PROMIGAS	Corporate Information Security and Cybersecurity Policy	
Version: 13	Code: GNA-1656	Status: Current
Prepared by: Vanessa Rosales Gonzalez	Reviewed by: Henry De La Hoz	Approved by: Jimena Arango Pilonieta.
Position: Professional	Position: Professional	Position: Manager

TABLE OF CONTENTS

1. OBJECTIVES

1.1 GENERAL OBJECTIVE

To protect the information assets of Promigas and related companies, by managing and complying with the general principles that preserve information by defining policies, identifying risks and controls that establish roles and responsibilities of the key players involved in the Information Security Management System (ISMS).

1.2 SPECIFIC OBJECTIVES

- To establish guidelines to maintain confidentiality, integrity, availability and privacy of information and cybersecurity in Promigas and related companies.
- To define how information should be protected in a standardized manner based on the valuation of the critical information assets of Promigas and related companies.
- To ensure the Information Security and cybersecurity risk management in Promigas and related companies.
- To establish and implement controls that preserve the confidentiality, integrity, availability and privacy of information in Promigas and related companies.
- To determine roles and responsibilities of control authorities regarding the Information Security and cybersecurity pillars of Promigas and related companies.
- To guarantee the implementation of Information Security and cybersecurity requirements for business continuity and disaster recovery in Promigas and related companies.
- To define the general framework for managing the Information Security Management System (ISMS) in accordance to the business requirements and in line with the guidelines established in this corporate policy.

2. SCOPE

This is a corporate policy, so it applies to Promigas and related companies; and therefore to all direct and temporary employees, suppliers and contractors who in the performance of their duties use information and technological services of Promigas and related companies, regardless of their location, and shall abide by it according to the nature, size, complexity and structure of their operations.

Cases wherein it is not possible to totally or partially apply it must be reported as soon as any impediment is known, to the leader of the corresponding process, to the Information Security professional or to the risk and compliance management.

When this Policy refers to "PROMIGAS" or the "Company", it refers to PROMIGAS and related companies, i.e., companies controlled by Promigas, as defined in Document Management Standard **GNA-002-S1.**

3. DEFINITIONS

See Promigas Information Security Glossary **PIA - 1661** .

4. TERMS AND CONDITIONS

Threats that violate Information Security and cybersecurity can significantly affect the reputation of Promigas and related companies, as well as their most important information assets. Being aware of the consequences, and in response to their commitment to preserving the principles of Information Security and cybersecurity, Promigas and related companies have developed this corporate policy to protect and ensure the availability, confidentiality, integrity and privacy of information and the establishment, implementation, maintenance and continuous improvement of their information security and cybersecurity management system.

This document compiles the principles and internal rules that constitute the main foundations of the Information Security and Cybersecurity Policy for Promigas and related companies and are the basis for the implementation of the associated procedures.

The implementation of new business processes that generate physical or electronic information must comply with the guidelines defined herein and with provisions of the IT Policy **PNA-744,** or equivalent document for each company, as applicable, in order to protect the information.

The provisions of this policy apply generally to all information management, including ensuring the principle of security in the processing of personal data in accordance with the provisions of the statutory law 1581/2012 and regulatory decree thereof as defined in the Personal Data Protection Policy **GNA-1651**, or equivalent document for each company: for all of the foregoing the following applicable regulations are taken as a basis:

- NTC-ISO-IEC 27001:2013: This standard specifies the requirements for establishing, implementing, maintaining and continually improving an Information Security management system, within the context of the organization. This standard also includes requirements for the assessment and treatment of Information Security risks, adapted to the needs of the organization. The requirements established in this standard are generic and intended to be applied to any organizations, regardless of their type, size or nature.
- ISO/IEC 27000: is a group of international standards: Information Technology Security Techniques - Information Security Management Systems - Overview and vocabulary. It aims at helping all types and sizes organizations to implement and manage an Information Security Management System (ISMS).
- ISO/IEC 27701: Standard specifying requirements and providing guidance for establishing, implementing, maintaining and continually improving the Information Privacy Management System.
- Law 1581/2012 (Habeas Data): Whereby general provisions are issued for the processing and protection of personal data.
- Law 1273/2009: Information and data protection and comprehensive preservation of systems using information and communication technologies.
- SOX Act: U.S. law issued in 2002 aiming at improving the internal control environment of companies listed on U.S. stock exchanges; define and formalize responsibilities for compliance to prevent accounting and auditing errors.
- SEC *(Securities and Exchange Commission - "SEC"*): An agency of the U.S. Federal Government that exercises surveillance over key participants in the securities market and whose mission is to protect investors, keep the securities market organized, efficient and protected against fraud, maintain relevant market information, and facilitate the creation of capital.
- NIST Cybersecurity Framework: A framework based on existing standards, guidelines and practices for organizations to manage cybersecurity risk.

5. CONTENTS

5.1 STATEMENT OF COMMITMENT

Promigas is committed to the Information Security and Cybersecurity Policy, promoting a culture of compliance and control in accordance with the principles established by the information security and cybersecurity management system, therefore, it seeks:

Prevent damage to image and reputation through the adoption of and compliance with the Information Security and Cybersecurity Policy.

Continuously promote a corporate culture of information security and cybersecurity. Manage in a structured and strategic manner the information security and cybersecurity risks associated with the business and its relationship with third parties.

Moreover, each employee, temporary employee, contractor and supplier shall be responsible for applying the guidelines defined in this policy and for adapting their actions in accordance with the corporate values and information security and cybersecurity guidelines, as well as for reporting any incidents of which they may become aware.

