BUSINESS CONTINUITY POLICY (“BCP”)

PAGSEGURO INTERNET INSTITUIÇÃO DE PAGAMENTO S.A.

LEADER OF THE PRUDENTIAL CONGLOMERATE

Validity and Update

This Policy is valid for 2 (two) years as of the last revision date included in the table at the end of the document. It must be revised and updated before its maturity and in the event of changes in the applicable legislation and/or strategic guidance of the prudential conglomerate of PagSeguro Internet Instituição de Pagamento S.A.

1. INTRODUCTION AND PURPOSE

1. Introduction

This **Business Continuity Policy** (“BCP” or “Policy”) of **PagSeguro Internet Instituição de Pagamento S.A.** (“PagSeguro”), the leading institution of the Prudential Conglomerate, **BancoSeguro S.A.** (“BancoSeguro”) **PagInvest Corretora de Títulos e Valores Ltda.** (PagInvest CTVM), and **Wirecard Brazil Instituição de Pagamento S.A** (MOIP), institutions belonging to PagSeguro’s prudential conglomerate and collectively referred to as (“Companies”), was prepared based on current legislation and regulations issued by the Central Bank of Brazil (“BACEN”) and other regulatory entities, as well as best market practices.

Based on the concepts, principles, and guidelines established in this Policy, the Companies strengthen the risk management structure and corporate governance in Business Continuity, providing more security to their employees, clients, and shareholders in the face of unforeseen events, as well as seek to ensure an adequate level of organizational stability in the aftermath of any interruptions and throughout the recovery process.

1.2 Purpose

The purposes have been defined to support and maintain the security of the Companies' business processes, ensuring they return to their normal operational condition within an acceptable timeframe in the event of an incident. These purposes are measured through indicators and monitoring:

- % of the efficiency of Business Continuity Plans, identifying possible internal impacts that may compromise the continuity of the Companies;
- % of Load Tests conducted in the year to identify the system's capacity limit and the limiting factor (hardware, excessive response time, throughput);
- % of DR and Tabletop exercises for systems as well as exercises to preserve the lives of professionals and service providers, identifying possible internal and external threats and impacts that may compromise the continuity of the Companies;
- % of Training and Development for professionals and service providers in the mandatory Business Continuity Management (BCM) documentation path;
- Monitoring of continuous improvement actions and adequacy of the Companies' business continuity management system;
- Monitoring of business continuity documents to ensure that information keep up-to-date and available.

2. COVERAGE

This Policy applies to all internal audiences, processes, and departments of the Companies, regardless of the structure in physical or virtual units and/or access form, whether local or remote, to the Companies' environment.

Regarding other stakeholders: For Individual Clients (IC) and Legal Entities (LE), this Policy is applicable regarding the fulfillment of their needs and expectations, for which the Companies develop efficient means to securely process business operations at an acceptable level of predefined capacity during disruption.

2.1 Scope

Ensure the timely resumption at an acceptable level of critical business activities:

- ➢ Payment solutions for e-commerce, serving online stores, and commercial establishments,
- ➢ Enable loans, investments, and other products and services essential for the daily lives of clients, and
- ➢ The online investment platform of the PagBank digital account, which includes investments in CDs, Investment Funds, Equities, and public fixed income (*Tesouro Direto*).
- ➢ Payment system for physical and online stores.

In the event of interruption due to failures or significant disasters, applicable to critical systems classified as P1 (crisis) and P2 (unavailability) in Data Centers Glete, Tamboré, and public cloud environments such as AWS, OCI, etc., as well as critical and high-classified business processes located at physical structures at Avenida Brigadeiro Faria Lima 1384/1485, and Avenida Barão de Limeira 426/428, ensuring continuity plans capable of effectively responding to disruption.

2.2 Rules

Business Continuity is a comprehensive process that identifies potential threats inherent to the Companies' businesses and the possible impacts on operations arising from such threats. It provides a framework to develop a level of organizational resilience capable of effectively responding to and protecting the interests of stakeholders, the reputation, the Companies' brands, and their value-added activities.

Business Continuity includes the management of recovery in case of interruption and the overall management of the Continuity Program through training, plans, tests, reviews, and maintenance to ensure its operationalization and update.

3. DEFINITION

Operational Level Agreement (OLA): an agreement between an IT (Information Technology) service provider and another interested party. It supports the delivery of IT services to clients by defining the products, conditions, or services to be provided and the respective responsibilities between the parties.

