Document Type:	**STANDARD**		
Document Title:	**Third-Party Security**		
Responsible Area:	**IT OPERATIONS AND SECURITY**	Information Classification:	**PUBLIC**

Index

1. Introduction and Objectives

The purpose of this document is to establish minimum Information Security and Privacy guidelines and requirements for third parties that have access to EBANX data and information.

2. Scope and Users

This document applies to all third parties with the potential to access and affect the confidentiality, integrity, privacy or availability of EBANX's information and assets.

3. Terms and Definitions

Threat: It is the possibility of an undesirable event, internal or external, accidentally or purposely exploiting the company's security weaknesses, and potentially removing, disabling or destroying the information assets (resources), resulting in a harmful impact to EBANX.

Information Asset: It is any component (whether human, technological, software, document, system or equipment, etc.) that supports information from one or more business processes essential to EBANX's operations.

Authenticity: Principle that guarantees the veracity and origin of information or the identity of an entity (user, system, process).

Confidentiality: Protecting confidential information from being disclosed to unauthorized individuals, entities, or processes.

Availability: Ensuring that information and associated resources are available and accessible when needed by authorized users.

ebanker: Term used to refer to EBANX employees, temporary employees, partners, interns and minor apprentices.

EBANX: All companies in the EBANX economic group, including EBANX Payment Institution Ltd. (EBANX IP).

Information Security Incident and Privacy Incident: Violation of confidentiality, integrity or availability of institutional information in a material or reportable way, whether caused by unauthorized or accidental action. In the case of Privacy Incidents, it also represents inappropriate or unlawful processing of Personal Data.

Integrity: Protecting the accuracy and completeness of data and information. In an information security context, it means ensuring that data is not corrupted, altered, or destroyed in an unauthorized manner.

Non-repudiation: Guarantee in information security that the origin of an action or the integrity of information cannot be later denied by any of the parties. It establishes irrefutable proof of the event, usually through digital signatures and logs.

NDA (Non-Disclosure Agreement): A legal contract that establishes a confidentiality relationship between parties, prohibiting the disclosure of sensitive information to unauthorized third parties. Its primary purpose is to protect trade secrets and sensitive data.

Risk: Risk is the expectation of loss expressed as the probability that a threat can exploit the particular information asset, with a harmful outcome for the organization.

Information Security and Privacy Management System – ISPMS: Methodology based on ISO/IEC 27001, ISO/IEC 27701 and ISO/IEC 27002 standards that aims to establish a management and continuous improvement process for Information Security and Privacy.

Vulnerability: Weakness of an asset or control that can be exploited and then an event with a negative consequence can occur.

4. Directives

All third parties that have access to EBANX's information or information systems must comply with EBANX's Information Security and Privacy and Personal Data Protection Governance policies, as well as the associated documentation, when appropriate.

Third parties must protect EBANX's information against any unauthorized access, modification, destruction or dissemination, ensuring that the technological resources made available to them by EBANX are used only for the purposes informed and approved. In any operation that requires access to EBANX information, the third party must comply with the principles of Information Security: Confidentiality, Integrity and Availability.

In cases of doubts related to Information Security and Privacy and Personal Data Protection, third parties should seek guidance from their superiors or EBANX's Information Security and Privacy team. The Privacy and Personal Data Protection Notice is publicly available on the website, in addition to other documents, which guide the safe handling of the information and practices accepted and expected by EBANX.

4.1 Privacy and Protection of Personal Data

The privacy and personal data protection laws and regulations establish requirements and obligations for data processing activities. Many of these requirements and obligations aim to reduce the risk of leakage or internal failures that may cause damage to data subjects. There are several measures that can be adopted by processing agents to demonstrate that the activities are carried out considering the best practices and focusing on the protection of the data subject.

The EBANX respects the rights of any data subject and also complies with applicable laws and regulations, such as the LGPD in Brazil. For further details, the Privacy Notice, available on the website, explains the relevant principles and how we collect personal data and other types of personal data processing.

The EBANX data, processed by third parties, must be treated in accordance with current data protection regulations and practices accepted by EBANX.

4.2 Classification of Information

EBANX has established four levels of information classification: Public, Internal Use, Restricted, and Confidential. Information owned or handled by EBANX must be classified and handled in accordance with the levels of confidentiality established in *the "Information Classification*" standard.