5.2 REVISIONS

Risk and compliance management is responsible for modifying or updating the guidelines outlined hereunder. The information security committee may review and issue opinions on proposed adjustments or changes to the Information Security Policy - **GNA 1656.**

In order to ensure its validity, sufficiency and level of effectiveness, this document must be kept up to date, which is why it is defined that the Risk and Compliance Management team must periodically review it as established in the Internal Document Management Standard **GNA-002-S1** or earlier if circumstances are identified that require modification thereof.

5.3 POLICY COMPLIANCE

Compliance with the principles, guidelines, procedures contained in this Policy are mandatory and any exceptions must be notified to information security and documented as a risk incurred by the company and must be formally accepted by the process Leader.

Each employee, temporary employee and supplier shall be responsible for applying the criteria defined hereinunder and for adapting their actions in accordance with the corporate values and information security guidelines, as well as for reporting any incidents of which they may become aware.

5.4 PRINCIPLES

Information is one of the most important "Assets" and must be used in accordance with business requirements and only by the person authorized to use it. In order to comply with the established objectives and as part of the Information Security and Cybersecurity Policy, the following fundamental principles have been established:

- **Confidentiality:** business and third-party information must be protected, regardless of the medium or format in which it is stored.
- **Integrity:** Integrity of business information must be preserved regardless of the medium on which it is stored, whether temporary or permanent, or the form in which it is delivered.
- **Availability:** Business information must be available when legitimately required.

5.5 GOVERNANCE FOR INFORMATION SECURITY AND CYBERSECURITY MANAGEMENT

Promigas and its related companies must structure the functions and responsibilities regarding Information Security and Cybersecurity Risk and the corresponding management, in accordance with the Corporate Policy for Comprehensive Risk Management; this framework of reference defines the scheme of the three lines (formerly, lines of defense), considering (i) management by line of business, (ii) an independent Information Security risk management function, and (iii) an external review.

First line: Conformed by Company's management, process leaders, project managers and, in general, the collaborators who carry out process activities; they are the owners of the risks, including information security risks, and who must manage them, and are therefore responsible for maintaining effective internal control, executing risk control procedures and implementing the appropriate corrective actions.

The Information Security and Cybersecurity Policy recognizes that front-line employees, i.e., employees responsible for IT security and other employees executing processes or projects, are primarily responsible for identifying, assessing, managing, monitoring and reporting security and cybersecurity risks and incidents inherent to the products, activities, processes and systems related to their work. Those involved in this line must be familiar with its activities and processes, and have sufficient resources to perform their tasks effectively. Furthermore, they must comply with policies and procedures defined by the Organization, contributing to a solid Information Security and Cybersecurity corporate culture.

Second line: This line of defense is made up of the information security areas, which must establish the guidelines in this area and continuously monitor compliance with all Information Security and Cybersecurity Risk requirements.

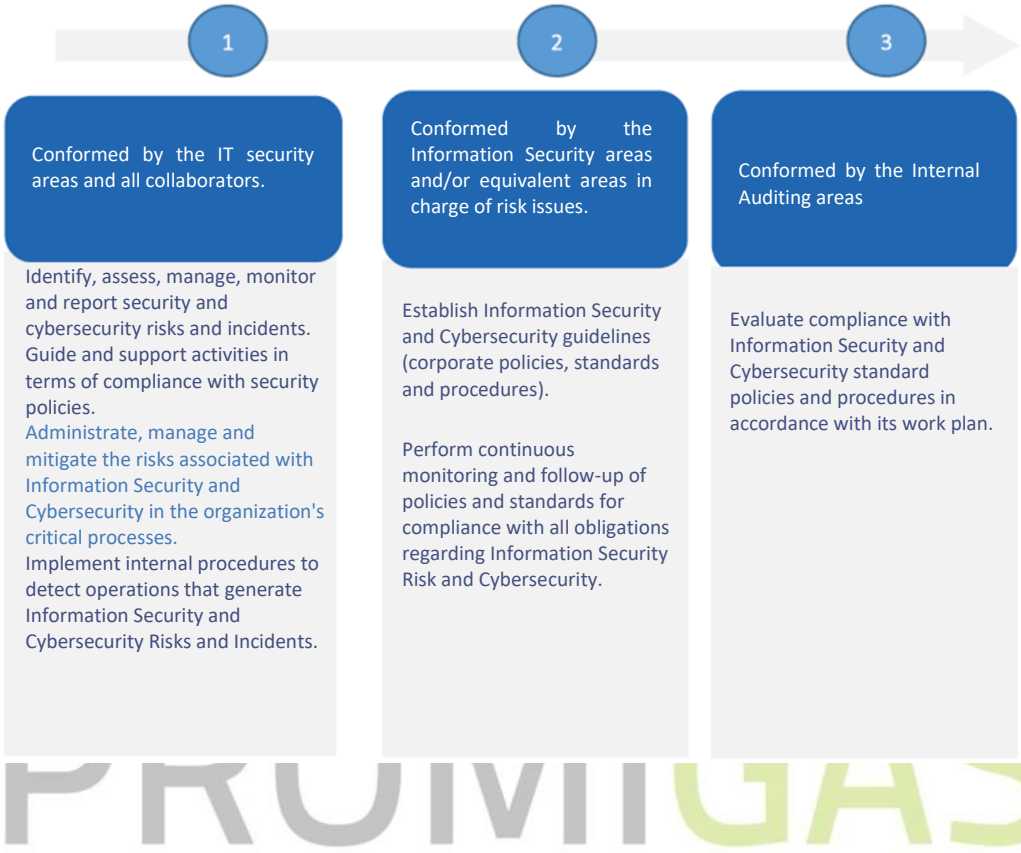
The Information Security area should present management results directly to the Information Security Committee or to senior management. It must also have sufficient resources to effectively perform all its functions and play a central and proactive role in the Information Security Management System. In order to do so, it must be completely familiar with the policies and procedures in place, legal and regulatory requirements and the Information Security risks arising from the business, including specific Cybersecurity issues.

