# Information security and Cybersecurity Policy

## Introduction and objective

SURA Asset Management recognizes information as a valuable asset that supports the company's processes and decisions. Therefore, it is committed to keeping its own and third-party information secure by using management and control strategies that make it possible to preserve its confidentiality, integrity, and availability, and to face the threats to which the company is exposed.

## Scope and framework of application

the guidelines contained in this document apply to all employees and third parties (clients, suppliers of services, or allies) involved in the operations and/or functioning of the processes of SURA Asset Management, its affiliates and subsidiaries having a significant participation (hereinafter the "company"), regardless of the modality under which they are working.

This policy applies to all the company information managed by SURA Asset Management, regardless of the mechanism under which the information is managed. It also applies to all information systems and mechanisms where the information and data are used and stored, regardless of whether it is a cloud-based system, software, company's own or third-party applications and/or technology tools.

These guidelines are established to identify, protect, detect, respond, and recover information by managing their associated risks. In the event that the regulations in a specific country or locality are stricter than the guidelines provided in this policy, such other regulation will prevail.

## Information security and cybersecurity guidelines

information, as an important company asset, must be properly protected, and the application of this document is a commitment to implement protection mechanisms. Thus, the company must :

i. Ensure that the information security functions (governance, operation, and monitoring) are aligned with the company's corporate governance.

ii. define and implement policies, processes, procedures, instructions and/or operating manuals that are clearly defined, approved, and published, to manage and develop the information security capabilities in line with the corporate definitions and guidelines.

iii. guarantee the existence of the necessary mechanisms to measure the operating effectiveness, the adoption of the guidelines, and to provide regular monitoring and follow-up in order to identify any deviations and areas for improvement vis-à-vis the guidelines of the policies, processes, responsibilities and/or controls defined by information security and cybersecurity, and report them to corporate headquarters.

iv. ensure that there are clear mechanisms for reporting, scaling, and communicating to corporate headquarters to enable them to have a consolidated view of the governance, operation, monitoring, functioning, and compliance with information security.

v. To have a corporate information security strategy and a budget assigned to implement the measures necessary to mitigate the risks identified with respect to information assets. Local information security strategies and programs must be aligned with the regional strategy.

vi. Manage the information security and cybersecurity risks within the framework of operating process and technology risks in order to define the information security controls, and identify, assess, and monitor such risks. To that end, the companies must guarantee:

    a. That they are part of the "purchasing, goods and services" program to identify, assess, deal with, and monitor risks arising from relationships with third parties, services, and new technologies.

    b. That they participate in projects involving the requirements of information security and cybersecurity in order to protect the information assets and the technology that supports them.

vii. guarantee information security for employees and third parties by aligning them with other internal processes to include information security aspects in the selection, hiring, development, and termination of human talent.

viii. implement annual training programs and campaigns to create awareness of the risks related to information security and cybersecurity, based on the dynamic outlook of the threats to which the company might be subjected.

ix. manage information assets for which it needs:

a. An inventory of information assets

b. A clear knowledge about the ownership of the information

c. Classify and manage information and technology assets according to corporate criteria and local regulations

d. Manage the lifecycle of the information

e. Establish information security controls for developing, acquiring, implementing, maintaining, processing, and disposing of information systems.

f. Have an appropriate logical access control and monitoring system.

x. Manage and operate security of the technology that supports the information and, therefore, it must:

a. Establish and maintain controls that ensure confidentiality, integrity, and availability of the information in technology operations, considering the security and cybersecurity of all technology assets that support SURA AM's operations, including infrastructure, networks, and telecommunications, among others.

b. Establish, carry out and maintain regular exercises for analyzing vulnerabilities, and penetration tests to identify and close possible security gaps in the area of technology.

c. Make appropriate use of the information technology which must be used only for the objective and purpose for which they were established.

d. Set up and maintain security and cybersecurity controls on end-user equipment

e. Establish mechanisms to encrypt information in transit and/or at rest that must be implemented in computer equipment, databases, applications, services, mobile devices, and/or any external storage device. All of the above according to the classification of information assets.

f. Use data masking and set up mechanisms to protect confidential and sensitive information and, at the same time, keep it legible so that it can be used freely without endangering the security of the information. This applies to all environments (production, testing, QA, and development).

g. Monitor events and cyber intelligence: implement active monitoring of events and weaknesses in information assets, as well as the consumption from cyber intelligence sources of threats as part of an information security incident prevention strategy. The monitoring of security events must include identifying unusual behavior by the critical personnel included in our security analysis program.

h. Manage brand security and protection by monitoring the appropriate use by all company employees inside and outside the organization.

i. The management of information security events and/or incidents that impact the availability, confidentiality, and integrity of the information must be aligned with the guidelines defined for business continuity management and/or crisis management in order to respond and recover the operation in an efficient manner and minimize negative effects on the achievement of the company's objectives, mission, and vision. Events involving kidnapping, theft, modification and/or publication of company information and which include extortion by cyber criminals, must be analyzed to assess the operational, legal and/or reputational impact, in addition to the control mechanisms to recover or restore the information. Additionally, they must be reported to the corporate information security officer who will inform or consult with Sura Asset Management's Board of Directors risk management committee , the plan to deal with the event.

## Main functions and responsibilities of the governance bodies

The company guarantees support for Information Security activities so they can implement, operate , maintain, and continuously improve the process through:

- **Board of Directors' Risk Committee:** In addition to the functions and responsibilities described in the "Policy for Managing Operating Risks" the Board will be responsible for monitoring the strategy and the resources to manage Information Security, and for determining the degree of maturity of the activities and the current risk exposure related to this specialty, monitoring their risk management, and the relevant Information Security events and incidents.

- **Regional Information security and cybersecurity committee:** This committee is responsible for following the corporate performance related to Information security , i.e., monitoring compliance with the regional strategic objective, the alignment of local initiatives with the corporate initiatives, following the information security risk management indicators, and following the global and regional threats affecting the company.

- **Integrated risk management committee:** In addition to the functions and responsibilities described under "Policies for Managing Operating Risks", this committee is in charge of making sure that information security management follows the approved objectives, policies, strategies, procedures and risk tolerance and appetite levels. In addition, it must promote the Information Security culture and monitor compliance with internal and external regulations.

- **Information Security Officer:** The information security officer is responsible for achieving the strategic information security and cybersecurity objectives through governance, management, and monitoring. This committee relies on each company's staff to implement their activities and comply with the regulatory requirements.

## Governance

The Board of Director's' Risk Committee of SURA Asset Management will approve this policy. Any changes must be approved by this governance body. Any exceptions to the compliance with this policy must be reviewed by the Information Security Officer and, when a high or critical level risk is identified, it will be sent up to the Board of Directors' Risk Management Committee.

## Dissemination and updates

Everyone covered by this policy must know and apply it, and comply with these provisions. The Information Security Department, representing the Information Security Officer, will be responsible for managing this policy and, thus, it will coordinate with the Information Security team this policy's compliance and dissemination.

This policy shall be effective as of the date on which the Board of Directors or a similar body approves it, and will be updated according to legal provisions, organizational changes, or other factors that might affect the guidelines described herein.