Cyber Security Policy

CONTROL SHEET

General Information

Title	Cyber Security Policy
Reference Number	POL_SEGINF_003
Version Number	V2
Status	Reviewed
Policy Owner Department	Information Security
Business Scope	XP Group Inc., XP Investments CCTVM S.A. and Banco XP S.A.
Scope of Geography	Brazil
Procedures and Other Related Documents	Resolution n° 4.658/18 e 4.752/19 of the National Monetary Council; XP Inc Group Information Security Policy
Dismissal from the Policy	NA
Keywords for Quick Search	Cyber Security, Incidents, Intrusion, Controls, Traceability, Culture, Dissemination

Version History

Version	Reason for Change	Date	Author	Department
1	Initial Version Revision	09/04/2019 09/04/2019 15/04/2019	Dalton Reis Bruno Stuani Paulo Fernandes	Information Security Information Security Legal
2	Annual Review	27/04/2020	Lucas Gomes Rafael Piotto Dalton Reis Paulo Fernandes	Information Security Legal

Approved by:	Bernardo Amaral Director	Guilherme Benchimol Director	Fabricio Almeida Director
Date: 28/04/2020			

SUMMARY

1. OBJECTIVE

The Cyber Security Policy ("Policy") of Grupo XP Inc. ("Group") aims to ensure the protection, maintenance of privacy, integrity, availability and confidentiality of information owned and/or under its custody, in addition to preventing , detect and reduce 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 the information security objectives.

This Policy demonstrates the commitment of the Group and its Senior Management in protecting and treating its customers' information, in order to provide full satisfaction with the security and privacy of their information. We also demonstrate our commitment to the regulatory and strategic aspects of the Group, thus complying with the main regulations in force.

This Policy is applied to Group companies, notably XP Investments CCTVM S.A. ("XP Investments") and Banco XP S.A. ("Banco XP").

2. VALIDITY

This Policy may be revised annually or, when necessary, in the event of any change in the Group's standards, change in information security guidelines, business objectives or if required by the local regulator.

3. PRINCIPLE OF INFORMATION SECURITY

We consider that information assets are the most important assets in the financial market, therefore, treating them responsibly is our commitment. In this way, we are based on the principles of information security, whose objectives are the preservation of the ownership of the information, notably its confidentiality, integrity and availability, allowing the use and sharing in a controlled manner, as well as the monitoring and treatment of incidents arising from attacks cybernetics.

Confidentiality: ensure that the information handled is the exclusive knowledge of specifically authorized persons;

Integrity: ensuring that information is kept intact, without undue modifications – accidental or deliberate;

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

4. CONFIDENTIAL INFORMATION

Access to confidential information, including personal data, collected and stored by the Group is restricted to professionals authorized to use this information directly, and necessary for the provision of their services, with limited use for other tasks, and must also comply with the provisions of Information Classification Standard.

The Group may disclose confidential information in the following cases:

- Whenever you are required to disclose them, whether by virtue of a legal provision, act of a competent authority, order or court order;
- To credit protection and defense bodies and service providers authorized by the Group to defend their rights and credits;
- To financial market regulators; and
- For other financial institutions, provided that within the legal parameters established for this purpose, in this case, the user may, at any time, cancel his authorization.

5. CYBER SECURITY 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.

5.1 MANAGEMENT OF ACCESS TO INFORMATION

Access to information is controlled, monitored, restricted to the smallest possible permission and privileges, periodically reviewed, and canceled in a timely manner at the end of the employee's or service provider's employment contract.

Equipment and facilities for processing critical or sensitive information are kept in secure areas, with appropriate levels of access control, including protection against physical and environmental threats.

The Group's employees and third parties are periodically trained on the concepts of information security, through an effective program of awareness and dissemination of the cybersecurity culture.

5.2 PROTECTION OF THE GROUP'S ENVIRONMENT

Controls and responsibilities are established for the management and operation of information processing resources, aiming to ensure the security of the Group's technological infrastructure through effective management in the monitoring, treatment and response to incidents, in order to minimize the risk of failures and the secure administration of communications networks.

5.2.1 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, the segregation of conflicting functions and the classification of information.

System access control must be formalized and include, at a minimum, the following controls:

- The use of identifiers (access credential) individualized, monitored and subject to blocking and restrictions (automated and manual);
- The removal of authorizations given to users who are far from or disconnected from the Group, or who have changed their role; and
- Periodic review of granted authorizations.

