sophos
solutions

Process: INFORMATION SECURITY MANAGEMENT

INFORMATION SECURITY POLICY

Document No: **PL-SSI-01**

Version: **11**

Date: **30/03/2022**

Written by: **Information Security Group**

DOCUMENTO APROBADO POR

	REVIEWED BY	APPROVED BY
Name	Álvaro Barbosa	Felipe Villa Murra
Position	Risks and Information Security Manager	President & CEO
Date	30/03/2022	30/03/2022

1 ÍNDICE

2 HISTORIAL DE VERSIONES

Fecha	Versión	Autor	Descripción
21/08/2020	08	Risk & Information Security Administrator	Roles and responsibilities Activities of Risks and Information Security Area Actions affecting information security Responsibility of Sophos Solutions S.A.S and its Partners for Information Security Access Control Policy Work Policy in Protected Areas. Equipment Safety Policy Outside Company Facilities Malicious Software Protection Policy Vendor Relationship Policy Operational Change Control Policy Information Security Incident Management Policy Business Continuity Information Security Policy

			Cryptography Policy
11/03/2021	09	Risk & Information Security Lead	The scope of the Information Security Management System is updated The section on handling exceptions is updated as they are now handled by flow2I
02/09/2021	10	Risk & Information Security Lead	Remote Work Policy Change Control Policy Acceptable Use of Information Assets Policy Log Management Policy Associated norms are added.
30/03/2022	11	Risk & Information Manager	Strategic Policy becomes independent from security policies Security Policy is updated System objectives are updated Roles v Responsibilities are updated

3 INTRODUCTION

The Information Security Policy is aimed at promoting the security of all information assets of the Company in accordance with its corporate strategy, thus ensuring regulatory and normative compliance, in addition to the policies, procedures and controls established for that purpose.

4 UPDATE INFORMATION SECURITY POLICY

In compliance with the continuous improvement of the Information Security Management System, it is established that the Information Security Policy should be reviewed every 6 months from the last change made or when there are modifications or new guidelines that warrant it.

The update of the Security Policy shall be validated and approved by the Information Security Committee.

5 ASSOCIATED REGULATIONS

Information Security and Privacy	Intellectual Property
Political Constitution of Colombia. Article 15.	**Law 23 of 1982.-On copyright"**
Law 1266 of 2008.- By which the provisions Habeas data and the handling of information contained in personal databases, in particular financial databases, credit, commercial, service and third party countries and other provisions are issued.	**Decree 1360 of June 1989.-**By which logical support (software) registration is regulated in the National Registry of software in the National Registry of Copyright
Law 1273 of 2009.- Through which the Penal Code is amended, a new legal good is created - called "of information and data protection"- and are preserved integrally the systems that use the information and communications technologies, among other provisions.	**Law 44 of 1993.**- By wich the Act No. 23 of 1982 is added and amended and the Law 44 of 1993.- Amending Law 29 of 1944 and Andean Decision 351 of 2015 (Copyright).
Law 1581 of 2012.- By which general provisions are issued for the protection of personal data.	**Decision Andean 351 of 1993.** Common system on copyright and Related Rights

Decree 1377 of 2013.- By which Law 1581 of 2012 is partially regulated Law 1581 of 2012.	**Law 178 of 1994.-** Accession to the Convention of Paris for the Protection of Industrial Property
Law 1928 of 2018.- By which the " Convention of Cybercrime " is approved, adopted on 23 November 2001, in Budapest. - confirmed by the Constitutional Court, in the judgment C 224	**Decree 460 of 1995.-** Regulations of National Copyright Registry and Legal Deposit is regulated regulates the Legal Deposit
External Circular 029 of 2014 of the Superfinance. - Part I Title I Chapter IV — Internal control Includes continuity.	**Law 599 of 2000.-**Legal assets of the copyright
External Circular 029 of 2014 of the Superfinance. - Part I Title II Chapter — Safety	**Law 565 DE 2000.-** Accession to the Treaty of WIPO about Copyright
	Law 1915 of 2018 By which Act No. 23 of 1982 is amended and other provisions on copyright and related rights are established.

6 SCOPE OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

Through the implementation of ISO/IEC 27001:2013, Sophos Solutions S.A.S. adopts, establishes, operates, checks, and improves the Information Security System for Software Development Factory processes "including Project Planning and Management, Requirements Gathering, Analysis and Design, Construction, Testing, Implementation, Support and Consulting".

Sophos Solutions S.A.S is a Colombian multinational, with offices in the city of Bogota D.C. and Medellin, which provides consulting services, implementation of banking core, software factory for all types of organizations, especially in companies of the financial and stock sector.

6.1 INFORMATION SECURITY MANAGEMENT SYSTEM POLICY

Sophos Solutions SAS, understanding the importance of protecting the confidentiality, integrity and availability of information for each of the information assets and IT services it offers to the financial and stock market industry, as well as the Fintech industry as a leader in digital innovation, has committed to establish, implement, adopt, operate and improve the Information Security Management System as a cross-cutting instrument to identify, analyze, contain and remedy identified security risks in order to sustain the continuous improvement of the system, aligned with the company's regulatory and strategic requirements

Therefore, the Information Security Policy applies to internal stakeholders of Sophos Solutions SAS according to the scope determined for the Management System.

