I. INTRODUCTION

For GeoPark, information is a strategic asset that must be sufficiently protected to ensure business continuity, legal and regulatory compliance, and the trust of our customers, suppliers, partners and other stakeholders. Accordingly, we have established this information security policy that defines the principles, objectives, roles and responsibilities that govern the management of information security in our organization.

II. OBJECTIVE

- To preserve the confidentiality of information, preventing it from being accessed by unauthorized persons, entities, or processes
- To preserve the integrity of information, preventing it from being modified, manipulated or reproduced by unauthorized persons, entities or processes
- To preserve the availability and continuity of information and associated services, ensuring that they are accessible when required by authorized persons, entities or processes
- To guarantee the non-repudiation of information, ensuring that its origin and destination are verifiable and that it has not been altered in transit
- To comply with legal and regulatory obligations applicable to information and information security, as well as contractual and business requirements established by the organization and its stakeholders
- To improve the culture of information security in the organization, promoting commitment, responsibility and awareness of all members of the organization and related third parties

III. SCOPE

This policy applies to all information owned, processed, transmitted, or stored by GeoPark, regardless of its format, medium, or location. It also applies to all employees, contractors, consultants, partners, and third parties who access, use, or manage GeoPark information, or who provide information security-related services to the organization.

IV. GENERAL

Information security at GeoPark is based on the following principles:

- Information is an organizational asset that must be identified, classified, inventoried, and protected according to its value, criticality, and sensitivity.

- Information security is the responsibility of all members of the organization, who must comply with the policies, standards, procedures and good practices established for this purpose.
- Information security is managed comprehensively, considering technical, organizational, human, legal and ethical aspects.
- Information security aligns with the organization’s strategic objectives and is part of business, risk management, and continuous improvement processes.
- Information security is based on the NIST international framework, which includes identifying, protecting, detecting, responding to, and recovering from cyber threats.
- Information security is maintained through training, awareness, auditing, review, and regular updating of the protection measures implemented.

V. POLICY

This Policy establishes the necessary guidelines to implement, maintain and improve GEOPARK information security management so that it protects the Company’s information resources.

The following areas guarantee the above principles:

- **Computer access control**

  To prevent unauthorized access to computer systems, databases, or computer services, processes in place control the assignment of access rights. Information access authorizations are grouped into access profiles according to the activities associated with each role, ensuring the segregation of duties.

  Objectives

  - To prevent unauthorized access to computer systems and implement security mechanisms for user access
  - To record and review critical events and activities carried out by users in GeoPark systems

- **IT Security Management**

  Information systems and networks are important assets. To minimize the risk of damage to operational systems, they are kept properly updated and configured through reviews and a process of applying patches.

Objectives

- To ensure the security of computer systems
- To keep systems up to date with patches covering the latest vulnerabilities detected, as appropriate to operational needs
- To maintain systems configured with current security policies and standards (operating systems, databases, applications, etc.)

System Development and Maintenance

The development and maintenance of systems is a critical security point. Since software can be breached with the aim of causing incidents or anomalies, processes are implemented for changes in programs to follow a controlled flow.

Objectives

- To ensure the inclusion of security controls and data validation in the development or acquisition of computer systems
- To define and document the controls to be applied during the life cycle of systems and in the base infrastructure on which they are supported

Operations Management

Complete and appropriate information processing requires effective data processing management. Therefore, operations processes are defined and implemented for secure management of scheduled processing.

Objectives

- To ensure the proper and safe operation of facilities where information is processed and transmitted
- To establish responsibilities for data processing management and operation, including operational instructions and separation of duties

Communications Management

Computer systems communicate with each other, both within GeoPark and with third parties. Therefore, security mechanisms are established to ensure the confidentiality, integrity and availability of the information that is issued or received when exchanging data.

Objectives

- Establish special controls to safeguard the confidentiality and integrity of information that flows through GeoPark networks.

Physical Security

Physical security provides mechanisms to minimize the risks of damage to GeoPark. Therefore, security perimeters are applied to computing resources to prevent risks of unauthorized physical access. All GeoPark data processing centers have access restriction mechanisms.

Objectives

- To prevent and impede unauthorized access, damage or interference in computer processing areas
- To protect GeoPark's critical processing equipment by placing it in secure areas protected by a defined security perimeter, with appropriate security measures and access controls

IT Service Continuity Management

Contingency plans are implemented to ensure that all activities supported by information technology are restored within reasonable periods of time in the event of unexpected service interruptions and with the minimum levels of data loss tolerated by the business.

Objectives

- To minimize the effects of potential disruptions to GeoPark's normal operations (whether resulting from natural disasters, accidents, equipment failures, deliberate actions, or other events) and protect critical processes through a combination of preventive controls and recovery actions
- To analyze the causes of the interruption of the service and take the corresponding measures to prevent similar events in the future

Systems Security Review

Audit logs of critical security activities, exceptions, and events are produced and maintained. Processes are implemented to review these records and guarantee compliance with computer security processes.

Objectives

- ○ To control security events
- ○ To keep a record of critical system activities
- ○ To audit compliance with computer security processes

Asset Management

All Information Technology resources (hardware and software) used by GEOPARK and/or related companies are for GeoPark's business use. The use of any of them for other purposes, in principle, is not allowed. However, the Company allows the use of these resources for personal purposes, on the condition that such use does not affect the productivity of the person or persons who share the resources and that the restrictions detailed in this Policy are complied with.

Objectives

- ○ To control and document information on Hardware and Software configurations, computer tools will be used for the identification and control of computer equipment. The information generated will complement the Company's inventory management process
- ○ The installation and/or use of software that is not duly authorized by IThink is not permitted
- ○ The computer and communications resources that GEOPARK makes available to its employees are intended to be used for work activities. Occasional personal use is permitted, on the condition that it does not affect productivity and information security

Information Security Incident Management

Events in which incidents could potentially compromise information security will be monitored.

Objectives

- ○ To have the capability to detect and block intruders and attempts to access information or systems, to have the capability to perform tracking and identification tasks and forensic analysis on the computer systems where incidents have occurred
- ○ When merited by the seriousness of an incident and/or when an incident exceeds the response capacity of the internal team, a specialized company will be hired to resolve the situation

Supplier Relations

Suppliers must adhere to GeoPark's information security requirements.

Objectives

- Suppliers must comply with the Information Security Policy
- Suppliers must implement, if necessary, security controls that protect the Company's information under their responsibility

 Information Security Awareness

Awareness actions related to information security will be created and maintained for all GEOPARK employees.

Objectives

- To coordinate periodic awareness campaigns and actions

VI. ROLES AND RESPONSIBILITIES

The roles and responsibilities related to information security at GeoPark are as follows:

- Senior management is responsible for approving, disseminating and enforcing this policy, as well as allocating the necessary resources for its implementation and maintenance.
- The information security officer is responsible for coordinating, executing and monitoring information security activities in the organization, as well as advising, training and raising awareness among the other members of the organization and related third parties.
- Process managers are responsible for identifying, classifying and protecting the information they create, process or store in their respective processes, as well as for reporting and managing information security incidents that affect them.
- Information users are responsible for complying with this policy and with the standards, procedures and good information security practices that apply to them, as well as for reporting any situation or incident that puts the security of the information at risk.
- Information security service providers are responsible for complying with the information security requirements established by the organization and by the service level agreements subscribed, as well as for reporting and managing information security incidents that affect them.

VII. VERSION CONTROL TABLE

Version	Date	Author	Description
2	01/09/2016	IT Area	Document creation
3	25/06/2024	Richard Garcia Information Security Manager	Policy Review and Update