Information Security Policy for Vendors

TABLE OF CONTENTS

1. INTRODUCTION

The Information Security Policy for Suppliers/Third Parties and Business Partners ("Policy") aims to direct an effective program for protecting information assets, which will be the basis for establishing all Security standards and procedures. The Security policy establishes the Security requirements necessary for the approval of a service, product offered by the supplier, or business partnership by the Information Security area, before the start of the provision of the service, in cases where the supplier processes general or sensitive personal data of customers (e.g. Name, ID, Individual Taxpayer's Register (CPF), address, telephone, email), and employees (e.g. Name, ID, CPF, address, telephone, e-mail or related to an account and/or application of/or in the Cloud.

Information is one of the most important business elements for XP Inc. Group ("Group or XP Group") and, therefore, maintaining its confidentiality, integrity and availability are relevant factors for the Group's success. This document is intended for all employees who are part of the XP Inc. Group and any third parties/partners who use its infrastructure and who are involved in the design of solutions, systems, processes, products, or services.

2. SCOPE

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

3. RELATED DOCUMENTS

- Information Security Policy.
- Security Standard for Contracting and Acquiring Suppliers/Third Parties and Business Partners.
- Supplier/Third Party and Business Partner Assessment Procedure.

4. TERM OF EFFECTIVENESS, TERMINATION AND CYCLE OF REVISION

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

5. DEFINITIONS

XP Inc. Group.: XP Investimentos S.A., including subsidiaries in other countries, its Subsidiaries and Affiliates organized in Brazil, considered together, and XP US.

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.

API: Application Programming Interfaces - Sets of definitions and protocols that allow interaction between different software systems.

AppSec - Application Security: Area responsible for evaluating service provision/partnerships involving integrations or connections with systems/environment of the XP Inc. Group.

Privacy Area: Area responsible for evaluating service provision/partnerships that involve collecting, processing or sharing personal data and/or sensitive personal data.

Business areas: Internal areas of the XP Inc. Group is responsible for contracting suppliers and/or establishing business partnerships.

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

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).

Consent: Consent is one of the legal hypotheses for processing personal data and is essential to ensure the holder has control over their information. According to the Brazilian General Personal Data Protection Law (LGPD), consent must be:

a. Free: The data subject must have the option to consent or not, without coercion or negative consequences for not giving consent.

b. Informed: The data subject must be informed about what data is being collected, for what purpose and how it will be used. This includes information about sharing with third parties, if applicable.

c. Unequivocal: Consent must be expressed clearly, avoiding ambiguities.

Subsidiaries: The companies in which XP Investimentos S.A. is the Controlling Shareholder.

Data controller: Individual or legal entity, of public or private law, who shall make decisions referring to the treatment of personal data, notably the XP Inc. Group.

DAST: Dynamic Application Security Testing - Software security approach that analyzes a running application to identify vulnerabilities and security flaws.

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

EHT: Test Hacking Engineering: - Set of practices and methodologies used to evaluate and improve the security of systems, applications and networks through ethical hacking techniques. EHT aims to identify vulnerabilities and weaknesses in an IT environment before malicious attackers can exploit them.

Relevant Supplier/Third Party and Partner: A relevant supplier/third party and partner is one that, according to the analyses carried out by the Information Security (Information Security Governance) and Business Continuity team mentioned earlier in this document, is highly relevant to XP Inc. Group's technological scenario. To determine whether the scope of service provision is relevant, the supplier must

meet all of the following criteria: Processes general and/or sensitive personal data of customers and/or employees, provides processing/cloud storage services external to the Group and provides services that impact the business continuity of the XP Inc. Group. Development, consulting and auditing suppliers/partners are not classified as relevant suppliers/partners.

XP Inc. Group or XP: Companies controlled by XP Inc. and its Affiliates, incorporated in Brazil and the United States, considered together.

Hardening: It refers to strengthening the security of systems, networks and applications to reduce their vulnerabilities and minimize the risk of attacks. Hardening aims to create a secure configuration that protects information assets from unauthorized access and cyber threats.

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

Relevant incident: A relevant incident causes, directly or indirectly, a critical impact on the assets, services and information systems or computing resources of the XP Inc. Group, or that entails a relevant risk or damage to data subjects.

ISO 27001: It is an international standard that specifies the requirements for an Information Security Management System (ISMS) to protect sensitive information and ensure data confidentiality, integrity and availability.