This line also includes the teams responsible for leading the Organization risk management process, including information security risks, facilitating and monitoring the implementation of effective risk management practices, as well as assisting the first line of defense in defining and monitoring the controls necessary for effective risk management.

Third Line: The third line plays an important role in independently assessing the management and controls of information security and cybersecurity risks, as well as the policies, standards and procedures of the systems, reporting to the Audit Committee. The internal auditors who must conduct these inspections shall be competent and properly trained and not involved in the development, implementation and operation of the risk/control structure. This review may be performed by audit personnel or by personnel independent of the process or system under review, but may also involve appropriately qualified external parties.

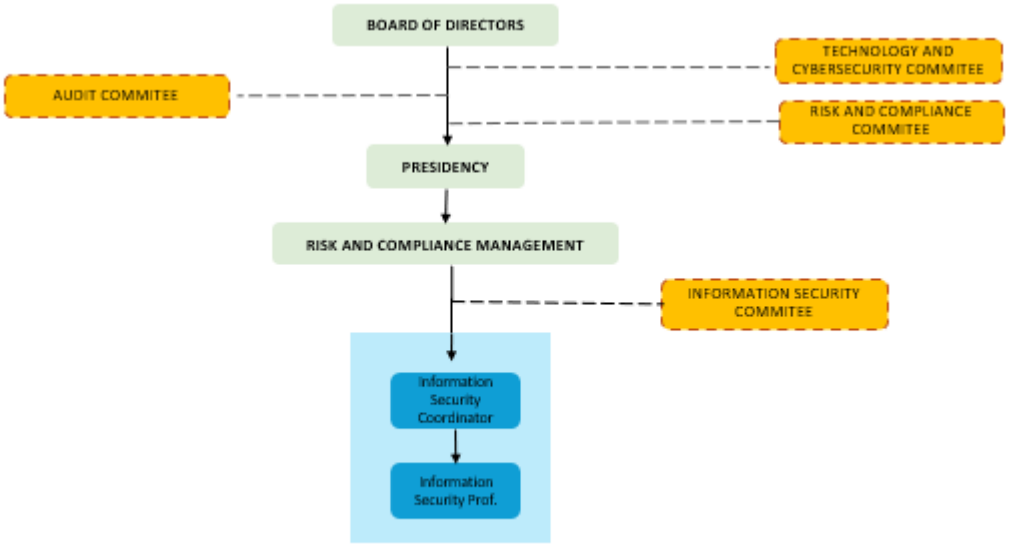
Composed of the Internal Audit teams, who are responsible for independently and objectively evaluating the Organization's risk management, reporting the results to the Audit, Risk and Corporate Governance Committee. Their assessment provides reasonable assurance on the effectiveness of governance, risk management and internal control, including how the first and second lines of defense achieve risk management and control objectives.

Figure 1 Diagram of the 3 lines of defense



5.6 INFORMATION SECURITY AND CYBERSECURITY GOVERNANCE STRUCTURE

Figure 2 Information Security and Cybersecurity Governance and Structure



5.7 INFORMATION SECURITY ORGANIZATION

In order to comply with the objective of the Corporate Information Security and Cybersecurity Policy, the following key players have been defined for the management of information security, so that they contribute to the implementation and operation of the Information Security Management System defined for the company.

Corporate Risk and Compliance Committee

Liability: Maintain the quality of the information security process, based on provisions set forth hereunder, taking the necessary preventive, corrective and improvement actions to guarantee correct implementation in the companies. This committee is convened in accordance with the provisions of the Corporate Risk and Compliance Annex - **GMA-1932**.

Members of the Risk and Compliance Committee:

- President
- Vice President of Finance and Administration
- Vice President of Transportation Operations
- Vice President of Corporate Affairs
- Vice President of Business Distribution
- Vice President of Transportation Business
- Manager of Corporate Risk and Compliance
- Risk Coordinator
- Compliance Coordinator
- Information Security Professional

Information Security Committee

Liability: Enforce the application of this Policy and related standards, procedures and regulations, support the projects and activities defined by the Risk and Compliance Committee regarding information security.

Members of the Information Security Committee

Main members

- Risk and Compliance Manager
- Liaison General Manager
- I.T. Manager - Enlace
- Infrastructure and Telecommunications Coordinator - Enlace
- IT Security Coordinator - Enlace
- Information Security Professionals (Committee Coordinator)

Guests

- Corporate Director of IT Security for Subsidiaries - Grupo Aval
- IT Security Specialist for Subsidiaries - Grupo Aval
- Information Security Officer - Corficolombiana

NOTE: The committee may include other guests depending on the topics to be discussed.

Risk and Compliance Manager - Promigas

Liability: Enforce the implementation, maintenance and proper functioning of the Information Security Policy and established procedures; in the Company information assets and under the guidelines of the Risk and Compliance Committee.

Liaison General Manager

Liability: Support decision making related to technical safety and leverage initiatives arising from the continuous improvement of the safety posture in the companies served by Enlace CSC.

Infrastructure and Telecommunications Coordinator - Enlace

Liability: Enforce the implementation, maintenance and proper functioning of the Information Security and Cybersecurity Policy, architectures, procedures, standards and norms, in the company technology platform, according to the requirements of the business areas and under the guidelines of the Information Security Committee.

Information Security Professional - Promigas

Liability: Perform the activities required for the implementation, maintenance and proper functioning of the Information Security Management System and the established procedures; on the company information assets and under the guidelines of the Information Security Committee or Risk and Compliance Committee.

