Cyber Security Policy

Prepared by FacilitaPay's Legal Team in May 2023.

1. PURPOSE

To establish the principles, guidelines and attributions related to information security, protecting the information of the institution, customers, and the general public, observing the best market practices and applicable regulations.

2. TARGET AUDIENCE

Employees of the FacilitaPay Group ("FacilitaPay"), regardless of the country in which they are located. Employees are:
• Partners and shareholders • Directors • Employees • Interns • Minor apprentices • Clients and/or individuals/legal entities that have a commercial relationship with FacilitaPay.

3. INTRODUCTION

Information is one of the main assets of the institution. Thus, FacilitaPay defines the Information Security and Cyber Security strategy to protect the integrity, availability and confidentiality of information. This strategy is based on incident detection, prevention, monitoring, and response that strengthens cybersecurity risk management and building a robust foundation for FacilitaPay's increasingly digital future.

To achieve this goal, we used the expanded perimeter protection strategy. This concept considers that information must be protected regardless of where it is, whether internally, in an affiliate, in a service provider or in an international unit, throughout its life cycle, from collection to disposal.

4. PRINCIPLES OF INFORMATION SECURITY

Our commitment to the proper treatment of FacilitaPay's information, customers and the general public is based on the following principles:

- Confidentiality: ensure that access to information is obtained only by authorized persons;
- Availability: ensure that authorized persons have access to information whenever necessary;
- Integrity: ensure the accuracy and completeness of the information and the methods of its processing, as well as transparency in dealing with the publics involved.

5. GUIDELINES

All information security policies must be available in a place accessible to employees and protected from change. Information security policies are reviewed annually by FacilitaPay with application in Brazil and abroad.

The inclusion of guidelines or exceptions by regulatory requirement and the publication in the units abroad, will be identified by the responsible for information security of the unit, who must formalize and submit in advance the proposal of guidelines or exceptions for approval by the Corporate Security Board.

Adherence to this Policy and any deviations, in Brazil and in units abroad, are reported periodically by the Corporate Security Department to the Executive Committee, Compliance Committee and other risk committees.

The information must be used in a transparent manner, for the purposes informed to the customer and in accordance with current legislation. The guidelines and any exceptions are complemented in procedures with specific rules that must be observed.

6. INFORMATION SECURITY PROCESSES

To ensure that the information processed is adequately protected, FacilitaPay adopts the following processes:

a) Asset Management

An asset is understood as anything that the institution considers as relevant to the business, from technological assets (e.g. software and hardware) to non-technological assets (e.g. people, processes and physical dependencies) as long as they are related to the protection of information. Assets, according to their criticality, must be identified, inventoried, kept up to date, have an owner, dispose of securely and be protected from improper access. Protection can be both physical (e.g., access-controlled rooms) and logical (e.g., shielding or hardening settings, patch management, authentication, and authorization). The assets of FacilitaPay, customers and the general public must be treated ethically and confidentially and in accordance with current laws and internal regulations, promoting the proper use and preventing undue exposure of information.

b) Classification of Information

Information should be classified according to confidentiality, according to internal policies. For this, the needs related to the business, the sharing or restriction of access and the impacts in the event of misuse of the information must be considered. According to the classification of confidentiality, the necessary protections should be established throughout its life cycle. The information lifecycle comprises: Generation, Handling, Storage, Transport and Disposal.

c) Access Management

Access grants, reviews and deletions must use FacilitaPay's corporate tools and processes. The accesses must be traceable in order to allow the individual identification of the employee or service provider who has accessed or changed the information, allowing their accountability. The granting of access must comply with the criterion of least privilege, in which users must have access only to the information resources essential for the full performance of their activities and duly authorized. Segregation of duties should permeate all critical processes, preventing a single person in charge from being able to execute and control the process throughout its lifecycle. The identification of any employee must be unique, personal and non-transferable, qualifying him as responsible for the actions carried out. The password is confidential, personal and non-transferable information, must be used as an electronic signature, and its sharing is prohibited.

d) Risk Management

Risks must be identified through an established process for analyzing threats, vulnerabilities, probabilities and impacts on those of FacilitaPay, so that appropriate protections are recommended. Recommendations are discussed in the appropriate forums. Products, processes and technologies must have the appropriate management of Information Security risks, to reduce risks to acceptable levels, regardless of whether they are within the infrastructure of FacilitaPay, partners or service providers. The technologies in use by the institution must be in versions supported by their manufacturers and duly updated. Any exceptions must be approved in the competent authority or have compensatory controls.