NetSec - IS Architecture: Area responsible for evaluating service/partnership provision that involves some component of the supplier/partner's architecture in the XP Inc. Group environment.

Offer: The item can be ordered via XP Inc. Group Service Catalog.

Open Banking or Open Finance: Set of rules and technologies that allow sharing financial data and services between financial institutions and authorized providers.

Data operator: According to section II of article 5 of the LGPD, this is an individual or legal entity, of public or private law, who performs the treatment of personal data on behalf of the controller.

Opt-In: Opt-in is a consent model in which the data subject explicitly expresses their will for their personal data to be collected and processed. This means that the user needs to take active action, such as marking a box or clicking a button, to consent to using their data.

Opt-Out: Opt-out is the option to withdraw or refuse processing based on consent. Consent is presumed until the data subject decides to cancel it.

OWASP: Open Web Application Security Project (OWASP) Top 10 - a list of the top ten security risks in web applications published by the Open Web Application Security Project (OWASP). This list is widely recognized and used as a guide to help developers, security professionals, and organizations understand and mitigate the most critical vulnerabilities in their applications. The list is updated periodically to reflect changes in the threat scenario.

Business Partners: Partner Entities of the Group that have alliances and contractual ties.

Patches: Patch (or Software Update) is a set of software code changes applied to correct problems, improve functionality or increase system security. Software developers frequently release patches to address known vulnerabilities, bugs, and flaws that affect the software's performance or security.

Phishing: It is a technique used to steal information by sending fake emails and obtaining personal information such as passwords, credit cards, CPF, and bank account numbers.

PoC: Proof of Concept—This involves testing/validating the solution, system, process, etc., before the actual contract or partnership.

***Runbooks*:** Documents that contain detailed instructions on how to perform specific tasks, operational procedures, or incident response processes in IT environments. Operations, technical support, and information security teams often use them to ensure that activities are carried out consistently and efficiently.

SAST: Static Application Security Testing - A software security approach that analyzes an application's source code for vulnerabilities and security flaws before the software is executed. This technique is performed during the initial stages of development, allowing developers to identify and fix security issues proactively.

SecOps - BlueTeam: Area responsible for evaluating service/partnership provision involving access to web applications (website).

Self-Assessment: XP prepared an assessment matrix with Security and Privacy controls based on ISO 27001, good market practices and XP controls.

Service Desk N3: Area responsible for evaluating service/partnership provision that requires installation on the XP Inc. Group notebook/desktop.

SOC 2 Type 2: Framework for service organizations that demonstrates adequate controls for data security criteria.

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

Pentest: Penetration Testing - Information security practice that involves simulating cyber-attacks on systems, networks or applications to identify vulnerabilities that malicious attackers could exploit. Penetration testing aims to assess the environment's security and provide recommendations to mitigate risks.

6. GENERAL PROVISIONS

6.1. General

Suppliers/third parties or business partners must comply with all Brazilian and US legislation requirements, where applicable. They must also commit to fully complying with the following items and requirements:

- Protect information against unauthorized access, modification, destruction or disclosure, maintaining its confidentiality;
- Ensure that the resources made available to you are used only for the purposes approved by XP Inc. Group;
- Ensure that the systems and information under your responsibility are adequately protected under Security requirements;
- Ensure the continuity of processing of relevant business information;
- Comply with the laws and rules that regulate intellectual property aspects;
- Comply with the laws that regulate the activities of the XP Inc. Group and its market;
- Select information security mechanisms, balancing risk, technology and cost factors;
- Immediately notify XP Inc. Group of non-compliance with the Information Security Policy for Suppliers/Third Parties and Business Partners.
- All suppliers approved by XP Inc. Group must comply with the General Terms and Conditions of Supply (GTC) or have equivalent sections in the agreement. Contractual changes or safeguards must follow the process with Procurement, Agreement Management and Legal, in which, if necessary, they request validation from interested parties. Legal is responsible for including sections and safeguards when necessary.
- The GTC does not apply to international suppliers.
- Suppliers/Third Parties and Business Partners that store and/or process general and/or sensitive personal data of customers, employees or access the XP Inc Group environment, provide and/or make available the system and/or provision of cloud services must undergo a Supplier/Service Provider/Business Partner Assessment process, requiring, when applicable, a SOC 2 type 2 report or other independent audit report upon contracting, in addition to a vulnerability scan using a cyber health verification tool if this scope includes the sharing and/or processing of general and/or sensitive personal data.