IT Security Coordinator - Enlace

Liability: Plan, coordinate and manage the company IT security processes. The coordinator must ensure the proper functioning of the IT security process, as well as the measures implemented to guarantee the security of the company IT infrastructure and networks.

Responsible for the information - All portfolio companies

Liability: Clearly identify the value of the information under his responsibility, know the risks to which it could be exposed and ensure that the necessary mechanisms are provided so that these risks are mitigated to acceptable levels. The Information responsible person is the one who requires the information in order to carry out his business process and who is responsible for managing and classifying it, according to the importance of the information for his area. It must also ensure compliance with the Information Security Policy and cybersecurity within his area and in order to do so, it must know the value of his information.

Information users - All portfolio companies

Liability: They are the other subjects that use the information and are responsible for protecting the information assets of Promigas and its related companies by complying with the Corporate Information Security and Cybersecurity Policy. Likewise, they must be alert to identify and report any non-compliance or lack of compliance with established standards or procedures.

Actor	Implementation Activities	Supervisory Activities
Board of Directors	Ensure availability of sufficient technical and human resources to adequately manage information security and cybersecurity. Demand compliance with governmental information security and cybersecurity rules and regulations. Participate in awareness and training programs on Information Security and Cybersecurity issues.	Monitor the information security and cybersecurity in Promigas and Subordinate companies, understanding the risks and ensuring risk management.
Senior Management	Provide Corporate Information Security and Cybersecurity principles, guidelines and directives, take relevant preventive and corrective actions for Promigas and related companies, identify, evaluate and include Information Security and Cybersecurity requirements in the corporate initiatives carried out for the entities. Promote the application and	Follow-up the compliance at corporate level with the policies of the Information Security and Cybersecurity Management System in each entity. Identify the level of maturity of the ISMS and progress in mitigating risks and closing information security and cybersecurity gaps.

Actor	Implementation Activities	Supervisory Activities
	appropriation of good information security and cybersecurity practices. Ensure the appropriation of the resources required for the implementation and operation of the information security management system. Enhance the information security culture of Promigas and its related companies' employees, temporary employees, contractors and third parties that manage information assets.	
Risk and Compliance Committee	Promote the development of the Information Security Organization. Inform Corporate Information Security and Cybersecurity principles, guidelines and directives, verify the development of Corporate Information Security and Cybersecurity projects and take the pertinent preventive and corrective actions. Inform about activities and projects that are of common interest and/or impact Promigas and/or related companies. Approve the guidelines deemed appropriate, in each of the related companies, for the improvement of Information Security Management.	Enforce the monitoring and compliance with the defined Information Security guidelines. Ensure that the Information Security Professional executes and controls the Information Security and cybersecurity policy. Be informed about the results of the Information Security and cybersecurity Management carried out by Promigas and related companies. Be informed about the Information Security Incidents occurred in the companies that have had a significant impact, identified through the different reporting sources and the action plans carried out to mitigate them. Identify the level of maturity of the ISMS and progress in

Actor	Implementation Activities	Supervisory Activities
		mitigating risks and closing information security and cybersecurity gaps.
Information Security Committee	Approve the feasibility of implementing technological changes to the elements making up the IT security Architecture. Approve the annual penetration testing schedule based on the proposal prepared by the Information Security Professional. Report to the Risk and Compliance Committee the relevant information security and IT issues discussed in the Information Security Committee. Review and determine the actions to be taken regarding information and IT security incidents detected or reported. Inform about the activities and projects that are of common interest and/or impact Promigas and/or its related companies. Provide feedback from the security workshops and ISMS diagnostics conducted and contribute to the continuous improvement of the Information Security posture. Define Corporate Information Security and Cybersecurity principles, guidelines and directives. Define Information Security and Cybersecurity requirements in the corporate initiatives carried out for the companies.	Verify the level of information security through the analysis of management indicators, in order to take corrective or improvement actions if required. Enforce the execution of the Information Security and IT Projects periodically and take corrective actions regarding those requiring it. Enforce activities compliance with the Information and IT security policy, procedures and standards. Follow up on the maturity level of the ISMS and progress in mitigating risks and closing information security and cybersecurity gaps.
Risk and Compliance Manager	Approve the Information Security and Cybersecurity Policy, Lead the	Ensure the updating of information security

Actor	Implementation Activities	Supervisory Activities
	development of the strategic information security plan. Coordinate with the areas the activities and projects aimed at enhancing the information security management program. Request the resources required for the implementation and operation of the information security management system. Fulfill other responsibilities as may be defined for Senior Management.	documents. Support and approve the guidelines for improvement in the processes of the Information Security and Cybersecurity Management System.
Information Security Professional	Define the company strategic information security plan based on business objectives. Lead the Information Security Committee. Adopt and disseminate the best practices suggested by the Committee. Propose and execute information security and cybersecurity dissemination and awareness plans. Promote the updating of the Information Security and Cybersecurity risk inventory. Adopt the guidelines established by corporate. Monitor and control aspects related to information leakage. Support the first line of defense in the process of identifying risks and controls, determining their criticality and verifying compliance with the action plans established in the management of information security and cybersecurity incidents.	Identify the Information Security Incidents and the measures that have been implemented to mitigate them. Monitor the risk assessment outcome. Define and monitor key performance indicators on information security and cybersecurity management.

