Cybersecurity Policy

CONTROL SHEET

General Information

Title	Cybersecurity Policy
Reference Number	POL_SEG
Version Number	v6
Status	Revised
Policy Owner Department	Information Security
Business Scope	XP Inc. Group
Regional Scope	United States
Procedures and Other Related Documents	CMN Resolution No. 4893/21 and 4910/21; SUSEP Circular No. 638/21 Rule - Cybersecurity for Regulated Entities, Information Security Policy, Information Security Policy for Third Parties and Data Privacy Policy
Exemption from Policy	NA
Keywords for Quick Search	Cybersecurity, Information Security, Protection, Incidents, Controls, and Social Engineering

History of Versions

Version	Reason for Change	Date	Author	Department
1	Initial Version Revision	04/09/2019 04/09/2019 04/15/2019	Dalton Reis Bruno Stuani Paulo Fernandes	Information Security Information Security Legal
2	Annual Review	04/27/2020	Lucas Gomes Rafael Piotto Dalton Reis Paulo Fernandes	Information Security Information Security Information Security Legal
3	Annual Review	08/03/2021 09/01/2021 10/06/2021	Fernanda Rodrigues Fernanda Gentil Paulo Fernandes	Information Security Information Security Legal
4	Annual Review	11/10/2022	Fernanda Rodrigues Fernanda Gentil Paulo Fernandes	Information Security Information Security Legal
5	Revision	07/05/2023	Fernanda Rodrigues Fernanda Gentil Paulo Fernandes	Information Security Legal
6	Annual Review	09/04/2024 10/17/2024 11/09/2024 11/13/2024 11/13/2024 12/11/2024 12/17/2024	Ricardo Faria Solange Batista Bruno Dantas Caroline Assunção Fernanda Gentil Fernanda Rodrigues Fernando Fabre	SecOps GIA AppSec AppSec Information Security Information Security Legal

Approved **Date:** 12/17/2024	Daniel Falcone Information Security	Fabricio Almeida Officer	Leonardo Cardoso Officer	Marino Aguiar Technology and Security

TABLE OF CONTENTS

1. PURPOSE

The Cybersecurity Policy ("Policy") of the companies of the XP Inc. Group ("Group") aims to ensure the integrity, availability and confidentiality of the information owned and/or under its custody, in addition to preventing, detecting and reducing vulnerability to incidents related to the cyber environment, defining the rules that represent, at a strategic level, the fundamental principles incorporated by the Group to achieve information security objectives.

This Policy demonstrates the Group's commitment to safeguarding and processing information, following the Group's best practices and guidelines under the Brazilian General Personal Data Protection Law ("LGPD") and the Data Privacy Policy. We also demonstrate our commitment to the group's regulatory and strategic aspects by complying with the main regulations in force.

Finally, this document is intended for all users of the XP Inc. Group and any third parties that use its infrastructure, and that are involved in the design of solutions, systems, processes, products, or services, as provided for in the Information Security Policy for Third Parties.

2. SCOPE

This Policy applies to companies of the XP Inc. Group.

3. TERM OF EFFECTIVENESS, REVOCATION, AND CYCLE OF REVISION

This document comes into force from the date of its approval and cancels previous versions or those that deal with the same subject. This Policy may be revised annually or whenever necessary, in case of any change in the Group's standards, changes in information security guidelines, business objectives or where required by the local regulator of any of the Subsidiaries.

4. DEFINITIONS

Controlling Shareholder: The shareholder or group of shareholders that control the Company and its Affiliates, bonded by agreement or under common control, that exercises the power of control, direct or indirect, over the company, under the terms of Law No. 6404/76.

Managers: They are the duly constituted members of the Executive Board.

Affiliates: Companies in which the Controlling Shareholder has significant influence (Article 243, paragraph 1, of Law No. 6404/76).

Subsidiaries: The companies in which XP Inc. is the Controlling Shareholder.

Prudential XP Conglomerate: XP Investimentos CCTVM S.A., Banco XP S.A., XP DTVM Ltda., and other companies of the XP Inc. Group, incorporated in Brazil and abroad, which fall within the definition set forth in Resolution No. 4950/21, of the Brazilian Monetary Council (CMN).

Anonymized data: Data related to a data subject who cannot be identified, considering the utilization of technical means reasonable and available at the time of its processing;

General personal data: According to section II of article 5 of the LGPD, this is information related to an identified or identifiable individual;

Sensitive personal data: According to section II of article 5 of the LGPD, this is personal data about racial or ethnic origin, religious belief, political opinion, filiation to a union or an organization of religious, philosophic or political nature, data referring to health or sexual life, genetic or biometric data, when bound to an Individual;

XP Inc. Group or Group: XP Inc. Subsidiaries, its Subsidiaries, and Affiliates organized in Brazil, taken as a whole.