7. RESPONSIBILITIES

7.1. Contracting Area for Supplier/Third Party Services and Partnerships

- When contracting suppliers/third parties or establishing partnerships that have employees who will access the internal network and data of the XP Inc. Group, the contracting area must ensure that everyone is aware of this Information Security Policy for Third Party Suppliers and Business Partners, as well as provide an XP notebook or Desktop as a service (DaaS) and an individual third party/partner user for the employees of the supplier/third party and partner.
- It is the responsibility of the business area to provide documentation for analysis, including, but not limited to, the SOC 2 type 2 report. For suppliers/third parties and relevant partners for whom SOC 2 type 2 is mandatory, if the supplier does not have the report, Corporate Risks will analyze it internally.

- It is the responsibility of the business area to ensure that all Information Security requirements have been met at the start of the supplier's service provision or the start of the partnership;

- Contact specialist areas to analyze and assess requirements by filling out the "Supplier/Service Provision/Business Partner Assessment" Offer available in the XP Inc. Group service catalog.

- Ensure that Legal area receives the appropriate information when validating contracts via the Agreements system, indicating the necessary details so that Legal area can include the appropriate regulatory sections.

7.2. Suppliers/Third Parties and Partners

- It is the responsibility of XP Inc. Group's Suppliers/Third Parties and Partners to observe and follow the guidelines established for compliance with this Information Security Policy for Third Parties and Business Partners;

- Third parties/partners who access XP Inc. Group environment, process general and sensitive personal data and/or sensitive information must be aware of this Policy.

- All activities performed must comply with current legislation and the regulations of regulatory bodies and entities regarding Information Security;

- The contracting of partnerships between institutions authorized to operate by the Central Bank of Brazil or in which the contracted partner acts on behalf of the contracting institution for the purposes of sharing data (Open Banking or Open Finance) is prohibited. For the possibility of contracting partnerships with entities not regulated by the Central Bank, the contracting must observe the requirements present in this document. In the case of participation for the purposes of sharing data and joint provision of services to the consumer, there must be prior and explicit consent from the customer.

It is mandatory to complete the XP Self-Assessment in the case of service provision or Call Center partnership.

7.3. Information Security (Information Security Governance)

- Evaluate and direct specialized areas of Information Security, as well as issue a consolidated opinion of the areas consulted so that the supplier/third party and partner implement the necessary recommendations for each type of specific product or service.

- The specialist areas of Information Security that can evaluate a service provision or partnership are: Privacy, SecOps - BlueTeam, NetSec - IS Architecture, AppSec - Application Security and Service Desk N3.

- Analyze the requirements of the request for hiring, partnership or any type of procedure for PoC or approval of products and services.

- Indicate, from an Information Security perspective, the relevant suppliers/partners that should be communicated to BACEN and SUSEP, with communication to these bodies being carried out by the Legal Department.

- Register all documentation corresponding to Information Security, including SOC 2 type 2 report review documents.
- Review relevant suppliers/partners based on SOC 2 Type 2 report at least annually.

7.4. Business Continuity

- Analyze the requirements of the new hiring request or any type of procedure for PoC or approval of products and services.
- Evaluate and provide a Business Continuity opinion so that the supplier implements the necessary recommendations for each specific type of product or service.
- Check suppliers' responses in scenarios where the product or service is unavailable.
- Review and indicate, with a Continuity perspective, which relevant Continuity suppliers should be communicated to BACEN and SUSEP, with communication to these bodies being carried out by the Legal area.
- Request signature and register all documentation corresponding to Business Continuity.

7.5. Compliance Offshore

- Intermediate communications or requests from regulatory entities (NFA, FINRA, SEC among others) applicable in the USA in audit cases.

7.6. Corporate Risks

- Evaluate Suppliers that present a high/extremely high risk to the XP Inc. Group or that do not meet Information Security requirements.