Agreement de Service level (ASL): a definitive agreement signed between the Company's departments and suppliers, describing services, service level goals, as well as the roles and responsibilities of the parties involved in the agreement.

Business Impact Analysis (BIA): the process of analyzing the impact of a disruption on the organization over time.

Activity: the set of one or more tasks with a defined output.

Priority activities: activities whose urgency is determined to avoid unacceptable impacts on business during a disruption.

Audit: a systematic, independent, and documented process for obtaining audit evidence and objectively evaluating it to determine the extent to which audit criteria are met.

Backup: a backup copy of data from a device to another location or storage media that can be restored in case of accidental loss or corruption of data on the original device.

Information Security and Data Governance Committee: a permanent body with institutional power that monitors, establishes rules, and resolves on interests, among other matters, regarding the continuity context within the Companies.

Business Continuity: the ability of an organization to continue delivering products or services at an acceptable level with predefined capacity during a disruption.

Competence: the ability to apply knowledge and skills to achieve intended results.

Large-Scale Disasters: floods, inundations, fires, collapses, accidents, terrorism, pandemics, or any other situation not foreseen in this Policy that impacts the continuity of the Companies' activities.

Disaster Recovery (DR): a process that includes one or more sets of procedures and plans responsible for the recovery of services after an extreme event.

Disruption: an incident, whether foreseen or unforeseen, that causes an unplanned and negative deviation from the expected delivery of products and services according to the organization's objectives.

BCM: Business Continuity Management.

Incident: an event that may represent or lead to business disruption, losses, emergencies, or crises.

WI: Work Instruction.

CVM Instruction 555, of December 17, 2014, with amendments introduced by CVM Instructions 563/15, 564/15, 572/15, 582/16, 587/17, 604/18, 605/19, 606/19, 615/19, and CVM Resolution 3/20: address the constitution, administration, operation, and disclosure of information for investment funds.

Work Instruction GCN.ITR.004: aims to ensure the systematic approach to the use of the Incident Response Room.

Work Instruction GCN.ITR.005: ensures the recording and treatment of incidents, guaranteeing the normalization of the operation and/or affected service as quickly as possible within the company’s structure.

Continuous Improvement: recurring activity to enhance performance. NBR ISO 22301/2020 Standard: the foundational standard for the Business Continuity Management System – Requirements.

Media: mechanisms in which data can be stored, in addition to the form and technology used for communication - includes optical disks, magnetic disks, CDs, tapes, and paper, among others. Multimedia resources combine sounds, images, and videos, which are different types of media.

Minimum Business Continuity Objective: the minimum acceptable levels of services and/or products for the Companies to achieve their business objectives during a disruption.

Stakeholders: individuals or organizations that can affect, be affected by, or understand being affected by a decision or activity, such as clients, owners, employees, suppliers, bankers, regulators, unions, partners, or society, which may include competitors or opposing interest groups.

OCP – **Operational Continuity Plan**: composed of pre-defined procedures intended to maintain the operational continuity of an organization's vital services in the event of abnormalities.

IMP – Incident Management Plan: a plan oriented towards responses to incidents that may occur in the operational center. It considers the incident occurrence, structure, actions, and communication through the company's channels.

DRP – Disaster Recovery Plan: based on the importance and sensitivity of assets, it defines the planning for restoration, actions related to the mobilization of resources to address crises, recovery procedures for environments, or transfer to redundancy sites.

TVP - Testing and Validation Plan: regular tests conducted by the Continuity Management Group, which, together with other Companies' departments, structure and conduct tests, correcting plan irregularities and submitting them to the knowledge of managers so that they can promote constant improvements and adjustments.

Business Continuity Plan: documented information that guides the organization to respond to disruption and resume, recover, and restore the delivery of products and services according to business continuity objectives.

Policy: intentions and guidelines of an organization, as formally expressed by its Senior Management.

Backup Policy: establishes guidelines for backup procedures to minimize the possibility of data loss or damage, as well as enables recovery in case of incidents resulting from voluntary or accidental actions.

Process: a set of interrelated or interactive activities that transform inputs into outputs.

Professional: any employee, statutory executive officer, intern, or third party of the Companies and departments of the UOL Group that serve them.

Resilience: refers to the Companies' ability to resume normal activities after a business interruption event.

CVM Resolution 35/21: establishes rules and procedures to be observed in transactions with securities on regulated securities markets.

