GEOPARK

| Document | 01 Política | Name | Information Security Policy |
|---|---|---|---|
| System | 03 Finanzas | Sub-System | 05 IT |
| Code | 03-05-102 | | |

| Issuance Date | Effective Date | Prepared by | Approved by | Version N° | Page |
|---|---|---|---|---|---|
| 04/08/2025 | 04/08/2026 | Lina Gantiva (Líder de Gobierno y Cumplimiento) | Cinthya Sánchez (Directora IThink) | 03 | 1 de 17 |

## I. OBJECTIVES

The purpose of this policy is to comply with the legal and regulatory obligations applicable to information and information security, as well as with the contractual requirements of the business established by the organization and its stakeholders, ensuring:

- The protection of the confidentiality, integrity, and availability of information.
- The implementation of proactive measures to restrict unauthorized access and protect information that is sensitive to GeoPark. Our objective is to protect data from potential threats and attacks, and ensure its confidentiality, integrity, and availability. This ensures that only authorized people and systems can access information, keeping our most critical assets safe.
- That awareness is increased among employees, contractors and suppliers about cybersecurity risks and basic security knowledge, skills and experience, to encourage commitment, responsibility and awareness among all members of the organisation and related third parties.
- The preservation of information and telecommunications systems, enhancing prevention, detection, reaction, analysis, recovery, response and investigation capacities regarding new threats.
- The strengthening of data governance and information security in the organization, ensuring the reliability, availability, and integrity of information assets, and promoting a culture of accountability and regulatory compliance.
- The creation of mechanisms and processes to record and document the origin, transformation, use, and destination of data throughout its entire lifecycle.
- That structuring, governing, and optimizing our organization’s data assets, as well as its Data Security Management and Data Storage and Operations Management, is considered critical.
- The creation of clear roles and responsibilities for data management and the continuous improvement of data quality, along with the alignment of business objectives.

## II. SCOPE

This policy applies to all information generated, processed, stored or transmitted as part of GeoPark’s activities, as well as to the systems, technologies and processes used to manage it. It is mandatory for all employees, contractors, suppliers and third parties who access corporate information, regardless of their geographical location or the means used for such access.

Information protection encompasses both physical and digital environments and includes all levels of data sensitivity and criticality according to classification definitions set by the organization.

## III. GENERAL

### DEFINITIONS

- **Information Security:** The set of principles, policies, processes, and controls designed to protect GeoPark's information, ensuring its confidentiality, integrity, and availability, as well as business continuity and regulatory compliance.

- **Information:** Any data generated, processed, stored, or transmitted by GeoPark, regardless of format, medium, or classification level, that has value to the organization and must be protected.

- **Confidentiality:** The principle that ensures information is accessible only to duly authorized persons, systems, or processes, preventing unauthorized disclosure.

- **Integrity:** The principle that protects the accuracy, consistency, and completeness of information and processing methods, preventing unauthorized or accidental modifications.

- **Availability:** The principle that ensures information and associated assets are accessible and usable by authorized users when required by the business.

- **Information Assets:** Anything that has value to GeoPark and requires protection, including information, databases, documents, hardware, software, services, technological infrastructure, and networks.

- **Information Classification:** The process by which information is categorized according to its level of sensitivity and criticality in order to define appropriate security controls. The categories include:

  - Public
  - Restricted (Internal / External)
  - Confidential
  - Strictly Confidential

- **ISMS (Information Security Management System):** A systematic and documented framework of policies, procedures, and controls that enables the management of information security risks at GeoPark, aligned with standards such as ISO and NIST.

- **Information Security Incident Management:** A structured process to detect, analyze, contain, eradicate, recover from, and learn from events that may

compromise information security, incorporating continuous improvement of data governance.

- **Information Security Incident:** A real or potential event that compromises or threatens the confidentiality, integrity, or availability of GeoPark's information or systems.

- **Data Owner:** The role responsible for ensuring that data is properly managed in compliance with regulations, including its classification, access control, authorized use, lifecycle management, and strategic alignment.

- **Encryption:** A cryptographic mechanism that transforms information into an unreadable format to protect it from unauthorized access, both in transit and at rest.