8. INFORMATION SECURITY REQUIREMENTS

8.1. CONDUCT OF SUPPLIERS/THIRD PARTIES AND PARTNERS WITHIN THE XP INC GROUP ENVIRONMENT

8.1.1. Logical Access and Acceptable Use

- Logical access to the XP Inc. Group's internal network environment must be requested by the manager responsible for the contract or partnership, through the XP Service Catalog tool. The request will be evaluated and approved as necessary, following corporate Information Security guidelines.
- For suppliers/third parties and partners who need to access the XP Inc Group environment remotely, the manager responsible for the contract must provide an XP notebook or Desktop as a Service (DaaS) with access through a single and individual user, limited to the work resources and environments necessary to perform their functions;

- It is the duty of the manager responsible for the supplier/third party and partner to inform the validity of the service provision or partnership contract at the time of requesting access, as well as to request the deletion of access when there is no longer a need for it;
- The use of supplier/third party and partner computers and/or personal/corporate computers is prohibited.
- Access, download or distribution of any content that violates copyright and property rights within XP Inc. Group network is prohibited. Likewise, access to or distribution of pornographic content of any nature or content that violates the Statute of Children and Adolescents is not permitted;
- When applicable, the username and password made available to the supplier/third party and partner are for exclusive use and cannot be disclosed or shared;
- The supplier/third party and partner must keep their access credentials secure, and will be responsible for any improper use;
- It is the responsibility of the third party/partner company to communicate any dismissal of its employees so that they have their access duly cancelled in the XP Inc. Group environment; and
- Sharing usernames and passwords is prohibited.

8.1.2. Information Security Incident Notification

Information Security incidents and non-conformities that are known to the third party/partner must be immediately communicated to the contract manager so that they can conduct the incident notification process through formal means.

Once opened, the triage, analysis, treatment and response process follows the same flow as internal incidents at XP Inc. Group.

For details on the types of incidents and their criticalities, see Exhibit I of this Policy.

8.1.3. Equipment Safety

- Each user is responsible for the protection and physical integrity of the physical or virtual devices containing XP Inc Group information that are under their care; and
- Each user must be aware that the use of any IT resource in the XP Inc Group environment is subject to inspection, whenever local law permits.

8.1.4. Conduct Violation

The following situations, without limitation, are considered violations of this Policy:

- Any actions or situations that may expose XP Inc. Group to financial and image loss, directly or indirectly, potential or real, compromising its information assets;

- Misuse of corporate data, unauthorized disclosure of information, trade secrets or other information without the express permission of XP Inc. Group;

- Use of data, information, equipment, software, systems, codes or other technological resources for illicit purposes that may include violation of laws, internal and external regulations, ethics or requirements of regulatory bodies in the area of operation of the XP Inc. Group; and

- Failure to immediately report any breaches of the Policy.

8.2. SECURITY AND PRIVACY CONTROLS IN THE SUPPLIER/THIRD PARTY AND PARTNER ENVIRONMENT

If the service provision involves sharing and/or processing of general and/or sensitive personal data, the supplier/partner in question will be registered by the Information Security Governance team in a cyber-health verification tool, which analyzes the vulnerabilities exposed to the internet from a domain. This platform provides a Security Score with 5 classification levels (A, B, C, D and F), where score A is the maximum score.

At a minimum, the overall score of this supplier/third party and provider must be B, receiving a suitability and compliance report in order to achieve score A. If it does not achieve the minimum result for the provision of its service, it will be rejected by the Information Security Governance team, until it implements the necessary improvements generated by the platform's recommendation plan or is approved in an extraordinary manner by the company's Corporate Risk team, duly formalized. If the supplier does not have its own domain, the analysis will be waived.

The supplier/third party and partner that offers cloud services, processes and/or stores data from the XP Inc. Group in its environment, must follow the following Information Security guidelines, set out in this policy:

8.2.1. Privacy

- Present, through documentation, the data flow from the XP Inc. Group in the supplier/third party and partner environment, containing its entire life cycle (collection, processing, storage, sharing and deletion).

- Inform the XP Inc. Group what information is collected, for what purpose, what legal hypothesis is used to base the processing of the data, where it is stored and for how long, as well as minimizing it whenever possible.

- Have an impact assessment related to the general and/or sensitive personal data of a data subject (RIPD/DPIA), as well as have a process that grants XP unrestricted access to its processed and stored information, as provided for in the scope of the service provided.

- Have an opt-in and opt-out process for the data owner to express their views in advance and freely about sharing through the provision of a service/partnership.