Level of Confidentiality	Marking	Classification criteria	Access restriction
Public	PUBLIC	Public information must not harm the organization in any way or violate any applicable laws or regulations, such as privacy rules.	The information is available to the public.
Indoor Use	INDOOR USE	Unauthorized access to information can cause minor damage and/or inconvenience to the organization.	The information is available to all employees and authorized third parties under NDAs or contract containing specific clauses regarding the confidentiality of the information.
Restricted	RESTRICTED	Unauthorized access to information can harm the organization's business and/or reputation.	The information is available only to a specific group of employees and authorized third parties under NDAs or contract containing specific clauses regarding the confidentiality of the information.
Confidential	CONFIDENTIAL	Unauthorized access to information can cause catastrophic (irreparable) damage to the organization's business and/or reputation. Sensitive Personal Data and payment data fall into this category.	The information is available only to individuals selected from within the organization and authorized third parties under NDAs or contract containing specific clauses regarding the confidentiality of the information.

Any type of information in any format (e.g., written, printed, video, image, media, verbal, digitally stored, transmitted by electronic mail), which does not have an identified Classification, is considered for INTERNAL USE.

Third Parties must be vigilant when talking about or sharing confidential information of EBANX in public spaces, social media or during teleworking. They should also avoid naming other entities in conversations, considering that EBANX may be bound by Non-Disclosure Agreements (NDA) with these parties.

4.3 Intellectual Property

Information (such as applications, documents and courses) produced by third parties or external parties, in the performance of their contracted functions, belongs to EBANX, unless the contract specifies otherwise.

The third party must comply with the legal and regulatory aspects of intellectual property and immediately notify EBANX's Information Security team or Legal Department in case of violation of this rule or intellectual property laws.

4.4 Roles and Responsibilities

This standard sets forth the responsibilities of all individuals involved in the following topics:

4.4.1 Monitoring

- The third parties should be aware that any information that is accessed, received, or transmitted on the local network and the Internet is subject to monitoring, inspection, and logging in order to ensure the integrity of the data and information and for auditing purposes, including the prevention of cyber threats;
- Third parties shall cooperate fully with any audit activity initiated by EBANX, including audits conducted by third parties on behalf of EBANX.
- Independent third parties can perform vulnerability scans and penetration tests on the IT infrastructure that processes sensitive EBANX information, taking a risk-based approach. The results of these tests and the remediation plans should be communicated to EBANX's Information Security team;
- All security investigations will be managed or coordinated by the Information Security team. EBANX and its economic group companies monitor many aspects of user behavior, including servers, workstations, and other network access devices. Where applicable, and

not limited to, the following logs will be scanned for security issues and vulnerability exploitation:"

- Intrusion detection system events;
- Firewall events;
- User account events;
- Network scan events;
- System error events;
- Application events;
- Internet browsing events;
- Data backup and recovery events;
- Occurrences of Service Desk problems;
- Phone activity - detailed call reports;
- Surveillance camera activities;
- Network printer events.

4.4.2 Access Rights

Third-party access to network resources, web applications, and physical facilities is limited and determined by the necessity of their activities. They must also respect the levels of access to EBANX systems, networks, equipment, facilities and information, as established by the Information Security team.

4.4.3 Physical Security

To access EBANX's facilities, third parties must respect the following security measures:

- Third parties must identify themselves and register at the reception. Inform the person accompanying and the purpose of the visit prior to granting an identification badge for entry into an EBANX facility;
- Use the identification badge granted to him/her, while within the premises of EBANX;
- Third parties who need access in restricted areas must be accompanied by an ebanker, who must accompany them throughout their stay. Third parties must not use the badge

outside EBANX's facilities and premises, they must keep the badge in a safe and confidential place;

- Third parties may keep the badge in their possession while the provision of services to EBANX is active. At the end of the contract/service, the badge must be returned immediately.
- In cases of loss, theft, robbery or misplacement of the identification badge, it must be reported immediately to the Information Security team, the Reception and ebanker responsible for contracting the service.