- **Vulnerability:** A weakness in a system, process, software, hardware, or human factor that may be exploited by a threat to compromise information security.

- **VPN (Virtual Private Network):** Technology that enables a secure and encrypted connection over public networks, allowing remote access to GeoPark's corporate resources under established security controls.
- **Cloud:** A model for storing and accessing data and services over the internet

- **SLA (Service Level Agreement):** A contract or part of a contract that defines the level of service a provider (internal or external) commits to delivering to a customer.

- **IT (Information Technology):** The department or set of functions within an organization responsible for managing, operating, and maintaining the technological infrastructure (hardware, software, networks, systems) that supports business operations.

## SECURITY PRINCIPLES TO PROTECT OUR BUSINESS

GeoPark establishes guidelines to implement, maintain, and improve information security management that align with fundamental security principles:

- **Confidentiality**: Ensuring that information is accessible only by authorized individuals.
- **Integrity**: Protecting the accuracy and completeness of information and processing methods.
- **Availability:** Ensuring that authorized users have access to information and associated assets when needed.
- **Risk Management**: Managing information security through a formal process of risk assessment and procedure.
- **Regulatory Compliance**: Ensuring that all information security activities comply with relevant laws, regulations, and contractual requirements.

- **Awareness and Training:** Raising awareness and training all staff in their information security responsibilities.

Information security is based on the NIST international framework that covers the phases of identifying, protecting, detecting, responding to, and recovering from cyber threats. Information security at GeoPark is a strategic pillar, especially given the sensitivity and value of the data we handle in the oil and gas sector. While Cybersecurity and IT decide on policies and tools, the effectiveness of our security position depends on the shared responsibility of each employee as data custodians.

The following principles aim to guide each worker in their daily data custody duties, ensuring that protecting our data assets is inherent in all activities:

- Principle of Individual Responsibility
- Principle of Purpose and Minimum Access
- Principle of Confidentiality
- Principle of Integrity: Preserving Accuracy
- Principle of Availability: Ensure Timely Access
- Principle of Awareness and Vigilance
- Principle of Regulatory Compliance and Internal Policies

## SAFETY AND USAGE RULES FOR GEOPARK PERSONNEL

GeoPark establishes security standards for its employees, partners, and third parties to protect the Company's information resources and ensure the security principles that protect our business, workstations, and mobile devices used to conduct business or that are connected to the internal network. The purpose of these standards is to protect data and technology and information assets from loss, modification or destruction.

## LOGICAL SECURITY (CLASSIFICATION AND DATA PROTECTION)

Information security is a fundamental principle at GeoPark. To ensure satisfactory data protection, there is a periodic information classification review that represents an integral part of the Data Governance model and reinforces each employee's data custody responsibilities.

Access management is essential in the protection of information and systems, both individually and by role. GeoPark implements processes to control the allocation of access rights, prevent unauthorized access, properly authenticate users, and log and audit relevant events. These guidelines, along with the definition of strong passwords, are detailed in the **Password Policy,** a key document regarding the application of these controls. **The classification of information and security controls** applicable to each category are defined in **Annex 1**.

## PHYSICAL SECURITY

Physical security provides mechanisms to minimize the risks of damage to GeoPark. Security perimeters are applied to computing resources to prevent risks of unauthorized access. All GeoPark data processing centers have access restriction mechanisms in protected areas and are protected by defined security perimeters, with appropriate security measures and access controls.

GeoPark will decide on conducting specific guidance on maintaining the physical security of its workstations, mobile devices, and work areas, and maintaining safety while traveling.

## ASSET MANAGEMENT

All information technology resources (hardware and software) belonging to GeoPark and/or related companies are provided exclusively for use in GeoPark business. Any other use is not permitted, in compliance with the restrictions established in this policy:

- Identification and control tools will be used to control records of computer equipment with information on Hardware and Software configurations. 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 made available by GeoPark to its employees are intended to be used for work activities. Occasional personal use is permitted, and the Company acknowledges that minimal and sporadic personal use may be unavoidable or even beneficial to employee morale. However, this permission is strictly conditioned on two critical points:

    - **Zero Effect on Productivity:** This means that personal use should not interfere with job responsibilities, cause work delays, or take up significant time that should be spent on Company tasks.
    - **Zero Effect on Information Security:** This is the most critical condition from the cybersecurity perspective, and means that personal use must not, under any circumstances, jeopardize the confidentiality, integrity, or availability of Company information. This includes:
        - Not visiting malicious websites or downloading content that could have malware or viruses.
        - Not sharing Company credentials or information.
        - Not storing excessive or personal information unrelated to work that may compromise the Company's ability to manage its assets.
        - Not using unapproved personal cloud services to handle corporate data.

