Information Security

PSIE001 – EXTERNAL INFORMATION SECURITY POLICY

Classification: Open

Version 1.5

Elaboration:	Approval:	Creation date:	Validity:
Information Security	CGSI	11/13/2022	11/15/2026

SUMMARY

1. INTRODUCTION

1.1. Objective

The purpose of this policy is to publicly present LG lugar de gente's information security guidelines.

1.2. Scope

It covers all the business units, members of the board of directors, members of the advisory committees to the board of directors, employees, third parties, service providers, partners and suppliers of LG lugar de gente.

1.3. Responsible

The Information Security department is responsible for updating this policy.

1.4. Terms and Definitions

See **Information Security Concept Organization Standard and PDP**.

1.5. Document Location

This document was created, updated, approved and published through LG lugar de gente's official processes and can be found published on LG lugar de gente's official website.

2. PRINCIPLES OF THE INFORMATION SECURITY POLICY

Information is understood to be any content or data that has value for the organization or its clients. It can be stored for restricted use or exposed to the customer for consultation or handling. It can be printed or written, spoken or transmitted by e-mail or electronic means. Regardless of the form in which information is presented or the means by which it is shared or stored, information is LG lugar de gente's and its clients' greatest asset, and therefore essential to the business. As such, it must be properly protected and used in an ethical and secure manner, guaranteeing reliability by protecting it:

a) Confidentiality: Ensuring that information is not disclosed or available to unauthorized individuals, entities and processes;

b) Integrity: Ensuring the accuracy and completeness of information and processing methods;
c) Availability: Ensuring that information is always accessible and available when needed.

3. INFORMATION SECURITY GUIDELINES

To address all the effort and maintenance required for Information Security, LG lugar de gente has established the following guidelines:

a) An Information Security and Privacy Management structure has been established and maintained with the support of Senior Management, through an Integrated Information Security and Privacy Management System (SGSI and SGPI) implemented at LG Lugar de gente;
b) All information is used with a sense of responsibility and in an ethical and secure manner, for the exclusive benefit of corporate business, as provided for in the LG lugar de gente Code of Ethics and Conduct;
c) All information assets are properly identified, classified and monitored;
d) The identification of each LG lugar de gente employee is unique, personal and non-transferable, qualifying them as responsible for the actions carried out;
e) All risks are analyzed, classified and presented to a committee that will decide on the appropriate treatment for them;
f) All security incidents and personal data breaches are reported to the Information Security department for analysis, evaluation and treatment;
g) LG lugar de gente identifies, follows, documents and keeps itself updated in relation to the laws that regulate its activities, as well as aspects of intellectual property, as presented in ESI001 - SGSI and SGPI SCOPE DECLARATION;
h) LG lugar de gente, through its senior management, has Strategic Information Security Objectives considering this policy, the applicable Information Security requirements and the results of Risk Management, according to the guidelines established in DEA001 - APPLICABILITY STATEMENT;
i) All employees, service providers, partners and suppliers who have access to LG lugar de gente information, as well as that of its clients and partners, formally adhere to the "PSI_PPDP Awareness and Understanding Agreement", undertaking to fully respect this PSI and the rules that support it.

4. INFORMATION SECURITY MANAGEMENT

In order to maintain a satisfactory level of security, the Information Security Management Committee (CGSI) was set up, which adopts Security Standards to support the guidelines presented:

a) In NSI006 - ACCESS CONTROL STANDARD, for managing access by employees, service providers, partners and suppliers to information assets, which are duly approved by the person responsible for the information (manager, board of directors or person in charge as defined in the information documents), which access will allow manipulation, whether for simple consultation or for alteration;

b) In NSI009 - ELECTRONIC MAIL USAGE STANDARD, containing organizational guidelines for the use of e-mail under the "@lg.com.br" domain, allowed only for internal and external employees, and for third parties in accordance with the third-party contracting process;

c) The organization adopts a comprehensive business continuity management process that identifies potential threats to LG lugar de gente and the possible impacts on business operations should these threats materialize. This process provides a framework for developing organizational resilience that is able to respond effectively and safeguard the interests of the parties involved. The business continuity management system (SGCN) includes policies, planning activities, responsibilities, procedures, processes and resources;

d) In NSI014 - SECURE DEVELOPMENT STANDARD AND INFORMATION SECURITY AND PDP REQUIREMENTS, which contain mandatory guidelines and controls for information protection, applicable to the development, acquisition, and updating of systems and software, aiming to ensure security, privacy, and compliance throughout the entire lifecycle of the organization's solutions;

e) In NSI005 - REMOTE ACCESS STANDARD, containing guidelines for granting remote access to employees and service providers, previously requested and authorized by the responsible area;

f) In NSI008 - CLEAN TABLE AND ACCEPTABLE USE OF ASSETS STANDARD, containing guidelines for the use of corporate mobile equipment intended for use on the job to carry out employees' work activities and to communicate with the company, suppliers or clients, and should only be used for this purpose.

It defines the physical security perimeter, access to restricted environments in a controlled manner and only authorized users are allowed. Access to the company entrance is controlled and monitored. Employees, third parties and visitors must carry

visible identification. Access to restricted rooms is segregated from other company environments in order to guarantee the protection, availability, integrity and confidentiality of the information handled by LG lugar de gente.