Third Parties: Suppliers/Business partners who provide services or offer products to the XP Inc. Group.

5. GENERAL PROVISIONS

Ensure the confidentiality, integrity and availability of information owned or under the responsibility of the Group; Third Parties, Affiliates, Business Partners, Suppliers, and service partners must comply with all requirements, as well as commit to fully following the items of this policy and the Information Security Policy for Third Parties;

6. INFORMATION SECURITY PRINCIPLE

We believe that information assets are the most important assets in the financial market, therefore, treating them responsibly is our commitment. Therefore, we are based on the principles of information security, whose objectives are to preserve the ownership of information, notably its confidentiality, integrity, and availability, allowing its use and sharing in a controlled manner, as well as the monitoring and processing of incidents arising from cyber attacks.

Confidentiality: ensure that the information processed is known exclusively to specifically authorized persons;

Integrity: ensure that information is kept intact, without undue modifications—accidental or intentional;

Availability: ensure that information is available to all persons authorized to process it.

7. CONFIDENTIAL INFORMATION

Access to confidential information, including general and/or sensitive personal data, collected and stored by XP Inc. Group is restricted to professionals authorized to directly use such information, and necessary for the provision of their services, with limited use, and must also comply with the Information Classification definitions provided for. The Group values privacy and information protection within the scope of the Brazilian General Personal Data Protection Law ("LGPD") and the Data Privacy Policy. The Group may disclose confidential information in the following circumstances:

- Whenever you are obliged to disclose them, whether by virtue of a legal provision, act of a competent authority, court order or warrant;
- To credit protection and defense bodies and service providers authorized by the Group to defend its rights and credits;
- To financial market regulatory bodies; and
- For other financial institutions, as long as it is within the established legal parameters and the applicability collected in relation to consent. In this case, the user may cancel their authorization at any time.

7.1. CONCEPT

Confidential Information: Any and all information, whether patented or not, verbal or otherwise presented, tangible or intangible, which may include, but is not limited to, technical, operational, commercial, financial, legal information, know-how (skill and/or knowledge acquired), inventions, processes, formulas and designs, whether patentable or not, business plans, accounting methods, techniques and accumulated experience, business plans, budgets, prices, expansion plans, business strategies, discoveries, ideas, concepts, techniques, projects, specifications, diagrams, templates, samples, flowcharts, computer programs, codes, data, source codes, disks, floppy disks, tapes, marketing and sales plans, any customer information, and any other technical, financial, legal and/or commercial information related to the Group, its customers, partners, suppliers, and employees.

8. CYBERSECURITY MANAGEMENT FRAMEWORK

The management of security controls aims to ensure that operational procedures are developed, implemented and maintained or modified in accordance with the objectives established in this Policy.

9. MANAGING ACCESS TO INFORMATION

Access to information is controlled, monitored, restricted to the least possible permissions and privileges, reviewed periodically and revoked promptly upon termination of the employee's or service provider's employment agreement.

Relevant, but not limited to, information processing equipment and facilities are kept in secure areas with appropriate levels of access control, including protection against physical and environmental threats. The Group's employees are periodically trained on the concepts of Information Security, through an effective awareness program and dissemination of the cybersecurity culture.

10. PROTECTION OF THE GROUP'S ENVIRONMENT

Controls and responsibilities are established for the management and operation of information processing resources, aiming to guarantee security in the Group's technological infrastructure through effective management in monitoring, processing, and responding to incidents, with the aim of minimizing the risk of failures and the secure administration of communications networks.

- Authentication

- Access to the Group's information and technological environments must be allowed only to persons authorized by the Information Owner, taking into account the principle of least privilege, segregation of conflicting roles and the information classification.

- Access control to systems must be formalized and include, at a minimum, the following controls:

  a) The use of individualized identifiers (access credentials), monitored and subject to blocking and restrictions (automated and manual);

  b) The removal of authorizations given to users and/or employees who are removed or dismissed from the Group, or who have changed roles; and

  c) Regular review of the granted authorizations.

10.1. Information Security Incident Management

The behavior of possible attacks is identified through detection controls implemented in the environment, such as content filter, malicious behavior detection tool, Antivirus, Antispam, among others. We adopt procedures aimed at preventing, analyzing, and dealing with incidents.

10.2. Information Leakage Prevention

Data loss prevention control aimed at ensuring that confidential data is not lost, stolen, or made improperly available *in the external environment* by unauthorized users.

10.3. Intrusion Tests

Internal and external Penetration Tests at the network and application layers must be performed annually.