- Access management and control for privileged users and their respective withdrawal when the employee or contractor no longer needs access: Access rights will be reviewed on a regular basis to ensure continuity of business need and the revalidation of privileges.

**Access control to applications and systems:** use secure login procedures to control access to applications and systems, including multi-factor authentication.

*Using encryption*

- Use encryption based on risk criteria, such as sensitivity or information classification.
- Protect data in transit on public and private networks and secure information stored in applications or systems to mitigate threats.
- Protect and encrypt cryptographic passwords throughout the password management lifecycle.

GeoPark understands that, from time to time, our employees may need to make limited personal use of Company assets. Our goal is to create an environment of trust and productivity, while protecting GeoPark's resources and ensuring compliance with our policies.

## INFORMATION 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 a review and patching process. This is anticipated to guarantee the security of computer systems, keep systems updated with patches that cover the latest vulnerabilities detected, as appropriate to operational needs and in accordance with respective security policies and current standards (operating systems, databases, applications, etc.).

## SYSTEM DEVELOPMENT AND MAINTENANCE

Given that software can be breached with the intention of causing incidents or anomalies, processes are in place for changes in programs follow a controlled flow. This ensures the inclusion of security controls and validates the protection of our information assets. The privacy of personal and sensitive data must be inherently considered in the entire life cycle of our system development and maintenance and not just added as afterthoughts.

Information security and data privacy are not optional at GeoPark and are fundamental pillars that must be integrated from the beginning of each project. To do this, we adhere to best practices and key considerations that are defined in **Annex 2**.

## OPERATIONAL MANAGEMENT SECURITY

Comprehensive and appropriate information processing requires effective data processing management. Accordingly, operational processes are defined and implemented for the secure administration of the programmed data handling, guaranteeing the appropriate and secure operation of the facilities where information is processed and transmitted, the respective establishment of responsibilities for their management and operation, including operational instructions and the separation of functions.

Daily IT operations must follow secure procedures, including managing changes, backups, and event monitoring.

- Maintain operational procedures and make them available to relevant users.
- Operational procedures may include:
  - Installation and configuration of applications and systems
  - Start-up and closing procedures
  - Authentication and authorization management
  - Maintenance and support procedures
  - Information handling procedures, including automated and manual activities
  - Problem determination and management
  - Logging and monitoring
  - Communication with support and escalation contacts
  - Security Incident Management
  - Security Testing
  - Vulnerability and patch management

## COMMUNICATIONS MANAGEMENT

At GeoPark, there are interactions between various computer systems, both internally and with third parties. Security mechanisms are in place to ensure that the exchange of data in these communications is carried out under conditions that guarantee the confidentiality, integrity and availability of the information. Accordingly, specific controls are applied to protect the information that transits through GeoPark networks.

## IT SERVICE CONTINUITY MANAGEMENT

Contingency plans are implemented to ensure that all IT-supported activities are restored within reasonable timeframes in the event of unexpected service interruptions and with the lowest possible levels of data loss tolerable by the business.

The effects of possible interruptions to GeoPark's normal activities (whether these are the result of natural disasters, accidents, equipment failures, deliberate actions or other

events) are therefore minimized and critical processes are protected through a combination of preventive controls, recovery actions, analysis and corresponding measures to prevent similar events in the future.

## PHYSICAL AND ENVIRONMENTAL SECURITY

Audit logs are made and kept of critical security activities, exceptions, and events. Review, auditing and control processes for events and records of critical activities are implemented to guarantee compliance with information security processes.