e) Risk Management in Service Providers and Partners

The service providers and partners hired by FacilitaPay must be classified considering some criteria, according to the internal document. Depending on the classification, the service provider or partner will undergo risk assessment, which may include on-site validation of IS controls, remote evaluation of evidence or other assessments, as well as monitoring of any corrections and improvements implemented by service providers and partners. Service providers and partners must report relevant incidents (as defined in item 6.f of this Manual) related to FacilitaPay information stored or processed by them in compliance with legal and regulatory determinations.

f) Treatment of Information Security and Cyber Security Incidents

The Cyber Security area monitors the security of FacilitaPay's technological environment, analyzing events and alerts to identify possible incidents. The incidents that are identified by the alerts are classified with respect to impact, according to the criteria adopted by FacilitaPay. For its degree of relevance will be considered aspects such as impact on the financial system and compromise of customer data and the general public. Incidents classified as relevant must be reported to the Regulator, the data subject, and the Compliance Committee, when they involve personal data that may entail risk or cause material damage to the holders. All incidents go through a process of treatment and communication, where all the information pertinent to the incidents such as cause, impact, classification, etc. are recorded.

Information on incidents that may impact financial institutions in Brazil should be shared with other institutions, in order to collaborate with risk mitigation according to legal and regulatory determinations. Abroad, the management of information security and cyber incidents is carried out by the International Unit, which must report them in a timely manner to the Corporate Security Directorate in Brazil.

The Risk area will prepare an Annual Report containing the relevant incidents that occurred in the period, actions taken to prevent and respond to incidents and results of continuity tests. This report shall be submitted to the Risk Committee and the Board of Directors, in accordance with legal and regulatory determinations. In order to improve incident response capacity, FacilitaPay conducts business continuity tests simulating scenarios of critical Cyber Security incidents, which may compromise the availability and/or confidentiality of information. Every employee must be proactive and diligent in identifying, communicating to the Information Security area and mitigating risks related to information security.

g) Information Security and Cyber Security Awareness

FacilitaPay promotes the dissemination of Information Security principles and guidelines through awareness and training programs to strengthen the Information Security culture. Periodically, awareness campaigns or training are made available that may be face-to-face or online, related to confidentiality, integrity and availability of information. These campaigns are conveyed through emails, corporate portal, e-learning, media or social networks to employees and customers.

h) Governance with the Business and Technology Areas

The initiatives and projects of the business and technology areas must be aligned with the principles and guidelines of information security.

i) Physical Security of the Environment

The Physical Security process establishes controls related to the granting of physical access to the environments, according to the criticality of the information treated in these environments, as described in the internal documents.

j) Safety in the Development of Application Systems

The systems development process should ensure adherence to the institution's internal documents and good security practices. Productive environments should be segregated from other environments and with access only via application by previously authorized users or approved tools.

k) Log Recording

It is mandatory to record logs or audit trails of the computing environment, for all platforms, in order to identify: who made the access, when the access was made, what was accessed and how it was accessed. This information must be protected against unauthorized modifications and access.

l) Cyber Security Program

FacilitaPay's Cyber Security Program is guided by the following principles: • Current regulations; • Best practices; • World scenarios; • Risk analysis of the institution itself. According to its criticality, the actions of the program are divided into: • Criticisms: Consists of emergency and immediate corrections to mitigate imminent risks; • Support: Short/medium term initiatives to mitigate risk in the current environment, keeping the environment safe, respecting the risk appetite of the institution and allowing long-term/structuring actions to be carried out; • Structuring: Medium/long-term initiatives that address the root cause of risks and prepare the company for the future.

m) Perimeter protection

To protect FacilitaPay's infrastructure against an external attack, we use, at a minimum, tools and controls against: DDoS, Spam, Phishing, APT/Malware attacks, intrusion of network devices and servers, application attacks and external scanning. To mitigate the risk of information leakage we use preventive tools installed on mobile devices, workstations, in the electronic mail service, in the web browsing service, in the printing service, in addition to the use of encryption for data at rest and in transport. In order to increase protection, physical or logical connection to the institution's corporate network by unmanaged or unapproved private equipment is not allowed.

n) Governance with International Units

International units must have an information security officer, independent of the business and technology areas, who reports to the Corporate Security Department.