The following activities are prohibited unless specifically authorized:

- Any type of video, photograph or audio recording in the restricted areas, which involves other ebankers without consent or captures information from EBANX;
- Connect any electrical device to a power source in the safe areas;
- Touching or otherwise tampering with any equipment installed in secure areas;
- Connect any device to a network;
- Store flammable materials or equipment;
- Use any type of heating device.

4.4.4 Passwords

Users should employ good security practices when creating and using passwords, according to the following guidelines:

- Passwords should not be disclosed to others, including management and system administrators;
- Passwords should not be written down on any physical media, and the only possible storage is the password management application provided and authorized by the Information Security team;
- Each user must enable multi-factor authentication (MFA) on all systems that provide this feature;
- User-generated passwords should not be shared through any channel (verbally, in writing, or electronically, etc.). They should be changed if there is any indication that the

passwords or the system may be compromised, in which case a security incident should be reported;

- Strong passwords should be created or changed as follows:
    - Using at least twelve characters;
    - Using at least one numeric character;
    - Using at least one uppercase and at least one lowercase alphabetic character;
    - Using at least one special character;
- Passwords should not be based on personal data (e.g., date of birth, address, family member's name, etc.);
- Passwords must be changed every 3 months;
- Passwords should not be composed of dialect words or jargon of any language or any words written backwards;
- Passwords must be changed on the first login to a system;
- Passwords should not be stored in an automated login system (e.g., scripts, automations, or browser);
- Passwords created and used for personal purposes must not be the same as those used for commercial purposes;
- If a system is shared between users, with the proper authorization of the Information Security team, access must be carried out exclusively through the password vault. It is critical that the shared password is unique and not reused from personal accounts or other systems.

4.4.5 Acceptable Use

Information assets should be used only for business needs for the purpose of performing organization-related tasks, and the use of these assets is subject to the following rules:

- To ensure the security and integrity of the company's data, it is forbidden to use EBANX equipment for personal purposes. EBANX is not responsible for backing up personal information of third parties.

- Third Parties must be aware of the use of EBANX's technological resources and any other resources allocated to them. Therefore, they should not download software on computers or hire software solutions without EBANX approval, regardless of the area of activity of the third-party employee;
- Third parties should be aware of the use of EBANX's email account, using it only for purposes related to EBANX's business;
- Requests for contracting software must be made by the EBANX business area responsible for contracting the Third Party, and must follow the guidelines of *EBANX's* Third-Party Contracting Standard;
- The third party must not install or use peripheral devices or other devices to store and read data (e.g., USB flash drives) without the express permission of EBANX's Information Security team.

4.4.6 Remote Access

Third parties who act remotely must ensure the security of EBANX's data and information and that of its customers. To do so, they must follow these guidelines:

- Remote access must be done only through authorized devices and protected by strong passwords, with two-factor authentication enabled and using the access tools provided by EBANX;
- Protect information from unauthorized access in your remote workplace, which needs to be suitable for the activities;
- When using mobile devices in public places, the user must take care that the data cannot be read by unauthorized persons.

4.4.7 Table, Screen and Clean Slate

- When working with EBANX data and information, the third party must ensure that no confidential or sensitive information is visible to any unauthorized person (whether another employee or third party).

- To prevent unauthorized access, paper documents and confidential storage media should be removed from desks, printers, photocopiers, and other locations whenever the authorized person is absent from the workstation.
- When absent from the workstation, ebankers and third parties should always block the computer screen. In addition, the system has an automatic lock that is activated after two minutes of inactivity.
- Whiteboards and glass boards containing internal, restricted and/or confidential information must have their contents erased after use.

4.4.8 Credit Card Data

Third parties are not allowed to request credit card data, whether by email, phone or any other means. If this information is received accidentally, the Information Security team should be notified immediately.

4.4.9 Encryption

Information must be encrypted when transmitted externally and, whenever possible, in internal communications. Avoid verbal transmission of EBANX data and information in public or shared spaces.

4.4.10 Secure Development

Secure Development certification is a mandatory prerequisite for all developers contributing to the development repository. This certification must be updated annually.

There are environments prepared to perform code validations, tests, and proofs of concept that are managed by the CloudOPS team, who are the administrators of the environment. Access to the source code of any program must be restricted and strictly controlled.

4.4.11 Security Controls

Third parties must put controls in place to prevent, detect, eradicate and recover from malware threats;

Any changes to the systems or applications that process EBANX's confidential information should be reviewed and tested to ensure that there is no impact on business operations or information security.