- Locate infrastructure assets in controlled access areas, except those intended for public use.
- Apply risk-based access controls, which may include blocking or protecting areas to:
    - Allow access only to authorized persons
    - Uphold physical security during power outages
    - Keep access logs

## INFORMATION SECURITY INCIDENT MANAGEMENT

Events in which incidents that could potentially compromise information security are monitored to detect and block intruders and attempts to access information or systems, and to carry out tracking and identification tasks and forensic analysis on systems where the incidents have occurred.

## SECURITY INCIDENT RESPONSE

GeoPark's ability to respond effectively to security incidents is crucial. However, an effective response goes beyond the immediate mitigation of harm. To continuously strengthen our security position and data governance, we explicitly integrate incident management into the continuous improvement cycle of data governance. This approach aligns with best practices from recognized standards.

When justified by the severity of an incident and/or when an incident exceeds the response capacity of the internal team, the services of a specialized company will be hired to ensure its resolution and carry out the corresponding evaluation, review and updates to incorporate the lessons learned in this constantly evolving area.

A team comprised of the Cybersecurity Incident Response Team (CSIRT) and the Cybersecurity team meets to evaluate information about new and previously reported incidents. Incidents will be delegated to the appropriate persons for evaluation, investigation and resolution.

The Security Operations Center (SOC) monitors threats to the Company's networks and systems. The SOC uses various threat intelligence sources to identify, monitor, and

address internal threats, and has access to a broad range of advanced detection and response technologies.

Details on the incident life cycle and how it drives improvement in data governance are found in **Annex 3**.

## INFORMATION SECURITY AWARENESS

GeoPark will provide annual mandatory and customized cybersecurity training to all employees, covering aspects such as how to recognize, avoid and report suspicious activity and/or potential security incidents, which can range from lost mobile phones to laptop malware, phishing incidents, and misdirected emails. The team will request permission to hold phishing drills to assess and prepare employees to recognize and respond to email threats. Employees will also receive guidance and training on the use of Company assets to help them understand security risks and comply with IT policies.

## REMOTE ACCESS SECURITY POLICY

The Remote Access Security Policy establishes the rules and procedures in remote access to the corporate network and internal systems, which is only allowed through secure connections (VPNs) with strong authentication and from devices that comply with the Company's security standards.

## BACKUPS

Backups are managed with a frequency aligned to the **"Backup Policies"** document in which all the machines that are in the Azure cloud have a Snapshot Policy configured. The policy applied depends on the service provided by each machine, to protect data by ensuring its availability and recovery in case of loss or failure.

## STORAGE MEDIA

This refers to protecting information stored on physical devices (such as hard drives, USBs, etc.) and cloud storage systems or restricting their use through a range of measures from the use of strong passwords to data encryption and access management to prevent unauthorized access, data loss and other threats.

## EXTERNAL INFORMATION SYSTEMS

Systems or components over which the organization has no direct control or oversight in the application of safety requirements and controls, or in the evaluation of their

effectiveness. These systems may include personal devices, private communication devices, or systems belonging to third parties with which the organization interacts.

## POLICY COMPLIANCE

GeoPark employees will comply with the security policy, which will be defined, shared, published and accepted by each employee, contractor or third party, safeguarding the information created, processed, transmitted by their business processes to minimize financial, operational or legal impacts due to its incorrect use.

## ROLES AND RESPONSIBILITIES

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

- Senior management is responsible for approving the policy, making the policy known and enforcing it, as well as allocating the resources necessary for its implementation and maintenance.
- The head of Cybersecurity is in charge of 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 generate, 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 information security 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 to, as well as for reporting and managing information security incidents that affect them.

- The Data Owner is critical to the security and compliance of our information. This role not only centralizes accountability, but also actively strengthens our security position by ensuring that data is managed with the highest protection possible and in compliance with regulations.

  Data Owner responsibilities are:

  - Classifying data
  - Defining access controls
  - Authorizing third-party access
  - Lifecycle data management
  - Approving uses and purposes

- Strategic alignment
- Participating in incident management

## GeoPark Security Policy Compliance

GeoPark's Information Security Policy is not just a set of guidelines, but an active commitment to protecting our most valuable assets. We have implemented a comprehensive framework for evaluation and continuous improvement to guarantee both effectiveness and consistent compliance. Reviews and the measurement of key performance indicators support this framework.

