brighten
simplify your business.
together.

GENERAL INFORMATION SECURITY POLICY (GISP).

A.5_ Politicas Segurança da Informação

Code/Unit: A05.003	**Type**: Digital
Confidentiality: Public	**Available on:** Microsoft Teams / Sharepoint

Brighten ISO/IEC 27001 certified

Version Control

Date	Version	created / edited by	Update Description	Approved (A) by: Date:
Dez 2020	V1.0	SB	Documento Base	A: Managing Partner Data: Dez 2020
Fev 2021	V1.1	SB	Atualização do ponto objetivos	A: Managing Partner Data: Fev 2021
Dez 2021	V1.2	SB	Atualização de template	A: Managing Partner Data: Dez 2021

Index

1. INTRODUCTION

This document is part of **Brighten S.A.** (hereinafter referred to as "Entity", "Organization" or "Brighten") Information Security Policy, being framed in the Information Security Management System (ISMS).

1.1. Purpose

Brighten recognises that **preserving the confidentiality, integrity and availability of information** is critical to the ongoing operations of our business. Failure to secure this key business asset significantly increases the risk of financial and reputational damage to us and our partners.

This policy statement outlines our commitment to ensuring **Continual improvement of ISMS** and the continued **security of the information assets** managed by or on behalf of **Brighten**.

1.2. Scope and Audience

This policy statement applies to all **Brighten** employees, temporary staff, contractors, consultants, partners (hereinafter referred to as "employees") and third parties who have access to and/or hold **Brighten**'s data and systems.

Information assets governed by this Policy Statement include, but are not limited to: physical assets, hardcopy files and reports, computer systems, software files, databases and backups.

In addition to adequate access to the information necessary for the performance of their duties, all employees shall be responsible for understanding and complying with this policy.

2. INFORMATION SECURITY PRINCIPLES

Brighten's information security policies, both in their definition and in their daily implementation, must be guided by the following principles:

1. ***Protection and Classification of Information*** - ensure the protection and classification of information and its supporting assets in terms of integrity, authenticity, availability and confidentiality;

2. ***Legal compliance*** - both the policy and the tasks performed within its scope are subject to the applicable legislation, as well as to the internal rules and regulations

regarding information approved by Management, customer requirements and others external to the organization;

3. ***Need for access*** - access to information should be restricted, exclusively, to people who need to know it in order to fulfill their functions and tasks;

4. ***Transparency and Responsibilities*** - ensure transparency. The responsibilities and role of stakeholders in information security must be clearly defined and subject to periodic monitoring and auditing;

5. ***Proportionality*** - information security activities must be proportional to the risks to be mitigated and limited to what is necessary;

6. ***Policies compliance*** - defined security policies and procedures must be integrated into work processes and the performance of daily tasks must be guided by compliance with them;

7. ***Information*** - all policies and procedures are publicized and communicated to all employees who need them for the performance of their functions and tasks;

8. ***Training*** – employee training and awareness plans must be defined, approved and executed, focusing on the domain of information security and on the specific policies and procedures adopted in this area;

9. ***Security Incident Management*** - carry out an appropriate security incident management, through processes of prevention, detection, registration, communication, treatment and investigation of incidents and vulnerabilities that may compromise information security, protection of personal data or interrupt business continuity.

10. ***Continual Improvement*** - continual improvement of the ISMS, including demonstrating the suitability and adequacy of it and how effective it is, as a necessary condition for customer satisfaction and trust, and as a differentiating and competitive factor.

3. POLICY STATEMENT

We shall employ pragmatic, cost-effective controls to reduce information security risk to an acceptable level and ensure that:

- Information will be **protected against unauthorised access**;
- **Confidentiality** of information is **assured**;
- **Integrity** of information is maintained;
- Information and information systems are **available** when needed;
- **Legislative, regulatory** and **contractual** security requirements are **met**.

We shall strive to manage risks that may adversely impact the security and integrity of critical or sensitive information assets used by or managed by the business.

4.RESPONSABILITIES

Information Security Management specific responsibilities and authorities are detailed in the internal document "*SI_Politica de Segurança da Informação*".

Additionally our Information Security Policy set applies to all users that have access to our information and information systems, and applies equally to management, permanent and temporary staff, contractors, consultants, partners, and suppliers. **Brighten** shall ensure that all users are issued with this policy. All users shall be responsible for understanding and complying with this policy. Non-compliance may lead to staff disciplinary action, or prosecution for legal, regulatory and / or contractual breaches.

Brighten Audience, identified above, is required to report any actions or conditions that appear to violate the spirit or intent of the following statement and its supporting policies.

Ultimate operational responsibility for information security rests with the Chief Executive Officer.

Senior management team is responsible for managing and implementing the policy and related procedures on a day-to-day basis.

Where responsibilities are unclear, the Chief Executive Officer will decide who is responsible for an aspect of information security.

Line Managers are responsible for ensuring that their teams are aware of:

- Information security procedures applicable to their area;
- Their personal responsibilities for information security;
- How to obtain further advice on information security matters.

5. POLICY UPDATE

This Policy takes effect on the date of its publication and will be reviewed whenever it is considered necessary.