4.4.12 Data Retention and Disposal

Third parties must return or dispose of information or data (including personal data) of EBANX in their possession, custody or control in the following situations:

- i) When they are no longer necessary for the original purpose ii) if there is no legal requirement that determines storage iii) after the termination of the Agreement. The period that is longer among these conditions is valid;

In addition, the return or disposal must occur immediately, upon request by EBANX, at any time;

EBANX's sensitive data or confidential information must be stored in accordance with the established storage periods and only for as long as is necessary for the purposes for which it was collected in accordance with the Personal Data Retention, Disposal and Destruction Standard.

4.4.13 Transfer and Sharing of Information

Some practices that must be followed when transferring and/or sharing information internally or externally from EBANX:

- It is prohibited to submit materials with content that is disturbing, unpleasant, sexually explicit, rude, libelous, or containing any other unacceptable or illegal content;
- If a third party receives a suspicious email, especially if there is evidence of a phishing attempt, they should report the content immediately through the "Phish Alert Button (PAB)" and communicate it to the Information Security team through the email infosec@ebanx.com;
- When sending messages, documentation, presentations or any information classified as Internal, Restricted and Confidential, the third party must protect it, as set forth in *the Information Classification Standard*;

- When sending EBANX information to any recipient, internal or external, consider the impact of improper access and implement the necessary security measures to mitigate this risk.
- When sharing relevant, internal, restricted, or confidential information, make sure the recipient has a signed Non-Disclosure Agreement (NDA) or a contract containing confidentiality clauses that protect EBANX data.
- Avoid sending files with Personal or confidential Data, if necessary, protect with a password;
- It is not allowed to publicly post materials that are considered internal, restricted, and/or confidential;
- It is forbidden to access corporate files on unknown, non-approved equipment or without adequate protection.
- Do not download, install or access non-approved software sites;
- Third parties should be aware of their surroundings when communicating in public spaces and social media. Avoid talking about insider, restricted, or confidential information, and do not mention third parties (companies or individuals) related to EBANX.

4.5 Penalties

In case of violation of the guidelines set forth in this document and in other documents related to the activities provided, the third party will be subject to immediate contractual termination, without prejudice to other sanctions provided for in the contract and in applicable laws. EBANX reserves the right to take all appropriate legal measures to protect your data, information and assets in case of non-compliance with the established standards.

4.6 Incident Reporting

A Security Incident refers to any event that compromises or may compromise the Confidentiality, Integrity or Availability of data in an information system. This can include malicious activities such as hacker attacks, viruses, malware, phishing, unauthorized access, among others. Where Personal Data is involved, it will be called a Privacy Incident.

The third party that suspects or identifies a Security Incident (including violations of the Policies and/or observed security vulnerabilities) or a Privacy Incident, must report it immediately through MyEBANXLife or the email infosec@ebanx.com. This quick action allows EBANX to respond to the incident quickly and effectively, minimizing damage and protecting information.

The Information Security team may request more information as needed.

4.7 Training and Awareness

All third parties who have access to restricted and confidential data and information must receive Information Security and Privacy awareness and training.

The Information Security team is responsible for promoting training and awareness to ensure that third parties understand their responsibilities in relation to the pillars of Information Security, confidentiality, integrity and availability of EBANX data and information.

5. Normative References

- **ISO/IEC 27000:2018** – Information Security Principles and Vocabularies.
- **ISO/IEC 27001:2022** – Requirements for Information Security Management Systems (ISMS).
- **ISO/IEC 27002:2022** – Information Security Controls.
- **ISO/IEC 27018:2019** – Practices for the Protection of Personal Data in Cloud Services.
- **ISO/IEC 27701:2019** – Information Privacy Management System (SGPI).

6. Related or Supporting Documentation

- Password Security Standard;
- Information Classification Standard;
- Data Encryption Standard;
- Remote Access Standard;
- Secure Development Standard;
- Personal Data Retention, Disposal and Destruction Standard;

- Information Security and Data Privacy Awareness Program Standard;
- Information Security and Privacy Incident Management Standard;
- Physical Security Standard;
- Third Party Recruitment Standard;
- Information Security Policy;
- Privacy Governance and Data Protection Policy.