- For Open Banking or Open Finance suppliers, it is prohibited to enter into partnerships with the aim of the contracted partner acting on behalf of the contracting institution for sharing purposes.

8.2.2. Access Control

- Have a documented Access Management process;
- Grant unrestricted access to XP Inc. Group to data and information stored or to be processed by XP Inc. Group, in accordance with the specific services defined, valuing the confidentiality, integrity, availability and recovery capacity of this data and information;
- Provide visibility to the procedures and controls used to provide services, as described in the item above, in particular, for the identification and segregation of the Group's data, through physical or logical controls;
- Limit the use of shared accounts or generic users, maintain login-related controls, such as forcing password changes on first access, blocking the user with certain invalid attempts, requiring a complex password pattern, among others;
- Have a formalized process for granting, changing and revoking access, especially those with privileged actions.
- Establish methods for controlling physical and logical access of visitors; and
- Have VPN controls and similar for remote access by employees.

8.2.3. Vulnerability Management

- Prevent, detect and reduce vulnerability to incidents related to the cyber environment, demonstrating its best efforts using procedures and controls that cover, at a minimum, authentication, encryption, intrusion prevention and detection, data leak prevention, periodic testing and scanning to detect vulnerabilities, application of security patches, application of hardening to its servers and workstations, protection against malicious software and blocking of non-approved software, establishment of traceability and segmentation mechanisms for the computer network, maintenance of backup copies of data and information.

8.2.4. Service Monitoring and Incident Management

- Ensure that it has the highest capacity level in the provision of information and management resources to monitor the services to be rendered, as well as to ensure compliance with legislation and regulations in force, besides adhering to all the certifications required by XP Inc., as described in topic 8.2.8, and/or BACEN for the execution of the contracted services; and
- Inform and provide access to XP Inc. Group, when requested, to the management resources appropriate for monitoring the contracted services.
- Have dedicated teams and tools to monitor the capacity and availability of your assets, correlating alerts and generating incident alerts automatically;
- Have a structured Incident Response process, including the categorization of incidents and runbooks for handling and resolving known incidents.

- Provide, whenever requested, information related to the number of incidents that took place in the period of 12 months, classifying them by their relevance.

- Keep the XP Inc. Group permanently informed about any limitations that may affect the provision of services or compliance with current legislation and regulations.

8.2.5. Security in Systems Development

- Develop considering the security and privacy standards (within General Data Protection Law scope) accepted by the market (Privacy and Security by Design);

- Describe the security features and data accessed by the applications, which must be evaluated by the Information Security area (AppSec - Application Security) during the approval phase (Ex: Technical specification and/or Functional Diagram);

- Use integrity validation routines to prevent errors, whether involuntary or intentional, using fictitious data, anonymization and masking in a non-production environment;

- Perform security analysis with SAST/DAST tools on the source code;

- Perform security analysis on your applications (EHT and intrusion tests);

- Provide security validations in the quality and code verification process. At a minimum, those listed in the OWASP TOP 10, as detailed in the "Secure Development Standard" document, should be considered.

- Provide, in the case of customer routing platforms, minimum requirements described in CVM resolution 35 art. 18 and perform pentests on a biannual basis, as well as share all test reports with XP Group Inc.

- Have mechanisms to protect APIs.

8.2.6. Business Continuity, Data Management, Retention and Storage

- Define a business continuity program to ensure that possible incidents do not affect the services provided to the XP Inc. Group, especially considering the disaster recovery plan, with regular testing of assurance controls in order to verify how prepared the Supplier/Third Party and Partner company is for real cases;

- Inform and provide access to XP Inc. Group, when requested, about the security measures for the transmission and storage of data and information, as well as their disposal, using secure deletion procedures (media and paper);

- Have a backup execution process, which is carried out periodically on assets that store XP Inc. Group information, in order to avoid or minimize data loss in the event of incidents;

- Have a database with an audit trail enabled for access and commands to assets that store information from XP Inc. Group;

- Assets that store XP Inc. Group information must have personal data encryption.

8.2.7. Training and Awareness

- Have an annual Information Security and Data Privacy awareness training program for all employees, including the mandatory application of the supplier's Code of Conduct for newly hired employees.

- Include in your Data Security and Privacy training and awareness program, campaigns such as phishing, guidance on social engineering, external lectures, Information Security and Data Privacy newsletters, etc.