When technological reasons or higher orders make it impossible to apply the requirements set out in this policy, the person responsible and/or the applicant shall immediately report them to the Information Security area so that alternative measures can be adopted to minimize the risks, as well as an action plan to correct, monitor or eliminate them;

g) In NSI004 - INFORMATION HANDLING AND CLASSIFICATION STANDARD, containing guidelines for classification, labeling and other rules for handling information according to confidentiality and the necessary protections, as follows: Public, Internal, Restricted and Confidential, and must be handled, stored and disposed of correctly to guarantee the information security aspects of LG lugar de gente's business and its clients' information;

h) The organization has mapped processes with labeled artifacts published on the intranet (Entre a Gente), in addition to the tangible and intangible information assets identified individually, inventoried, protected and monitored for undue access. The media are properly managed in accordance with the information security requirements established and implemented at LG lugar de gente;

i) In NSI018 - CRIPTOGRAPHIC KEY MANAGEMENT STANDARD, which contains guidelines that establish a set of rules adopted by LG lugar de gente to ensure the standardization of cryptographic techniques, their proper application and techniques, their proper application and responsibilities, with the aim of maintaining security in the transportation or storage of information, regardless of the medium used. It also contains rules on the transmission of information, for resources, providing for the use of control including personal data processed by the organization, to ensure privacy in the communication of data from LG lugar de gente and its customers;

j) LG lugar de gente has specific processes for change management, both in the development of its software and for changes in infrastructure. The change management process is applied to ensure that controls and modifications to information processing systems or resources are carried out with planning, so as not to cause operational or security failures in the organization's production environment. In addition, the entire change management process is published on the LG lugar de gente intranet (Knowledge Portal) and aims to ensure that all company employees have access to the procedures relating to change management;

k) In NSI003 - RISK ANALYSIS, EVALUATION AND TREATMENT STANDARD, containing guidelines and rules for identifying risks through an established process for

analyzing vulnerabilities, threats and impacts on information security processes (Confidentiality, Integrity and Availability);

l) In NSI007 - INFORMATION SECURITY INCIDENT TREATMENT STANDARD, containing guidelines for managing all incidents affecting information security, by opening a ticket in specialized software used for incident management, among which are reported to the Information Security area, which analyzes the incident and takes the appropriate actions, passing on the treatment to the responsible areas;

m) In NSI017 - SGSI AND SGPI STANDARD AND INDICATORS, containing guidelines to ensure the continuous improvement of the Integrated Information Security and Privacy Management System (SGSI and SGPI), based on the ISO/IEC 27001:2013, ISO/IEC 27701:2022, ISO/IEC 27018:2021 and ISO/IEC 27017:2015 standards, having the indicators and metrics for monitoring the SGSI and SGPI throughout the PDCA cycle;

n) In NSI011 - SUPPLIER MANAGEMENT STANDARD, containing guidelines aimed at ensuring that there are no legal, regulatory or contractual violations in the organization's information security requirements in relation to the management of services carried out by suppliers, partners and third parties;

o) In NSI019 - CLOUD SECURITY AND PRIVACY STANDARD, which contains guidelines for the contracting, management, and secure use of cloud services, establishing security, privacy, and compliance requirements applicable to SaaS, PaaS, and IaaS-based solutions within the organization's corporate environment;

When technological reasons or higher orders make it impossible to apply the requirements set out in this policy, the person responsible and/or the applicant shall immediately report them to the Information Security area so that alternative measures can be adopted to minimize the risks, as well as an action plan to correct, monitor or eliminate them.

5. MONITORING AND AUDITING

LG lugar de gente monitors and records all use of information generated, stored or transmitted within the company. To this end, the organization presents, in NSI016 - SGSI AND SGPI INTERNAL AUDIT STANDARD, guidelines for maintaining appropriate controls and audit trails or records of activities at all points and systems that the company deems necessary in order to reduce risks, and reserves the right to:

a) Implement other systems to monitor access to workstations, internal and external servers, e-mails, browsing, the Internet, mobile or wireless devices and other network

components. The information generated by these monitoring systems can be used to identify users and their accesses;

b) Inspect any files on the network, on the workstation's local disk or in any other environment to ensure strict compliance with this PSI;

c) Install other protection and intrusion detection systems to guarantee the security of information and access perimeters.

6. PENALTIES

LG lugar de gente has established that for any and all violations of the Policy and other Information Security Standards that support it, an information security incident must be opened and duly analyzed and treated in accordance with the information security incident management process provided for, and must then be reported to the CGSI/CGPDP. Consequently, the incident is investigated through an internal procedure, which is conducted by the head of the area in which the professional who committed the infraction is assigned, in conjunction with the Human Resources area and LG lugar de gente's Legal department.

If the CGSI/CGPDP deems it appropriate, the employee or third party involved may, for the duration of the internal investigation process, be removed from office or suspended.

Any employee or third party suspected of violating the Information Security Policy and/or Standards is guaranteed fair and correct treatment, and any and all measures resulting from the violation must be applied proportionally to the occurrence based on the Code of Ethics and Conduct, Confidentiality Agreement, Information Security Policy and Standards of LG Lugar de Gente and current legislation.