6.1 Intellectual Property

Intellectual property is the protection that falls on intangible goods, such as: trademarks, distinctive signs, advertising slogans, domain names, business names, geographical indications, industrial designs, invention and utility model patents, intellectual works (such as literary, artistic and scientific works, database, photographs, drawings, illustrations, architectural projects, musical works, audiovisual works, texts and etc.), computer programs and business secrets (including trade and industry secrets). Any and all inventions, creations, works and improvements that have been or will be created or made by the employee to FacilitaPay, in the capacity of administrator, employee and/or intern, during the entire term of the employee's mandate, employment contract or internship contract, belong exclusively to FacilitaPay. Any information and content whose intellectual property belongs to FacilitaPay, or has been made available by it, including information and content that has been obtained, inferred or developed by the employee himself in his work environment or using company resources shall not be used for private purposes, nor passed on to third parties, without prior and express authorization from FacilitaPay. It is the duty of all employees to ensure the protection of FacilitaPay's intellectual property. 6.2 Statement of Responsibility Periodically FacilitaPay employees must formally adhere to a term, committing to act in accordance with Information Security policies. The contracts signed with FacilitaPay must have a clause that ensures the confidentiality of the information.

7. ROLES AND RESPONSIBILITIES

The corporate policies, strategies and processes of Information Security are supervised in Brazil and abroad by the Corporate Security Department and discussed in the specific risk forums of the areas and in the Executive Committees that deal with Operational Risk or Technology.

7.1 Internal Controls The roles and responsibilities of Internal Controls are described in the following FacilitaPay Manuals:

- FacilitaPay Code of Conduct;
- FacilitaPay money laundering prevention policy.

7.2 Corporate Security

• Improve the quality and effectiveness of its processes, seeking the integrity, availability and confidentiality of information; • Protect information from threats seeking to ensure business continuity and minimize risks to the business; • Establish, implement, operate, monitor and ensure the continuous improvement of the information security management system. • Define and formalize the objectives, controls and strategy of information security governance, together with the Executive Committee on Information Security. • Coordinate actions to achieve the objectives and strategy of information security governance approved by the committees, involving the responsible areas. • Establish and disseminate a culture of information security. • Propose investment for information security. • Define the information security policies and standards to be applied in the processes, products and technologies. • Define minimum security standards for International Units and Controlled Companies in Brazil and abroad and Entities maintained or managed by FacilitaPay, ensuring alignment with the information security objectives defined by the company.

7.3 International Units

They should proactively act in the identification, prevention and correction of risks and report periodically to the Corporate Security Department.

7.4 Related Companies and Entities

Related companies controlled in Brazil and abroad and entities maintained or managed in relation to FacilitaPay must evaluate the guidelines and requirements established in this policy and its annexes, periodically reporting to the Corporate Security Board the risks identified, adapting their internal security procedures according to their business segment and risk appetite. These companies must be classified and have a governance model based on risk assessment, which considers the following aspects: Impact on the image of Society, Model of Architecture and Connectivity with Society, and Volume of sensitive data stored. This governance model can vary between evaluation and direct monitoring of adherence to the defined controls or following a declaration of adherence to be carried out by the company itself.

7.5 Information Security Executive Committee

Must prove the strategy, objectives, budget and actions necessary for the mitigation of the risks of information security processes.

7.6 Technology Area

Keep the technology park available and updated with the safety standards implemented, within the deadlines compatible with the levels of risks.

7.7 Business Area

Protect FacilitaPay's information under your responsibility.

8. DISCIPLINARY SANCTIONS

Violations of this policy are subject to disciplinary sanctions provided for in the internal rules and legislation in force where the companies are located.

9. RELATED DOCUMENTS

This Corporate Information Security Policy is complemented by specific Information Security procedures in accordance with legal and regulatory aspects and approved by the Superintendence of Governance and Cyber Security Projects and Cyber Security Operational Superintendence, subordinated to the Corporate Security Department, within the structure of FacilitaPay's Risk and Finance Area.

9.1 Frameworks and Regulations

• Resolution 4,658 of the Central Bank Resolution 4,752 of the Central Bank General Law of Protection of Personal Data - Law No. 13,709/2018 10. •

10. GLOSSARY

• APT (Advanced Persistent Threat): Advanced persistent attacks. Cyber Security: is the term that designates the set of means and technologies used in the defense of information systems, infrastructure, computer networks and / or personal devices, in order to prevent damage, theft, intrusion, alteration or destruction of information. Relevant Damage: Action that may impact the privacy of the individual, and may cause high risk to their physical or moral integrity. Technology park: set of infrastructure assets and technology systems. Segregation of duties: consists of the separation of activities between areas and people potentially conflicting or who have privileged information, in which the employee can not exercise more than one function in the processes of authorization, approval, execution, control and accounting.

11. INFORMATION SECURITY COMMUNICATION CHANNELS IN BRAZIL:

• Received a suspicious email and want to send it for review? Forward email to: legal@facilitapay.com • Suspected information security incidents? Forward email to: legal@facilitapay.com

This document was machine-translated to the English Language. In case of an identified discrepancy, the original writing, in the Brazilian Portuguese, shall be considered as standard.