8.2.8. Services and Certifications

- Notify immediately about the subcontracting of relevant services to XP Inc. Group.

- Comply with, whenever the cloud computing and/or data storage services are rendered in primary locations abroad, existing agreement between BACEN and the inspection authorities of the countries where the services may be rendered, ensuring that the provision of the mentioned services will not cause harm to its operation, nor obstacles to BACEN activities.

- It is desirable to have information security or business continuity recognition, proven by certification. and/or independent external audit reports, which may be the SOC 2 type 2 report. In the case of a supplier/third party and relevant business partner, it is mandatory to have and make available to XP Inc. Group the SOC 2 Type 2 report.

- Inform and provide access to XP Inc. Group, when requested, about the certifications required for services, as well as reports related to the controls used in the provision of contracted services, prepared by a specialized independent auditing company. and

- Have mechanisms to communicate anomalies or relevant security incidents to XP Inc. Group, the individuals involved and the National Data Protection Authority (ANPD) for cases in which the supplier/third party and business partner acts as Controller. In cases of Data Operator, in incidents involving data in which XP Inc. Group is the Controller, the supplier/third party and business partner must immediately notify the Group, as described in topic 8.2.4. Communication to the regulator is prohibited in cases where the Data Controller is XP Inc. Group.

9. CORPORATE RISK MANAGEMENT

The specialist areas of Supplier Management, Legal, Information Security and Business Continuity define, with an independent view, the level of risk in the provision of services. The risk level varies between low, medium, high and very high. If one of these areas reports that, in their view, the supplier/third party and partner poses a high or very high risk, the Corporate Risks team is called upon even if there is no rejection. The independent risk view does not define the final risk of service provision.

If a supplier/third party and partner does not meet the required requirements/documentation, presents weaknesses that expose the XP Inc Group to risks or has a high/very high risk determined by specialist areas, an internal analysis will be carried out with the Corporate Risks area, contract manager and

other applicable areas to address the appropriate response to the risks or definitive rejection of the provision of the service or partnership.

10. NON-COMPLIANCE WITH REGULATIONS, PROCESSES OR WORK INSTRUCTIONS RELATING TO SECURITY

Non-compliance with the Information Security policies, standards, and procedures will trigger the initiation of a procedure to investigate potential irregularities ("Information Security Incident") and, depending on the case, will lead to the application of applicable penalties, in accordance with current legislation, such as notifications, warnings, or even the termination of the employment contract, internship, or service agreement, with the awareness of the responsible manager.

It is important to note that repeat offender employees (specifically within the same category/nature of the incident) are referred to the Compliance team, to have guidance, warnings, and/or other appropriate measures recorded. All actions taken by the Compliance team impact (based on the chosen penalty model) directly on the employee's Conduct Score.

Access and permissions that are not in line with the guidelines established in this Regulation must be granted on an exceptional basis in accordance with the Exception Handling Procedure managed by Corporate Risks.

The rules established herein must be widely disseminated and periodically reviewed with those who may be affected by their guidelines. At no point will any employee be allowed to claim ignorance of the Information Security guidelines as a justification for violations or non-compliance.

11. EXHIBIT I

Event Matrix and Information Security Incident Classification.

Level	Risk Characteristic	Category	Reporting deadline	Procedure to adopt
Very High	Problems faced or anticipated have the potential to disrupt all relevant operations and processes for an extended period of time. Event that involves significant financial damage, massive breach of client financial confidentiality or direct access to information considered relevant.	External Attacks Misuse or internal abuse Leak or theft Service interruption Human Error Vulnerabilities Others	Within 2 hours of identification	Communicate by e-mail the person responsible for intermediating the contract between the Vendors and XP Inc.
High	Observable degradation of key services and relevant processes is likely to occur with the potential to affect organizational value or reputation. Breach of clients' financial confidentiality in isolation or direct access to information considered restricted.	External Attacks Misuse or internal abuse Leak or theft Service interruption Human Error Vulnerabilities Others	Within 6 hours of identification	
Medium	There is likely to be a measurable impact on relevant operations and processes, but the risk of affecting organizational value or reputation is considered low. Event that, if not properly treated, could evolve into a high-risk situation.	External Attacks Misuse or internal abuse Leak or theft Service interruption Human Error Vulnerabilities Others	Within 24 hours of identification	