Actor	Implementation Activities	Supervisory Activities
	Promote the implementation of plans, projects or initiatives to assist companies in case of information security and cybersecurity incidents. Record security incidents reporting them to the appropriate authorities according to the level of criticality.	
IT Manager	Define the company IT security strategic plan. Conduct IT security risk analysis of applications, products, operating systems, tools, networks and physical access devices. Propose improvements to the Corporate Information Security and Cybersecurity Policy. Ensure and enforce the implementation of established IT security architectures. Perform a periodic diagnosis of the company IT security. Ensure the execution of tactical plans to strengthen the ISMS maturity, mitigation of risks and security vulnerabilities on the technological platform. Ensure the existence of processes, resources and technologies to adequately maintain technical security management aligned to corporate information security and cybersecurity policies.	Review the IT security of the programs to be installed in the company. Ensure the implementation of IT security measures required to maintain an adequate use of corporate information through mobile devices.
IT Security Coordinator / Infrastructure and Telecommunications	Identify security risks in the administrated resource and manage the implementation of	Analyze Significant Information Security and Cybersecurity Incidents detected or identified

Actor	Implementation Activities	Supervisory Activities
Coordinator	mitigating controls. Inform the Information Security Professional about new risks identified and in particular about new Cybersecurity risks. Participate in the Information Security Committee. Adopt and disseminate the best practices suggested by the Committee. Support the second line in the risks and controls identification process, as well as in their evaluation and assessment. Implement and operate IT security and cybersecurity controls. Ensure timely closure of security breaches on the technological platform. Lead the design and execution of activities and strategies in the different stages of cybersecurity incident response.	through the various reporting sources and implement mitigation plans. Ensure that measures are taken to respond to incidents reported and to prevent future incidents. Adopt current best practices in the market with respect to incident response. Define and monitor key performance indicators on IT security management and Cybersecurity.
Responsible for the information	Identify, classify and protect the information under their responsibility, know the risks to which it could be exposed and ensure that the necessary mechanisms are provided so that these risks are mitigated to acceptable levels, considering cost-benefit for their business area and the organization. With the support of the second line, identify the key controls to mitigate the identified risks. Execute controls to mitigate risks	Monitor and enforce that the work team complies with the security and cybersecurity policy.

Actor	Implementation Activities	Supervisory Activities
	(Self-control). Report to the IT security and information security areas, any information security event or incident and in particular any event concerning cybersecurity. Define and execute action plans to mitigate risks of information at his charge.	
Information users	Implement the guidelines and strategies of Information Security and Cybersecurity, which guarantee the protection of the companies' information. Processing business information in accordance with the defined level of confidentiality.	Identify risks in the resources to which it has access and make suggestions to improve the security conditions implemented.

5.8 CORPORATE INFORMATION SECURITY AND CYBERSECURITY GUIDELINES.

The following points provide a high-level and general description of the information security and cybersecurity guidelines that establish the guidelines for maintaining the confidentiality, integrity, availability and privacy of information and cybersecurity in Promigas and related companies. In addition, this policy is complemented by the Information Security Manual **GMA-2099**, which specifies and expands the guidelines for each domain of the Information Security Management System.

5.8.1 INTELLECTUAL PROPERTY.

BUSINESS INFORMATION IS A VITAL ASSET OF PROMIGAS AND THEREFORE MUST BE PROTECTED.

Pursuant to the Intellectual Property Policy **GNA-1841**, PROMIGAS information, regardless of its presentation, medium or format, in which it is created or used to support business activities, qualifies as business information or information asset that must be classified.

Information security and business cybersecurity are the set of protective measures taken by the company against accidental or malicious disclosure, modification, theft or destruction of its information. Such protection measures are based on the relative value of the information and the risk that it may be compromised.

Information responsible parties are expected to ensure that business information is appropriately protected to preserve the Information Confidentiality, Integrity, Availability and Privacy.

PROMIGAS must have the necessary means in place to ensure that each employee or third party preserves and protects information assets in a consistent and reliable manner. Any person attempting to disable, defeat, or override any security control shall be subject to appropriate disciplinary action.

OWNERSHIP OF THE INFORMATION MUST BE MAINTAINED.

Intellectual Property is defined as any patent, copyright, invention or information owned by PROMIGAS. All content developed while working for the company is considered to be the Company intellectual property and for exclusive use thereof, therefore, it must be protected

against disclosure, appropriation or use that undermines PROMIGAS competitiveness; also, compliance with the provisions of the Intellectual Property Policy **GNA-1841** shall be ensured

5.8.2 INFORMATION RESPONSIBLE PERSON.

THERE MUST BE A DESIGNATED PERSON RESPONSIBLE FOR EACH PROMIGAS INFORMATION ASSET WHO SHALL ENSURE INFORMATION SECURITY BASED ON THE RISKS TO WHICH THE INFORMATION IS EXPOSED.

PROMIGAS uses information to develop its mission activity. This is created and made available to those involved in the different processes so that they can develop and achieve their respective goals within the business framework.

There must be assigned a person responsible for the information used by PROMIGAS in the business objectives development, who uses the information in his/her area and is responsible for correct use thereof. Thus, such responsible person is who makes the decisions that are required for the protection of his/her information and determines who the users are and their privileges of use. In PROMIGAS, the vice presidents, managers, directors, coordinators and other heads of the different departments, or those delegated by them, shall be responsible for the information.

5.8.3 INFORMATION SECURITY AND CYBERSECURITY RISK MANAGEMENT.

THE INFORMATION SECURITY AND CYBERSECURITY RISKS TO WHICH PROMIGAS INFORMATION IS EXPOSED SHALL BE IDENTIFIED, EVALUATED AND MITIGATED ACCORDING TO THEIR VALUE, PROBABILITY OF OCCURRENCE AND IMPACT ON THE BUSINESS.

Business information must be protected based on its value and the risk in which it may be compromised. Therefore, the Information Security and Cybersecurity Committee shall periodically conduct an analysis of the state of the business with respect to information security and cybersecurity to determine or update the relative value of the information, the level of risk to which it is exposed and the respective responsible party.

