

## GENERAL POLICY FOR INFORMATION SECURITY

At Grupo SURA (hereinafter the Company) information is considered a strategic asset for carrying out our business. This is why it is imperative to recognize that adequate treatment of information poses major challenges and tasks that require responsible planning, organization, management, preservation, and protection, to ensure its availability, integrity, and confidentiality. This directive complements national and international regulations, and sets forth the general and specific guidelines that define the action framework with respect to the security of information in the Company.

### Scope and framework of application

The provisions and guidelines established herein must be followed by employees, suppliers, members of top management, members of the boards of directors (“Directors”), and by anyone who has access to Company information.

### General guidelines

- Everyone who has access to Grupo SURA’s information must act in compliance with the provisions and guidelines established in this policy and in the other internal and external regulations that develop and/or complement them.
- Users who access and/or manage Grupo SURA’s information are responsible for applying the necessary controls to avoid loss, change, or unauthorized disclosure, and for protecting the information from all security risks to which it might be exposed.
- Members of top management will be in charge of defining the guidelines to manage information security risks, including them in the Company’s strategic plans, and ensuring that the resources necessary for the purpose are made available.
- The Company, through the Corporate Affairs Vice Presidency, will define the structure and necessary resources, and will staff the same with trained personnel with decision-making power to implement the information security system, and to apply the mechanisms identified for identification, evaluation, mitigation, and control.
- The information security system development must respond to the Company’s specific needs, and will be reviewed and updated on a regular basis, to ensure it is effective and timely
- The Company must have a data protection policy that makes it possible to protect the information obtained from shareholders, investors, suppliers, employees, and any other individual who has contact with Grupo SURA. In addition, it must

establish the necessary procedures for managing the personal data contained in the Company’s databases.

### Specific guidelines

### **a) Information security incident or event management**

- The Company, through its Vice Presidency for Corporate affairs, will define the area in charge of hearing, investigating, and providing a timely response to all information security incidents that occur.
- Security event or incident reports are mandatory for all recipients of this policy.
- All incidents or events must be recorded, verified, classified, prioritized, evaluated, and investigated according to the procedure defined for that purpose.
- Each incident must be treated according to its impact, following the established procedure, and ensuring that the action plans established for the solution of the incident receive follow-up.
- Documentation about information security incidents or events must be treated as restricted information. This information must be taken into consideration to prevent future incidents.
- Any decision about information security events that justifies contacting the authorities or give rise to legal action, must include the participation of the Management for Legal Affairs and Compliance, and the Directorate for Internal and Shared Services.

### **b) Education and culture:**

- The Company must define an education strategy focused on the recipients of this policy, to promote a culture based on the appropriate treatment and protection of information, applying the guidelines defined for that purpose.

### **Governance**

This policy must be approved by Grupo SURA's Presidential Committee and any changes to the policy must be approved by that same body. Monitoring and updating this policy will be the responsibility of the Vice Presidency for Corporate Affairs.

### **Dissemination and updates**

this policy will be disseminated to every employee, supplier, member of top management, director, and anyone who has access to and/or manages Grupo SURA's information, and will be updated according to the organizational changes, legal provisions, or other aspects that might affect the guidelines established herein.