The other policies resulting from the implementation of the ISMS and its continuous improvement process will be adopted and enforced by all identified stakeholders

6.2 OBJECTIVES OF THE INFORMATION SECURITY MANAGEMENT SYSTEM

1. Assess the security controls currently in place in order to support the ISMS in line with standard 15027001 and the needs of the organization by proposing a current profile and an objective profile.
2. To generate information security awareness among employees of the company through training and awareness-raising defined as a means to control security incidents.
3. Control information security incidents by analyzing reports obtained from different sources in order to mitigate their causes and/or consequences.

4. Identify the Vulnerabilities to which the entity is exposed through own and third party analyzes in order to take actions that allow to close the security breaches presented by the organization and that may jeopardize the confidentiality, integrity and availability of the information.
5. Control the security breaches identified in Development Projects to customers by analyzing the security findings obtained in information security audits.

6.3 ROLES AND RESPONSIBILITIES

The structure defined for assigning Roles and Responsibilities for information security management shall be:

SENIOR MANAGEMENT	PRESIDENT & CEO VICEPRESIDENT SPECIAL PROJECTS
COMMITTEE ON SECURITY OF INFORMATION	PRESIDENT & CEO VICEPRESIDENT SPECIAL PROJECTS MANAGER OF STRATEGY AND VALUE CREATION CHIEF OPERATION OFFICER LEGA L MANAGER & DEPUTY SECRETARY GENERAL CORPORATE MANAGER INFORMATIC SECURITY AND TECHNOLOGY MANAGER IT LEADER CHIEF FINANCIAL OFFICER VICEPRESIDENT GLOBAL TALENT VICEPRESIDENT GLOBAL SALES VICEPRESIDENTS PROJECTS VICEPRESIDENT PRODUCTS AND SUBSIDIARIES GLOBAL TALENT MANAGER VICEPRESIDENT REGIONAL SALES COUNTRY HEAD NORTH AMERICA INNOVATION MANAGER QUALITY & PROCESSES MANAGER RISK & SECURITY INFORMATION LEAD RISK LEADER
FINAL USER	COLABORATORS
INTERNAL AUDIT	GLOBAL INTERNAL AUDIT MANAGER GLOBAL INTERNAL AUDIT LEADER TI

Based on the role and responsibility allocation structure defined, the responsibilities assigned to each role are listed below

6.4 SENIOR MANAGEMENT

The top management is the highest organ of the company, therefore, its responsibility for the continuous improvement of the Information Security Management System is:

- Approve policies for information security management.
- Support the definition and guidelines of the strategy for information security management.
- Provide the necessary resources and assign the roles, responsibilities, and levels of authority to implement and maintain information security management.
- Monitor the improvement and continuity of the Information Security Management System.

6.5 COMMITTEE ON INFORMATION SECURITY

The Information Security Committee is responsible for:

- Analyze and provide suggestions for improvement to the presidency on all guidelines of information security management.
- Analyze and deliver improvement suggestions to the presidency on measurement models and risks for information security management.
- Recommend the imposition of disciplinary measures for cases that the Risk and Information Security Area reports for non-compliance with established security policies within the organization.
- Analyze and recommend the implementation of controls to prevent information security risks.
- Analyze and Implement information security culture generation programs.
- Implement and monitor indicators that measure the objectives associated with the System of Information Security Management.
- Analyze external and internal issues in the light of information security.
- Analyze the performance of the Information Security Management system.
- Analyze the results of security feedback from external suppliers/customers.
- Analyze opportunities for improvement.

The information security committee may be attended by analysts or leaders from different areas, but they will have no say.

This committee will meet on a quarterly basis and will deal with issues related to the Information Security Management System.

The internal auditor shall be permanently invited to the committee and shall have a voice, but no vote.

6.6 FINAL USER

- The Sophos Collaborators are responsible for the quality, integrity and veracity of the data entered in the different information systems used within the company (whether own or third parties).
- Collaborators are required to comply with the guidelines and permissions granted by the owner on its information assets.
- Sophos employees must comply with the Security Policy set forth in this document and all policies derived therefrom.
- Sophos Collaborators must ensure compliance with Information Security policies within their immediate work environment (internal to the company and in the Customer).
- It is the responsibility of collaborators, customers, and suppliers to report immediately and through the channels established by Sophos Solutions SAS, the suspicion or occurrence of events and / or incidents of Information Security related to the company.
- It is the duty of employees to use the company's information systems and network access solely for the purposes that link them to the company.
- It is the duty of partners to use only the software and other technological resources authorized by Sophos and/or the Sophos Customer.
- It is the duty of the Sophos Solutions SAS collaborators and Suppliers to ensure the Confidentiality, Integrity and Availability of the information assets used for the execution of their activities.
- It is the duty of the collaborators to use the different channels, tools and means of communication provided by the area of Information Security and Infrastructure to make specific requests for security, access, and services in front of their daily tasks.

- It is the duty of Collaborators and Suppliers to actively participate in Security courses, talks and awareness-raising organized by the Information Security area.

6.7 INTERNAL AUDIT

Validate the implementation and compliance of the Information Security Policy defined in this Directive, as well as the other policies resulting from the process of continuous improvement of the ISMS, the application of controls on information assets and the other requirements of the Information Security Management System.

"Sophos Solutions S.A.S. reserves the right to modify this document according to the changes that arise within the company"