Based on the information risk levels and assessment, each responsible person must perform a formal risk assessment, considering them as business risks and using the same risk assessment methodology, so that they are identified, evaluated and the necessary actions are applied to correct or mitigate them in accordance with the risk levels allowed by the company.

Each information user must be aware of the procedures for reporting risks that may have an impact on PROMIGAS information security, and they are required to immediately report any suspicion or observation of an information security and cybersecurity incident.

5.8.4 COMPLIANCE WITH REGULATIONS.

PROMIGAS SHALL COMPLY WITH LOCAL AND INTERNATIONAL PRIVACY AND INFORMATION SECURITY AND CYBERSECURITY REGULATIONS.

This policy is in accordance with and supports compliance with local and international laws and regulations relating to privacy, information security and cybersecurity. Therefore, such requirements must be included in the development of the Information Security and Cybersecurity System and specific actions must be established to keep PROMIGAS permanently aligned with such provisions.

The Company shall implement procedures and establish controls to ensure compliance with internal security standards and policies, statutory, regulatory and contractual requirements relevant to each information system. All areas whose processes must comply with applicable regulations shall have procedures in place to ensure legal compliance. Furthermore, and in order to maintain a sound level of security, this Policy must be supported by the best information security and cybersecurity practices.

5.8.5 TRAINING AND CREATION OF INFORMATION SECURITY AND CYBERSECURITY CULTURE.

PROMIGAS HAS ESTABLISHED A PERMANENT PLAN TO GENERATE AWARENESS OF INFORMATION SECURITY AND CYBERSECURITY FOR USERS AND THIRD PARTIES.

The company has a permanent program to ensure that users and third parties are aware of their responsibilities in Information Security and cybersecurity and the continuous threats that compromise the information they handle.

Employees and third parties must be aware of the information security and cybersecurity procedures that they must apply in addition to those required to perform their job duties. As part of the training program, new company hired personnel must receive training on PROMIGAS information security and cybersecurity requirements during their introductory period. Participation in information security training is mandatory for all Promigas employees.

5.8.6 PERSONNEL SECURITY.

PROMIGAS MUST PROVIDE THE NECESSARY MECHANISMS TO ENSURE THAT ITS EMPLOYEES COMPLY WITH THEIR INFORMATION SECURITY AND CYBERSECURITY RESPONSIBILITIES FROM START DATE TO TERMINATION DATE.

Employees joining PROMIGAS must follow a selection process, and once hired, they will have access to this Policy and the Information Security Manual **GMA-2099** for their knowledge and due compliance.

Employee contracts should include clauses setting forth the corresponding information security and cybersecurity responsibilities and compliance with the code of ethics, making them aware of the consequences in case of noncompliance therewith.

A record per employee of their knowledge and understanding of the Information Security and Cybersecurity Policy should be maintained by certifying annual information security and cybersecurity training.

5.8.7 THIRD PARTIES ACCESSING PROMIGAS INFORMATION LOCALLY OR REMOTELY IN LOCAL APPLICATIONS OR IN CYBERSPACE.

THIRD PARTIES USING PROMIGAS INFORMATION LOCALLY OR REMOTELY SHALL COMPLY WITH THE INFORMATION SECURITY AND CYBERSECURITY POLICY.

The use of PROMIGAS information by third parties, whether in local applications or in cyberspace, and whether accessed locally or remotely, must be formalized by means of agreements and/or clauses that make compliance with this Policy mandatory, as well as with the provisions of the document on INFORMATION SECURITY IN RELATIONSHIPS WITH SUPPLIERS AND CONTRACTORS **PPA-112.** Contracts must include the obligation to protect PROMIGAS information, the security requirements to mitigate information and cybersecurity risks and the consequences to which they would be subject in case of non-compliance.

Each relationship with a third party must have a high-level representative (such as manager, director or their delegates in the role of contract administrator) within PROMIGAS, who ensures the correct use and protection of business information. IT Management, in coordination with the high-level representative, shall periodically conduct a formal review of the access rights of users of external entities accessing company information.

5.8.8 INDIVIDUAL IDENTIFICATION AND AUTHENTICATION.

ALL USERS ACCESSING PROMIGAS INFORMATION MUST HAVE A MEANS OF IDENTIFICATION AND ACCESS MUST BE CONTROLLED THROUGH PERSONAL AUTHENTICATION.

Each user is responsible for his or her actions while using any PROMIGAS information resource whether local or in cyberspace. Therefore, the identity of each IT resources user shall be established and authenticated in a unique way and cannot be shared.

Once PROMIGAS users have been created and assigned their authorizations in the Information Systems, they will be able to access the information by means of their user and authentication key. Depending on the value of the information and the level of risk, PROMIGAS will define appropriate means of authentication, which cannot be shared (such as the password) and such means of authentication contain confidential information that must not be disclosed or stored in places that can be accessed by unauthorized persons.

5.8.9 CONTROL AND MANAGEMENT OF ACCESS TO INFORMATION LOCALLY OR IN THE CYBERSPACE.

THE USE OF PROMIGAS INFORMATION MUST BE CONTROLLED TO PREVENT UNAUTHORIZED ACCESS. INFORMATION PRIVILEGES MUST BE MAINTAINED IN ACCORDANCE WITH BUSINESS NEEDS, LIMITING ACCESS TO ONLY WHAT IS REQUIRED.

Physical and logical access control mechanisms should be established to ensure that information assets are protected locally and in cyberspace in a manner consistent with their value to the business and the risks of loss of confidentiality, integrity, availability and privacy of information.

Access rights must not compromise the segregation of duties and responsibilities. Locally and/or in cyberspace access to company information shall be granted only to authorized users, based on what is required to perform the tasks related to their responsibility. Access to PROMIGAS resources should be restricted in all cases, and should be granted specifically on a need-to-know and least privilege basis.