10.4. Vulnerability Scan

Internal and external network scans should be performed periodically. Identified vulnerabilities must be addressed and prioritized according to their criticality level.

10.5. Control Against Malicious Software

All assets (computers, servers, etc.) connected to the corporate network or using the Group's information must, whenever compatible, be protected with an anti-malware solution determined by the Information Security area.

10.6. Encryption

Every encryption solution used by the Group must follow the Information Security rules and the security standards of the regulatory bodies.

10.7. Traceability

Automated audit trails must be deployed for all system components, to reconstruct the following events:

- User authentication (valid and invalid attempts);
- Access to Information;
- Actions performed by users including, but not limited to, creating, updating, or removing system objects.

10.8. Network segmentation

- Computers connected to the corporate network must not be accessible directly via the Internet, with the exception of DaaS (Desktop as a Service) services;
- Direct connection of a third-party network using remote control protocols to servers directly connected to the corporate network is not allowed;
- Implement network control, traffic, and/or firewall protection.

10.9. Secure development

The Group maintains a set of principles for developing systems securely, ensuring that cybersecurity is designed and implemented throughout the systems development lifecycle.

10.10. Backups

The backup execution process is carried out periodically, in order to avoid or minimize data loss in the event of incidents.

11. BUSINESS CONTINUITY

The business continuity process is implemented through critical process mapping, business impact analysis, and periodic disaster recovery testing. This process includes the business continuity related to the services engaged in the cloud and the tests planned for cyber-attack scenarios.

12. DATA PROCESSING, STORAGE, AND CLOUD COMPUTING

In accordance with BACEN Resolution No. 4893/2021, Bacen Resolution 4910/2021, as well as SUSEP Circular No. 638/21, for the contracting of data processing and storage and cloud computing services, the Group ensures an effective procedure for adherence to the rules provided for in the regulations in force.

13. MAIN SECURITY RECOMMENDATIONS FOR CUSTOMERS AND USERS

In addition to the recommendations described below, there is a complete guide to Information Security best practices. You can access it via the link: https://lp.xpi.com.br/seguranca-xp.

13.1 AUTHENTICATION AND PASSWORD

The customer is responsible for the acts performed with their identifier (login), which is unique and accompanied by an exclusive password for individual identification/authentication when accessing information and technology resources.

We recommend that:

- Keep your password confidential, memorize it and do not record it anywhere. In other words, do not tell anyone and do not write it down on paper;
- Change your password whenever there is any suspicion that it has been compromised;
- Create quality passwords, so that they are complex and difficult to guess;
- Prevent other people from using your equipment while it is connected/logged in with your identification;
- Always lock the equipment when you leave.
- Whenever possible, enable a second factor of authentication (For example: SMS, Token, etc.).

13.2 ANTIVIRUS

We recommend that the customer maintain an updated antivirus solution installed on the device used to access the services offered by the Group. Additionally, have the operating system updated with the latest available updates.

13.3 SOCIAL ENGINEERING

Social engineering, in the context of information security, refers to the technique by which one person seeks to persuade another, often abusing naivety or trust, with the aim of deceiving, carrying out scams or obtaining confidential information.

13.3.1 *PHISHING, SMISHING, and/or VISHING*

Technique used by cybercriminals to deceive users by sending malicious emails, SMS, and/or voice messages in order to obtain personal information such as passwords, credit card, CPF, bank account numbers, among others. Approaches can occur in the following ways:

- When they seek to attract users' attention, whether for the possibility of obtaining some financial advantage, out of curiosity or out of charity;
- When they try to pass themselves off as official communications from well-known institutions such as: Banks, E-commerce stores, among other popular websites;
- When they try to induce users to fill out forms with their personal and/or financial data, or even to install malicious software that aims to collect sensitive information from users;

13.3.2 *SPAM*

These are unsolicited emails, which are generally sent to many people, typically containing content for advertising purposes. Furthermore, Spam is directly associated with security attacks, being one of the main causes of the spread of malicious codes, illegal sale of products and dissemination of scams.

13.3.3 FALSE TELEPHONE CONTACT

These are techniques used by fraudsters to obtain information such as personal data, passwords, tokens, cell phone identification codes (IMEI) or any other type of information to commit fraud.

13.3.4 FAKE CUSTOMER SERVICE CENTER

These are techniques used by fraudsters to obtain information through customer service. When they get in touch, they claim that there is some pending registration update. It then asks you to confirm or update your phone number. The customer is then asked to provide the security code that was sent, from which the scammer can reset the password.

14. COMMUNICATION

In case of any doubts, suggestions and/or signs of irregularities in compliance with the provisions of this Policy, they must be communicated to our service channels via the link.