INFORMATION SECURITY AND CYBERSECURITY POLICY

At Grupo SURA, information is considered a strategic asset for conducting business, and therefore it is important to recognize that proper information treatment involves great challenges and tasks that require responsible planning, organization, management, preservation and protection.

As far as the organization is concerned, information protection, quality, confidentiality and availability are matters of great relevance, and knowing this allows us to uphold the dependability of the Company in the eyes of its stakeholders and to minimize financial, legal, operational and reputational risks; which are often associated with how information is managed.

The following instructions are complementary to applicable national and international regulations and establish both the general and specific guidelines defining the information security and cybersecurity action plan in the Company, which is made up of manuals, processes, procedures, instructions and standards, among other binding documents.

Scope and Application Framework

The guidelines contained herein shall apply to members of the Board of Directors, Senior Management and collaborators at GRUPO SURA (hereinafter referred to as "the Company"). This policy will also be extended to suppliers who access, preserve and manage company information.

General Objectives

- Developing and implementing an information security model that allows the Company to manage the risks related to the management of information and to comply with all legal and contractual requirements in such matters.

- Defining and implementing best practices geared towards adequately protecting the information that the Company receives, generates and stores through different means (physical or digital).

- Creating a company culture that promotes information security and cybersecurity risk management.

General Guidelines

- The Vice-Presidency of Corporate Affairs shall define the structure and guarantee the necessary resources for the implementation of an Information Governance model geared towards the implementation of the risk identification, analysis, evaluation, management, monitoring and reporting mechanisms of the risks associated with information security and cybersecurity.

- Senior Management is responsible for promoting the management of information security and cybersecurity risks guidelines, incorporating them into the Company's strategic plans, ensuring the adoption of an Information Governance model and the availability of the resources required for this purpose.

- Processes and procedures should be established for the proper management of information security and cybersecurity risks as well as contemplating the stages of prevention, protection, detection, response, communication, recovery and learning.

- Collaborators and suppliers that access and/or manage information held by the Company are responsible for identifying, evaluating and classifying the information as well as guaranteeing its protection and conservation, applying any necessary controls to protect it from all security and cybersecurity risks to which it may be exposed.

- There shall be a Security Information and Cybersecurity Committee which will be accountable for the strategy and continuous improvement of the Information Governance Model.

- The information governance model that is defined and implemented shall respond to the particular needs of the Company and shall be reviewed and updated by the Information Security and Cybersecurity Committee, at least once every year or every time circumstances call for it.

- The Company shall have a personal data protection policy protecting all information gathered from shareholders, investors, suppliers, employees and any other natural person in contact with Grupo SURA, as well as establishing the necessary procedures for the proper management of the personal data contained in its databases.

- It is mandatory for all recipients of the present policy to report any security events or incidents.

- Recipients of this Policy shall report any anomaly or event that may potentially impact information held by the Company's information to the Internal Services area at notificaciones_seguridad@gruposura.com.co

- All incidents or events shall be logged, verified, classified, prioritized, analyzed and investigated following appropriate procedures.

- Documentation on information security or cybersecurity incidents or events shall be treated as confidential information. This information shall also be used to prevent or manage future incidents.

- The Corporate Legal Affairs, Compliance, Corporate Risks and Internal and Shared Services areas shall participate in any decision on information security event that merits contact with the authorities or that calls for legal action.

- An information security and cybersecurity risk assessment shall be implemented and results shall be notified to the Risk Committee of the Board of Directors no less than once a year.

Training and Culture

The Company shall establish a training strategy aimed at promoting a culture based on the proper treatment and protection of information and applying any relevant guidelines addressed to the recipients of this policy.

Governance

The Board of Directors of Grupo SURA shall approve this policy and any amendments thereof. Monitoring and updating shall be the responsibility of the Internal and Shared Services area.

Disclosure and update

This policy shall be disclosed to The Members of the Board of Directors, Senior Management, collaborators and suppliers who manage the information held by the Company. It shall be updated in line with organizational changes, legal provisions or other aspects that may affect the guidelines set forth herein.