5.8.10 INFORMATION CLASSIFICATION.

ALL INFORMATION, REGARDLESS OF THE FORMAT IN WHICH IT IS STORED, SHALL BE CLASSIFIED IN ONE OF THE FOLLOWING 3 CATEGORIES: RESTRICTED, INTERNAL AND PUBLIC, IN ACCORDANCE WITH THE INFORMATION CLASSIFICATION STANDARD ESTABLISHED BY THE COMPANY.

Like other assets, not all information has the same use or value, and therefore requires different levels of protection. All PROMIGAS information shall be classified by the Information Responsible based on a high-level analysis of the business impact on information security and cybersecurity, which determines its relative value and level of risk to which it is exposed. The methodology defined for classifying information is set forth in the Information Classification Procedure **GPA-1978**.

According to the risks identified, the Information Responsible and the Information Security Professional shall determine the necessary controls to provide an appropriate and consistent level of protection for the information with regards to PROMIGAS and its related companies, regardless of the medium, format or place where it is stored. These controls shall be applied and maintained throughout the life cycle of the information, from creation, during authorized use and until proper disposal or destruction.

5.8.11 CONTINUITY OF SECURITY.

ALL CRITICAL INFORMATION RESOURCES AND ASSOCIATED PROCESSES, WHETHER LOCAL OR IN CYBERSPACE, MUST HAVE A BUSINESS CONTINUITY PLAN AND BE PREPARED FOR INFORMATION SECURITY AND CYBERSECURITY ATTACKS. THE CONTINUITY OF INFORMATION SECURITY AND CYBERSECURITY MANAGEMENT IS MAINTAINED DURING CONTINGENCY SITUATIONS.

The information must be available for authorized use whenever required by PROMIGAS in the performance of its regular duties. Therefore, procedures must be developed, documented, implemented and periodically tested to ensure a reasonable and timely recovery of the company critical information, both locally and in cyberspace, without lowering the established security levels. This should be separated from both the technological means used by PROMIGAS and the possibility of the information being corrupted, destroyed or temporarily unavailable.

PROMIGAS shall establish measures to detect and mitigate the effects of information security and cybersecurity attacks such as denial of service and the entry of unauthorized malicious code. These measures shall be based on procedures and elements that allow PROMIGAS to be kept informed of the existence of these threats, to detect attacks immediately and to execute the relevant actions.

5.8.12 PHYSICAL SECURITY.

ALL PHYSICAL AREAS OF THE BUSINESS SHALL HAVE A LEVEL OF SECURITY COMMENSURATE WITH THE VALUE OF THE INFORMATION THAT IS PROCESSED AND MANAGED THEREIN. CONFIDENTIAL OR BUSINESS-SENSITIVE INFORMATION SHOULD BE KEPT IN LOCATIONS WITH RESTRICTED ACCESS WHEN NOT IN USE. ALL EMPLOYEES SHALL COMPLY WITH THE GUIDELINES FOR THE PHYSICAL PROTECTION OF RESTRICTED OR CONFIDENTIAL INFORMATION THEY USE.

The physical areas built to support the entire business operation must be equipped with the appropriate controls (e.g., doors, locks, card readers, biometrics devices, security cameras, etc.) according to the value of the information they contain.

PROMIGAS IT resources must be physically protected against unauthorized access and environmental threats to prevent exposure, damage or loss of assets and interruption of business activities.

Information classified as restricted with high confidentiality shall not be left unattended or uncontrolled, so PROMIGAS shall develop corporate standards to prevent critical business information from being accessed without authorization, including the implementation and compliance with the Clean Desk and Clean Screen guidelines.

5.8.13 ALERT MANAGEMENT.

PROMIGAS SHALL BE ALERTED IMMEDIATELY UPON OCCURRENCE OF VIOLATIONS TO THE INFORMATION SECURITY AND CYBERSECURITY POLICY.

Situations or actions violating this Policy must be detected, recorded and reported to the Information Security Professionals or Risk and Compliance Management immediately (alerts). Event and incident management strategies must be developed to prioritize these alerts and resolve them according to the information criticality for PROMIGAS. These strategies should include the definition of an immediate reaction organization to deal with these and other

situations that the company considers critical. Incident and security event management must be handled in accordance with the provisions of the IT Incident Response Plan **GPA-1664.**

5.8.14 AUDITABILITY OF INFORMATION SECURITY AND CYBERSECURITY EVENTS.

PROMIGAS INFORMATION SECURITY AND CYBERSECURITY RECORDS SHOULD BE REVIEWED ON AN ONGOING BASIS TO ENSURE COMPLIANCE WITH THE INFORMATION SECURITY AND CYBERSECURITY MODEL.

Persons responsible for Information must define the events considered as critical (for example: unsuccessful attempts to access the information system, deletion or alteration of information, among others) and the respective information security and cybersecurity logs that must be generated.

Information security and cybersecurity records must be activated, stored and permanently reviewed, and unexpected situations must be reported in a timely manner to persons responsible, as well as to the required security levels. The generating and managing records and media must be protected by controls that prevent unauthorized modifications or access, in order to preserve the integrity of the evidence.

5.8.15 CONNECTIVITY.

ALL CONNECTIONS TO PUBLIC NETWORKS MUST BE AUTHENTICATED TO PREVENT INFORMATION FROM BEING DISCLOSED OR ALTERED.

Connections to PROMIGAS private network must be made in a secure manner to preserve the confidentiality, integrity, availability and privacy of the information transmitted over the network. Likewise, all outgoing access to cyberspace and other private topologies must be over PROMIGAS-approved networks.

