OPERATIONAL RISK POLICY

PAGSEGURO INTERNET S.A.

Effectiveness and Update

This policy is valid for one (1) year from the date of last review indicated in the chart above, and it must be reviewed and updated before it expires, in the events of changes to the applicable law and/or strategic instruction provided by PagSeguro Internet S.A. (“PagSeguro”).

1. PURPOSE

This operational risk policy ("Policy") has the purpose to establish guidelines and principles associated to the structure and to the operational risk management process of PagSeguro Internet S.A. ("PagSeguro"), in the capacity of payment institution authorized to operate by the Brazilian Central Bank ("Central Bank"), pursuant to the provisions set forth in Circular No. 3.681, dated November 4, 2013 ("Circular 3681/13").

2. COVERAGE

This Policy applies to all employees, processes and areas of PagSeguro, regardless of its structuring as physical or virtual units, and/or the form of access, whether local or remote, to PagSeguro's environment.

3. PURPOSE

Operational risk management is intended to identify, assess, monitor, control and mitigate the operational risks which PagSeguro is subject to, in order to improve its internal procedures, control of its performance and sustainability of its earnings.

In order to achieve such purposes, this Policy shall be disclosed to and complied with by all of PagSeguro's employees, from all levels, according to the roles and responsibilities established herein.

4. DEFINITION OF OPERATIONAL RISK

For categorization purposes, PagSeguro uses the same definitions adopted by the Basel Committee and article 2 of Circular 3.681/2013, and defines operational risk as the possibility of losses as a result of the following events: (i) failure, deficiency or inappropriateness of internal processes, personnel and systems; and (ii) external events, including legal risk associated to the inappropriateness or deficiency of executed agreements, as well as sanctions due to non-compliance with legal provisions and indemnification for damages to third parties arising from the activities performed by a payment institution.

Taking into account PagSeguro's concern on its reputation, risks to its image have been included in the definition of operational risks. Accordingly, the impacts on the institution's reputation will be analyzed under the operational risk management structure.

4.1. Risk categorization

Pursuant to the provisions set forth in article 2 of Circular 3.681/2013, events related to losses arising from operational risk are divided into eleven categories, as follows:

a) Failures in protection and security of sensitive data related both to end users' credentials and the other information exchanged with the purpose of performing payment transactions;

b) Failures in identification and authentication of end users;

c) Failures in authorization of payment transactions;

d) Internal frauds;

e) External frauds;

f) Labor claims and deficient security at workplace;

g) Inappropriate practices related to end users, products and payment services;

h) Damage to its own physical assets or to the physical assets currently in use by the institution;

i) Events resulting in the interruption of activities performed by the payment institution or interruption of payment services;

j) Failures in information technology systems; and

k) Failures in the execution, meeting deadlines and management of activities involved in payment arrangements.

5. RISK MANAGEMENT STRUCTURE

PagSeguro's operational risk management structure covers the implementation and maintenance of the procedures established herein as described in item 6 below, which allow the identification, assessment, monitoring, control and mitigation of such risks, according to the responsibilities established herein.

6. RISK MANAGEMENT PROCEDURES

PagSeguro's operational risk management will be performed based on the summarized procedures below, among other procedures that may be approved by the Board of Executive Officers:

a) Identification, assessment, monitoring, control and mitigation of operational risk in PagSeguro's processes and systems;
b) Documentation and storage of information related to losses associated to operational risk;
c) Preparation, on an annual basis, of reports that allow the timely identification and correction of operational risk control and management deficiencies;
d) Performance of assessment tests of the implemented operational risk control systems;
e) Disclosure of this Operational Risk Management Policy to employees of all levels of the institution;
f) Protection and security mechanisms for stored, processed or transmitted data;
g) Protection and security mechanisms for networks, websites, servers and communication channels in order to reduce vulnerability to attacks;
h) Procedures to monitor, trace and restrict access to sensitive data, network, systems, databases and security modules;
i) Monitoring of failures in security of data and claims made by end users in this regard;
j) Review of data secrecy and security measures, especially after the occurrence of failures and before changes to infrastructure or procedures;
k) Preparation of a contingency plan comprising the strategies to be adopted in order to ensure that activities will continue to be performed and limit critical losses resulted from operational risk;
l) Implementation, maintenance and disclosure of communication and information structured process; and
m) Mechanisms to monitor and authorize payment transactions, in order to prevent frauds, detect and block suspicious transactions on a timely basis.

6.1. Process mapping

Process mapping refers to the identification and description of the company's processes, which provides a perspective based on processes and their internal or external relations instead of a perspective based on an

organizational chart/hierarchy. Such mapping is based on the risk and control dictionary, and it will be periodically reviewed, whenever material changes are made to the processes.

Risks, by their turn, are included in a risks dictionary, which refers to a list that relates risks to a major risk that has been analyzed (operational, liquidity, credit, market, legal etc.), as well as provides a description to such risks. PagSeguro defines all risks it has acknowledged and recognized in such list.

After process mapping, operational risks existing in the process are assessed, as well as the controls that are necessary to mitigate them, which process is known as risk mapping.

6.2. Control assessment

Controls are periodically assessed and, if necessary, action plans are established to solve any weaknesses found.

6.3. Incidents and failures

Any material incident or operational failure will be analyzed, as well as their impacts and their root cause will be identified, thus allowing the mitigation of similar events in the future or the full or partial acceptance of the risk.

6.4. Crisis management

Activities and critical areas will establish and implement their Business Continuity Plans, so that their processes are maintained or recovered in the event activities are fully or partially interrupted.

6.5. New products and services

Development process for new products or services will include the analysis of operational risks arising from their release.

6.6. Reports

Main operational risks identified, both potential and materialized risks, will be reported to the Risk Committees, as well as information on relevant action plans and Operational Risk Management indicators.

7. ROLES AND RESPONSIBILITIES

7.1. Chief Risk Officer

The statutory officer responsible for risk management before BACEN ("Chief Risk Officer") shall ensure that all the tasks described herein are accurately complied with and within proper term. His/her main responsibilities include:

a) To effectively establish and maintain the operational risk management structure within PagSeguro;
b) To disseminate the view, culture and concepts of the operational risk management throughout the institution;

c) To establish guidelines, methodologies, tools and forms to identify, assess, measure, monitor, mitigate and control operational risks;
d) To lead and perform regular processes to assess risks and controls within PagSeguro;
e) To monthly report the operational risk status and material events of loss within PagSeguro to the Executive Board;
f) To produce regulatory and managerial reports related to operational risk management; and
g) To ensure compliance with the regulations.

7.2. Managers

Each of PagSeguro's managers – employee responsible for one process, holding a non-specialized managerial position – is responsible for risk management of his/her areas, processes, systems and/or products. His/her main responsibilities include:

i. To ensure that all employees understand the risks and responsibilities involved in their daily activities, and that they comply with operational risk policies;
ii. To identify, assess, control and monitor the operational risks of their areas, processes, products and systems through methodologies offered by the operational risk management area;
iii. To timely report material information to the operational risk management area;
iv. To ensure that maps and processes and any other key documents of the area or the process are aligned with the operational risk policies and guidelines, assuring update and maintenance mechanisms of such documents;
v. To report any operational losses and other information requested by the operational risk management area;
vi. To ensure that all activities related to operational risk management are performed and that their results are reported to the superior in charge; and
vii. To ensure the conciliation of managerial information on operational losses reported to the operational risk area.

8. EXHIBITS

None.