### Consistent Verification and Validation

Compliance with our security policy will be systematically evaluated through:

- **Periodic Reviews:** The implementation and effectiveness of our security policies and procedures will be reviewed annually. These assessments, conducted by teams or trained personnel within GeoPark, will allow us to proactively identify areas for improvement, detect potential deviations, and ensure that our controls operate as expected.

### Key Compliance Indicators (KPIs): Measuring Performance

To ensure that our Information Security Management System is dynamic and data-driven, we will establish and monitor **Key Performance Indicators.** These KPIs will allow us to quantitatively measure the effectiveness of our security policy and the degree of compliance throughout the organization. The results of the KPIs will be reviewed regularly by senior management to make informed decisions and allocate resources strategically.

Examples of relevant KPIs include the following:

- Percentage of security incidents resolved within SLA times
- Quantity of critical vulnerabilities identified and remediated
- Compliance rate in safety training and staff awareness
- Results of penetration tests and vulnerability assessments
- Percentage of data classified correctly and with up-to-date revisions
- Compliance with third-party access controls as set forth in contracts and policies

### Commitment to Continuous Improvement

Evaluation through audits and KPIs is central to our commitment to continuous improvement. Audit findings and KPI analysis are not just reports; they are the engine that drives the constant review, updating and optimization of our security policies, procedures and controls. This feedback loop allows us to adapt to new threats, technologies, and

business and regulatory requirements, ensuring that our security position always remains resilient and effective.

Information security is a shared responsibility and an ever-evolving process at GeoPark, and compliance is assessed to ensure that everything we value is protected.

*Failure to comply with the Information Security and Privacy policy entails legal consequences arising from the entity's regulations and applicable national and territorial laws on information security and privacy. These consequences can include disciplinary sanctions, fines, and legal action by affected third parties.*

## ANNEXES

### ***Annex 1***

*Logical Security (Data Classification and Protection)*

- **Classification and security controls,** appropriate to different categories of information, data, and assets. All information must be classified according to its sensitivity and criticality (Public, Reserved, Confidential, Strictly Confidential) to determine the level of protection required.

- **Public**: Information suitable for sharing both internally and externally, which does not represent an operational impact or risk to the continuity of GeoPark activities.
- **Reserved**: Information for the exclusive use of GeoPark personnel and/or its suppliers or partners. Unauthorized disclosure could have a negative impact on GeoPark's operation. Only the person who applies the label can remove it.

    - ***Reserved/External***: Information for the exclusive use of GeoPark personnel and its partners or external suppliers.
    - ***Reserved/Internal:*** Information for the exclusive use of GeoPark personnel. It cannot be accessed by external personnel (neither geopark.com nor ext.geo-park.com).

- **Confidential**: Information that can only be used by specific personnel in an area as its unauthorized disclosure, even within GeoPark, could have a negative impact on operations. Only the person who applies the label can remove it.
- ***Confidential/Area:*** Information only accessible by people in an area.
  ***Note***: Each area shall have its own sub-tag, restricting access to the tagged information to whoever is part of that area.

- **Strictly Confidential**: Information whose distribution is limited to internal or external users authorized by the person who applies the label. Its unauthorized disclosure could have a serious negative impact on GeoPark's operation.
- The person who applies the tag shall define custom permissions for internal or external users. Such permissions can be:

- Viewer: The user can see contents but cannot edit, print, copy content, or change or remove protection.
    - Restricted Editor: The user can view and edit but cannot print, copy content, or change or remove protection.
    - Editor: The user can view, edit, print, and copy content, but cannot change or remove the protection.
    - Owner: The user can do anything with the document, including removing the protection.

***Annex 2***

*Best practices and key considerations:*

1. **Proactive versus Reactive Approach:**
   - Security and privacy are anticipated and prevented. We do not wait for incidents to occur or compliance issues to arise to act. From the conception of a system, security and privacy risks are identified and mitigated.