Resolution 4,502, of June 30, 2016: establishes minimum requirements to be observed in the preparation and execution of recovery plans by financial institutions and other institutions authorized to operate by the Central Bank of Brazil.

Resolution 4,557, of February 23, 2017: establishes the risk management structure and capital management structure.

Restore: the process of restoring the copied data to a desired stage in an accessible area.

Risk: the probability of failure of a particular event occurring, generating possible losses.

RTO - Recovery Time Objective: the period to resume a critical activity or process after its interruption. It is the "target time for recovery of an IT system, environment, or application after an incident." RTO defines the time that the Companies can live with the absence of this activity without major impacts. It has as delimiters the declaration of the contingency regime and the return of activity execution.

RPO - Recovery Point Objective: the position (point) at which the data of recoverable applications should be available after a disaster occurs. It is the point in time at which the information used by an activity must be restored to allow the operation of the resumed activity. It is the last moment in time when the data of a computer system are intact and stored in some way, available for use in a recovery process.

Critical System: information service considered essential for a critical business function, which may involve hardware, software, people, and processes necessary to ensure the viability or continuity of operations.

Contingency Site: the critical processes of the Companies. When contingency is activated, such processes are carried out remotely. Regarding the Data Center, redundant sites are available where critical systems run in Glete and AWS, and their contingency is in Tamboré, which can be used as active-active or active-standby as needed, characteristics, or limitations of each application.

Suspension of Activities: interruption of activities due to changes in the rules of regulatory and fiscal bodies, default by flags, or political conflicts.

4. ROLES AND RESPONSIBILITIES

All professionals, notably within their corresponding activities, have roles and responsibilities related to the Business Continuity Management. The positions listed below are identified as having direct functions and responsibilities for the Program:

4.1 Information Security (Business Continuity Management - BCM)

a) Analyze the results of Disaster Recovery (DR) tests for critical suppliers to the Companies, as established in Service Level Agreements (SLAs), and propose improvements;
b) Support the development of Disaster Recovery (DR) test checklists for various teams and business units, as well as the methodology for their execution in conjunction with those responsible and focal points for Business Continuity Plans;
c) Consolidate the results of Business Continuity and Disaster Recovery Plan exercises through the preparation of periodic reports, reporting them to the Information Security and Data Governance Committee and the Executive Board;
d) Fulfill the provisions of Business Continuity documents;
e) Define the methodology and tools to be used for Business Continuity Management, orchestrating the Program as a whole;
f) Implement the Business Impact Analysis (BIA) process annually in the Companies;
g) Propose projects and initiatives to improve Business Continuity Management for the Companies, seeking alignment with existing best practices;
h) Conduct critical analyses and regular updates of Business Impact Analysis (BIA) and risk analyses, considering possible opportunities for continuous improvement of performance and relevance to the business continuity program and this policy;
i) Develop the mandatory BCM documentary track and BCM training for the UniUOL Platform;
j) Receive significant impacts from the Executive Board for the preparation of BIAs;
k) Report the documented and evaluated test results to the Executive Board through the Information Security and Data Governance Committee, enabling continuous improvement of procedures, risk management, and recovery;
l) Report to regulatory bodies, agencies, and monitoring entities, whenever necessary, updated and reliable information about this program.

4.2 Employees

a) Seek guidance from the Information Security department with the Business Continuity Management team in case of doubts related to BCM, Standards, and Business Continuity;
b) Fulfill the provisions of Business Continuity documents;
c) Actively participate in testing and planning processes when required; and
d) Complete the mandatory BCM documentary track and BCM training for the UniUOL Platform.

4.3 Managers

a) Trigger and follow the Work Instruction (GCN.ITR.004) whenever necessary;
b) Trigger and follow the Work Instruction (GCN.ITR.005) whenever necessary;
c) In the event of an incident that has triggered the Business Continuity Plan, it must be reported to the Compliance department;
d) Fulfill the provisions of Business Continuity documents;

e) Ensure the active participation of professionals under their management in processes that involve the development, as well as participation in Business Continuity Plans;
f) Identify and appoint a responsible professional to represent business continuity management through its documents;
g) Participate in and nominate employees to take part in exercises and tests, validating over time the effectiveness and validity of their business continuity strategies and solutions;
h) Participate in the development of the Business Impact Analysis (BIA) to analyze the impact on business and assess disruption risks; and
i) Complete the mandatory BCM documentary track and BCM training for the UniUOL Platform.