5.2.2 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.

5.2.3 Information Leakage Prevention

Use of data loss prevention control, responsible for ensuring that confidential data is not lost, stolen, misused or leaked onto the web by unauthorized users.

5.2.4 Intrusion Tests

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

5.2.5 Vulnerability Scan

Scans of internal and external networks should be performed periodically. The identified vulnerabilities must be treated and prioritized according to their level of criticality.

5.2.6 Control Against Malicious Software

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

5.2.7 Cryptography

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

5.2.8 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 creating or removing system objects.

5.2.9 Network Segmentation

- Computers connected to the corporate network must not be directly accessible from the Internet;
- Direct connection to third-party network using remote control protocols to servers directly connected to the corporate network is not allowed;
- To request the creation, change and deletion of rules in firewalls and network assets, the requester must submit a request to the IS area, which will carry out the analysis and approval, sending it to be executed by the IT area.

5.2.10 Secure Development

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

5.2.11 Backup

The process of performing backups is carried out periodically on the Group's information assets, in order to avoid or minimize data loss in the event of incidents.

5.3 BUSINESS CONTINUITY

The business continuity process is implemented in order to reduce the impacts and losses of information assets after a critical incident to an acceptable level, through the mapping of critical processes, business

impact analysis and periodic disaster recovery tests. This process includes business continuity related to the services contracted in the cloud and the tests foreseen for cyber-attack scenarios.

5.4 PROCESSING, DATA STORAGE AND CLOUD COMPUTING

Pursuant to Resolution 4,658/2018 (and its amendment 4,752/2019), of the National Monetary Council, for the contracting of data processing and storage and cloud computing services, the Group ensures an effective procedure for adherence to rules provided for in the regulations in force.

6. MAIN SAFETY RECOMMENDATIONS FOR CUSTOMERS and USERS

6.1 AUTHENTICATION AND PASSWORD

The customer is responsible for the acts performed with his/her identifier (login / acronym), which is unique and accompanied by a unique password for individual identification/authentication in accessing information and technology resources.

We recommend that:

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

6.2 ANTIVIRUS

We recommend that the customer keep an antivirus solution updated and installed on the computer used to access the services offered by the Group. Also, have the operating system updated with the latest updates performed.

6.3 SOCIAL ENGINEERING

Social engineering, in the context of information security, refers to the technique by which a person seeks to persuade another, often abusing the user's ingenuity or trust, aiming to deceive, apply scams or obtain confidential information.

6.3.1 PHISHING

Technique used by cybercriminals to deceive users by sending malicious emails in order to obtain personal information such as passwords, credit card, CPF, bank account number, among others. Approaches to phishing emails can occur in the following ways:

- When they seek to attract the attention of users, whether for the possibility of obtaining some financial advantage, whether out of curiosity or charity;

- When trying to pass through the official communication of institutions known as: Banks, e-commerce stores, among other popular sites;

- When they try to induce users to fill out forms with their personal and/or financial data, or even the installation of malicious software that aims to collect sensitive information from users;

6.3.2 SPAM

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

6.3.3 FALSE PHONE CONTACT

These are techniques used by fraudsters to obtain information such as personal data, passwords, token, cell phone identification code (IMEI) or any other type of information for the practice of fraud.

7. COMMUNICATION

Any evidence of irregularities in compliance with the provisions of this Policy will be subject to internal investigation and must be immediately communicated to our service channels.

8. DEFINITIONS

Affiliates: Companies in which the Company has significant influence (art. 243, paragraph 1, of Law no.6.404/76).

Company: XP Investments S.A.

Subsidiaries: Companies in which the Company is the Controlling Shareholder.

Grupo XP Inc.: The Company, its Subsidiaries and Affiliates incorporated in Brazil, considered together, including Banco XP and XP Investments.

Confidential Information: Any and all proprietary or non-proprietary information, verbal or otherwise presented, tangible or intangible, including but not limited to technical, operational, commercial, financial, legal, know-how, inventions, processes, formulas and designs, patentable or not, business plans, accounting methods, techniques and accumulated experiences, business plans, budgets, prices, expansion plans, business strategies, discoveries, ideas, concepts, techniques, projects, specifications , diagrams, models, samples, flowcharts, computer programs, codes, data, source codes, disks, diskettes, 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.