protect against flooding and other environmental events;
- d.** Protection of the electrical, network and communications infrastructure;
- e. Physical protection of critical assets against accidental or intentional damage;**
- f.** Removal of equipment from the premises only upon recording in the asset inventory;
- g.** Equipment maintenance recorded and performed by an authorized supplier;
- h.** Work in secure areas (server room or rack, if any) only when accompanied by an authorized person.

	Physical Security Policy	SEG-POL-008-FIN
Publication Date: 10/15/2026	Information Security	Public

7. Monitoring

The Organization must monitor physical and environmental security controls in a manner commensurate with the identified risks, in order to detect security events, failures in the implemented controls and situations that may compromise the protection of assets and information.

The Organization must:

- a.** Implement monitoring mechanisms commensurate with the criticality of the protected areas, including, where applicable, CCTV systems, alarms, sensors or equivalent controls;
- b.** Protect monitoring systems and records against unauthorized access, alteration or deletion;
- c.** Carry out periodic checks or tests of the effectiveness of the physical and environmental controls implemented;
- d.** Record, assess and address identified failures in accordance with the processes established by the Organization.

Monitoring records must be protected, have a retention period of 12 months for access records and 90 days for images, in accordance with Annex B of the Document Management Standard, and remain available for audits, investigations and other verification needs, where applicable.

8. Incident Reporting

Events related to unauthorized access, intrusions, failures in physical or environmental controls and other situations that may compromise information security must be reported through the formal channels defined by the Organization and, when characterized as information security incidents, handled in accordance with the current incident management process.

Where the event may affect the continuity of operations, the procedures established for business continuity management must be observed, where applicable.

9. Third-Party and Cloud Environments

The physical security of the data centers that host the Organization's production environments is the responsibility of the cloud service providers engaged as relevant services, and is evidenced by independent audit reports (SOC 2) and certifications (ISO/IEC 27001) obtained and analyzed in accordance with the Cloud Chapter of the Cybersecurity Policy (Section 11.2).

	Physical Security Policy	SEG-POL-008-FIN
Publication Date: 10/15/2026	Information Security	Public

10. Remote Work, Clear Desk and Off-Premises Equipment

The guidelines on remote work, clear desk and clear screen, and on the protection of equipment off the premises are set out in the Secure Work Policy and in the Devices and Acceptable Use Standard, which establish the parameters for automatic screen lock, disk encryption and device management. The loss or theft of equipment is recorded and reported immediately as an information security incident.

11. Review

This document must be reviewed at least annually or whenever there are relevant changes in the Organization's context or in the applicable legal, regulatory or contractual requirements.

12. 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.

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 and 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.

13. 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.

	Physical Security Policy	SEG-POL-008-FIN
Publication Date: 10/15/2026	Information Security	Public

14. 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