4.4 Communication

In the event of a major disaster or suspension of activities, the Communication department of the Companies must inform their clients and shareholders through appropriate channels and teams regarding such situations, always considering the Legal department's opinion, which includes the legal – judicial and extrajudicial - aspects of the Companies. These actions are related to the Crisis Management Plan, which is addressed through GCN.ITR.004 - Methodology for using the Incident Response Room.

4.5 Risk and Compliance

a) Analyze the Business Continuity Policy to ensure that it is appropriate for the business continuity objectives of the Companies;
b) Communicate relevant incidents affecting critical systems that have a significant impact on clients, promptly report to the management bodies and Superintendence of Market Relations and Intermediaries (SMI), after the incident occurs, informing regulatory bodies, as specified in CVM Resolution 35;
c) Make the Policy (summary) available to stakeholders through the Companies' website;
d) Request the availability of the Business Continuity Policy on the Companies' intranet for employees; and
e) Request approval of the Business Continuity Policy from its sponsors, with its record through minutes.

4.6 CRO PagSeguro PagBank and CFO PagSeguro PagBank

a) CRO and CFO are sponsors of this Policy and responsible for ensuring that the program receives adequate support.
b) The effective responsibility for compliance with the provisions of this Policy lies with the manager of the respective departments. Furthermore, it is their responsibility to determine institutional guidelines based on values and principles established in this policy, internal control standards, regulations issued by regulatory and self-regulatory bodies, and best practices applicable.

5. GUIDELINES

The guidelines of the Business Continuity program are:

a) Improve the quality and effectiveness of the strategies, plans, and processes established for the continuity of their business, investing in methodologies that meet the standards for the sustainability of their business considering the needs and expectations of stakeholders;

b) Establish objectives, goals, controls, processes, and relevant procedures to improve Business Continuity and achieve results aligned with the policies and strategic objectives of the Companies. The monitoring of results and the achievement of objectives are measured and communicated to the senior management through critical analysis;

c) Identify and ensure the application of legal and regulatory requirements for the Companies as outlined in instructions and regulations, among others;

d) Conduct annual exercises and tests to validate the efficiency and validity of their business continuity strategies and solutions through tabletop exercises and disaster simulations that ensure the maintenance of continuity, as well as the operation of continuity plans. The results of exercises and tests are documented, allowing continuous improvement of risk management and recovery;

e) Review annually or following relevant changes (which may result from updates, migrations, implementation of new products, new demands, among other modifications informed by business units so that the impact assessed in each process remains consistent with the business reality) all documentation related to Business Continuity Management;

f) Analyze the impact of the interruption of the Companies' activities over time, determine their recovery times, and identify critical activities to recover them at an acceptable level time;

g) Ensure that all professionals understand their responsibilities regarding Business Continuity through training and awareness on the subject;

h) Develop a crisis management and response structure supported by adequate levels of authority and competence to ensure effective communication with stakeholders;

i) Establish roles and responsibilities of internal and external parties to the Companies;

j) Identify and evaluate third parties that play a critical role in the value chain and business process collaboration;

k) Ensure the periodic review of the performance of the Business Continuity Management System and the implementation of corrective and improvement actions;

l) Adopt risk mitigation practices appropriate to the dimension of threats and the extent of their possible impacts;

m) Establish the identification of practices for service resumption and mitigation of operational risk in a formal Business Impact Analysis process; and

n) Preserve the physical integrity of individuals through plans and exercises, ensuring the well-being of employees.

6. QUESTIONS

Questions about this Policy should be forwarded to the Information Security department, via email at l-pagseguro-dresden-continuidade@uolinc.com.

7. INFORMATION CLASSIFICATION

According to the Information Classification Policy, this Policy is classified as Internal Information.

8. MISCELLANEOUS

This Policy was approved by PagSeguro's Executive Board at the meeting held on April 10, 2023.

9. EXHIBITS

N/A

10. CHANGE CONTROL

Revision	Changes	Date
00	Initial issue | Information Security & Compliance	January/2019
01	First version | Information Security & Compliance	March/2020
02	Second version | Information Security & Compliance	December/2020
03	Third version | Information Security & Compliance	March/2022
04	Fourth version | Information Security & Compliance	April/2023

PAGSEGURO INTERNET INSTITUIÇÃO DE PAGAMENTO S.A. – INFORMATION SECURITY & COMPLIANCE