2. **Privacy by Default:**
   - GeoPark systems and applications must be configured by default to offer the highest possible level of privacy, especially in the processing of personal data. This means that the default settings should be the most restrictive, minimizing data collection, use, and disclosure.

3. **Security and Privacy Built into the Design:**
   - Security and privacy considerations are built into every phase of the software development lifecycle (SDLC), from planning and design, through coding, testing, deployment, to operation and decommissioning. This includes:
     - **Requirements analysis:** Identification of security and privacy needs from the beginning.
     - **Secure Design:** Implementation of secure architectures and design patterns.
     - **Secure coding:** Using secure programming practices to prevent common vulnerabilities.
     - **Security testing (SAST, DAST, penetration testing):** Conducting extensive testing to identify and fix security and privacy flaws prior to deployment.

4. **Visibility and Transparency:**
   - Data processing processes, as well as the security and privacy measures in place, must be transparent and understandable. This makes it easier for users to audit, comply and trust.

5. **Full Information Lifecycle:**
   - Security and privacy must be applied throughout the entire data lifecycle, from data collection and storage to processing, use, transfer, and secure disposal. This includes properly managing data retention.

6. **End-to-End Security:**
    - Security should protect all points in the data value chain, from the user interface to the database and any external systems that the application interacts with. This involves securing communications, and data storage and processing.

7. **Respect for the User:**
    - Wherever possible, systems should be designed to empower users (internal and external) with control over their data, making it easier to exercise rights such as access, rectification, erasure and portability of their personal data.

***Annex 3:***

*Incident Lifecycle as an Engine of Improvement:*

For GeoPark, every security incident, no matter how large, is an opportunity to strengthen capabilities, policies, and processes. As such, the incident management lifecycle is directly integrated into our continuous improvement approach, aligned with ISO/IEC 27035 principles and data governance.

**1. Preparation**

- **Data Governance**: Definition of roles and responsibilities, establishment of information classification policies and training of personnel in data custody.
- **Security**: Preparation of response plans, development of toolkits, safe communication and incident drills.

**2. Detection and Analysis**

- **Data Governance**: Involvement of data administrators to detect anomalies by knowing normal usage patterns and metadata traceability.
- **Security**: Continuous monitoring, log analysis, use of detection tools (IDS/IPS), and forensic analysis.

**3. Loss and Recovery**

- **Data Governance**: Prioritization of containment actions according to the classification of information, ensuring reliable restorations.
- **Security**: Incident isolation, threat elimination, secure service restoration, patching, and compensatory controls.

**4. Post-Incident (Lessons Learned and Continuous Improvement)**

- **Post-Incident Analysis**:
  - Evaluation of root causes and control failures.
  - Review of response effectiveness.
- **Adjustments to Data Governance**:
  - Review of handling, access and classification policies.
  - Improvement of flows, processes and tools.
  - Strengthening the role of the Data Administrator.
  - Re-evaluation of the information risk map.
  - Adjustments to data architecture for greater resiliency.
- **Technical Security Improvements**:

- New technologies, additional controls, and adjustments in monitoring and detection.

- **Data Classification Review**:
  - Re-evaluation of the sensitivity of the exposed data and corresponding adjustments.

## IV. REFERENCIAS

XX XX XX Política De Ciberseguridad.

## V. TABLA DE CONTROL DE VERSIONES

| Versión | Date | Author | Summary of Changes |
|---|---|---|---|
| 1 | 10/09/2016 | IT Area | Document creation |
| 2 | 14/07/2024 | Information Security Manager | 2024 Review and Update |
| 3 | 04/08/2025 | Governance & Compliance Leader | 2025 Review and Update |

| Responsibility | Name | Charge |
|---|---|---|
| Update | Lina Gantiva | Governance & Compliance Leader<br>Firmado por: Lina Gantiva López<br>63408619558E4C2...<br>8/4/2025 |
| Review | Edgardo Arrieta | Cybersecurity & Compliance Manager<br>Firmado por: Edgardo Arrieta<br>5BF8ADDC66D44DC...<br>8/4/2025 |
| Approval | Cinthya Sánchez | IThink Director<br>Signed by: Cinthya Sánchez<br>7E1C6D5F76134B8...<br>8/4/2025 |