Cybersecurity Policy

SUMÁRIO

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 Vendors/Third Parties and Business Partners.

2. SCOPE

All corporate environments, systems, employees, partners of the XP Group, and the companies of the XP Inc. Group themselves.

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

Administrators: They are the duly appointed members of the Board of Directors.

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

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.

Anti-malware: A computer program that protects the device against malicious software such as viruses, spyware, and ransomware. It detects, blocks, and removes these types of threats to keep the device secure.

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.

DaaS: Desktop as a Service - A cloud computing model where the virtual desktop infrastructure is offered and managed by a third-party service provider, in this case, by XP Inc.

Firewall: It is a security device that monitors incoming and outgoing network traffic, allowing or blocking certain types of traff

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

Information Asset: It is any data or set of data that holds value for an organization, whether in terms of supporting decision-making, regulatory compliance, or competitive advantage. This includes information such as documents, records, databases, and specialized knowledge that are essential for the company's operations and strategies.

Malware: Malicious programs designed to cause harm, steal information, or compromise the security of computers and networks. This includes viruses, worms, trojans, spyware, ransomware, among others.

Pentest, Penetration Test or Ethical Hacking Test (EHT): Information security practice that involves simulating cyber-attacks on systems, networks, or applications to identify vulnerabilities that could be exploited by malicious attackers. The goal of penetration testing is to assess the security of an environment and provide recommendations.

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).

Security Incident: It is a security event or a set of events, confirmed or suspected, that may impact the availability, integrity, confidentiality, or authenticity of an asset and/or information system, as well as any violation of the Information Security Policy and/or Data Privacy Policy.

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.

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

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

Token: It is an additional electronic device to complement the user's authentication.

Vulnerability: It is a deficiency in the software that, when exploited, can result in it still being impact bug, but with a security impact.

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

5. GENERAL PROVISIONS

The Cybersecurity Policy of the XP Inc. Group aims to ensure the confidentiality, integrity, and availability of information owned by or under the responsibility of the XP Inc. Group. Furthermore, it establishes that third parties, affiliates, business partners, suppliers, and service providers must comply with all established requirements, committing to fully adhere to the items set forth in this policy and the Information Security Policy for Third Parties and Business Partners.

The senior management maintains a continuous commitment to cybersecurity by promoting the constant improvement of related procedures and practices. This commitment is reflected in the allocation of adequate resources, the definition, approval, and review of clear policies, and active leadership to ensure that protection measures are always up-to-date and aligned with best practices and regulatory requirements. Additionally, senior management fosters a security culture throughout the organization by promoting training, periodic assessments, and continuous process reviews to strengthen the institution's cyber resilience.

6. DESCRIPTION OF RULES/PROCEDURES

6.1 INFORMATION SECURITY PRINCIPLES

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
- To other financial institutions, provided that the established legal parameters are respected and prior authorization is granted by the client. The client reserves the right to revoke this authorization at any time.

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.

8.1 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 and Data Protection, through an effective awareness program and dissemination of the cybersecurity and data privacy culture.

8.2 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 XP 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.

8.2.1 Authentication

Access to the Group's information and technological environments must be allowed only to persons authorized by the Information Owner, considering 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:

- The use of individualized identifiers (access credentials), monitored and subject to blocking and restrictions (automated and manual);
- The removal of authorizations given to users and/or employees who are removed or dismissed from the Group, or who have changed roles; and
- Regular review of the granted authorizations.

8.2.2 Gestão de Incidentes de Segurança da Informação

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.

The XP Group will share data related to relevant incidents within a specified period, as well as response actions to incidents and results of Business Continuity tests in the form of a report. This report will be approved by senior management in accordance with applicable regulations.

8.2.3 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.

8.2.4 Intrusion Tests (Pentest)

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

8.2.5 Vulnerability Scan

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

8.2.6 Control against Malicious Software

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

8.2.7 Criptografia

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

8.2.8 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.

8.2.9 Network segmentation

Networks must be logically segmented so that only approved environments communicate with each other, with the following conditions:

- 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 network connections from third parties and the use of remote-control protocols to servers directly connected to the corporate network are not permitted
- The XP Group implements network control, traffic monitoring, and/or firewall protection.

8.2.10 Secure development

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

8.2.11 Backups

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

8.3 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.

8.4 CYBERSECURITY IN SUPPLIERS

The XP Group has a management process for suppliers, partners, and third parties that provide technology services and/or handle sensitive data or information relevant to the Group's operational activities. These entities must adopt rigorous procedures and controls focused on the prevention and treatment of security incidents in accordance with applicable regulations.

Such procedures include implementing proactive measures to identify, mitigate, and respond promptly to potential threats or vulnerabilities, ensuring the integrity, confidentiality, and availability of information. Additionally, these companies are required to maintain detailed records of incidents and communicate immediately with the XP Group, ensuring transparency and agility in resolving issues, in compliance with internal policies and applicable regulations.

8.5 DATA PROCESSING, STORAGE, AND CLOUD COMPUTING

The XP Inc. Group has an effective procedure for contracting and using data processing, storage, and cloud computing services, aiming to comply with the rules established by current regulations.

The processing and storage of applications and data must be carried out exclusively in cloud environments previously approved by the Information Security department, whether public or private. Access to these environments must be managed and centralized through platforms that enable detailed tracking of requests and reviews in an agile and timely manner. Furthermore, all security controls established in internal policies must be rigorously applied. The use of any products or services offered by cloud providers must undergo prior evaluation by Information Security to ensure compliance and risk mitigation.

9. MAIN SECURITY RECOMMENDATIONS FOR CUSTOMERS AND USERS

9.1 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.).

9.2 Antivirus

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

9.3 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.

9.3.1 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.

9.3.2 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.

9.3.3 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.

9.3.4 Fake Customer Service Center

São técnicas utilizadas pelos fraudadores para conseguir informações através do atendimento ao cliente, ao conseguir contato argumenta de que há alguma pendência de atualização cadastral. Na sequência, pede a confirmação ou atualização do número de telefone. Então é pedido ao cliente que seja informado o código de segurança que foi enviado, a partir disso, o golpista consegue redefinir a senha.

10. 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.