Users of the information and third parties connecting to the private network shall comply with this Policy before the connection is made. This applies equally to any current or future connection on the PROMIGAS network using public networks.

The approval of the Information Responsible Person is required in order to remotely access PROMIGAS information; such accesses shall comply with the Identification and Authentication Policy.

5.8.16 USE OF LOCAL AND IN THE CYBERSPACE BUSINESS IT RESOURCES OF MOBILE DEVICES AND MOBILE WORK.

IT RESOURCES PROVIDED LOCALLY AND IN CYBERSPACE ARE FOR THE BUSINESS EXCLUSIVE USE.

PROMIGAS IT resources, both local and in cyberspace, are exclusively for business purposes and should be treated as assets dedicated to providing the tools to perform the required work. Information users and third parties who attempt to access information for which they do not have an authorized business requirement are in violation of this Policy.

In the use of PROMIGAS information, there should be no presumption of privacy, so when it is used, records of the activity performed may be created, which may be reviewed by PROMIGAS in accordance with the provisions of the Information Security Manual **GMA-2099**, which must be known and accepted by all employees.

PROMIGAS reserves the right to restrict access to any information at any time it deems appropriate. Personnel selected by the company may use restricted technology such as network monitoring, operational data and information security events.

No unauthorized hardware or software will be loaded, installed or activated in the IT resources, without prior formal authorization from the IT Management and opinion issued by the Information Security area.

To access PROMIGAS information both locally and in cyberspace through means such as mobile devices or accesses, the necessary controls must be implemented to reduce the risks introduced by these practices.

5.8.17 INFORMATION SECURITY AND CYBERSECURITY IN SYSTEM ADMINISTRATION PROCESSES

EACH PROMIGAS SYSTEMS ADMINISTRATION PROCESS SHALL COMPLY WITH THIS INFORMATION SECURITY AND CYBERSECURITY POLICY.

Information security and cybersecurity activities, standards and responsibilities must be included in each of the company systems management processes in order comply with this Policy.

Regardless of the authorship or liability for new developments and those required in support processes, the development area of IT Management must create and maintain a methodology

that controls the complete cycle of development and secure maintenance of systems. Information security and cybersecurity requirements should be identified prior to the design and development of information technology and cybersecurity systems. During development, these requirements must be included in the systems and if a modification is required, such modification must strictly comply with the secure development and information security requirements that have been previously established. The security level of a system cannot be diminished, so the information and systems in production shall not be used for development, testing or maintenance of applications.

All IT resources implemented in the company must follow the configuration of security parameters in accordance with the norms and standards established in the document **PPA-786** IT Resources Security Standards or equivalent document in each company. New technological components cannot be implemented without previously including all required security measures. For this purpose, the facilities available in the equipment, in terms of safety, must be implemented and adapted according to the defined norms and standards.

The use of virtualization and cloud computing in the company must be carried out with the necessary controls to mitigate the risks these technologies pose.

The implementation of a new system or significant change to existing ones should be reviewed by means of a risk assessment, which allows the detection of risks, the location of appropriate controls to mitigate them and safe operation.

The implementation of a technological change at the local level or in cyberspace that does not take into account the information security and cybersecurity requirements exposes PROMIGAS to risks. Therefore, each technological change must ensure compliance with the Information Security and Cybersecurity Policy and its respective underlying standards, and in the event of exposing the company to an information security and/or cybersecurity risk, this must be identified, evaluated, documented, assumed and controlled by the respective Information Responsible person.

5.9 INFORMATION SECURITY AND CYBERSECURITY ASSESSMENT MODEL.

For the identification of risks and the application of information security and cybersecurity controls, Promigas adopts the information security and cybersecurity assessment model. This model purpose is to evaluate the maturity level of the information security management system and identify improvement opportunities to enhance it, based on the domains and controls proposed in the NTC-ISO 27001:2013 standard and the NIST Cybersecurity Framework.

5.10 PENALTIES FOR NONCOMPLIANCE.

Failure to comply with this policy and underlying rules by action or omission shall result in legal consequences in accordance with the provisions of the code of conduct, the internal work regulations, the constitution and the law.

6. REFERENCE DOCUMENTS AND ANNEXES

Promigas documents related to this Policy are listed:

PIA-1661 - Information Security Glossary
PPA-212-S2 - User Code and Password Management Procedure
FA-432 - User Code Creation Form
PPA-727 - Change Control Procedure for IT Resources
PNA-744 - IT Policy
PPA-786 - Information Resources Security Standards
GNA-1651 - Personal Data Protection Policy
PNA-1863 - Security Requirements for Information Systems Projects
GPA-1978 - Classification of Information Procedure
PPA-1999 - Procedure for Management and Mitigation of Computer Vulnerabilities.
GPA-1664 - Computer Incident Response Plan
GMA-2099 - Information Security and Cybersecurity Manual

7. TRACK CHANGES

Version 10 changes - July 2022

- Adjustment is made to section 5.7 INFORMATION SECURITY ORGANIZATION by adding the General Manager of Enlace as the main member of the information security committee.
- The code and name of the procedure INFORMATION SECURITY IN RELATIONSHIPS WITH SUPPLIERS AND CONTRACTORS **PPA-112** is corrected.

Request No. 17338

Version 9 changes - February 2022

- The structure of the document is redefined with high-level policies aligned with the AVAL and Corficolombiana model.
- Annex 1 is deleted and moved to the Information Security and Cybersecurity Manual GMA-2099.

Request No. 16874

Version 8 changes - November 2021

- New guidelines are included in section 5.8 related to the governance of security logs.
- New guidelines are adjusted and included in section 5.14 related to the types of changes in the productive environment that must be escalated for information security knowledge and endorsement.
- Section 5.17 amendment related to third party access to information and the way to share it with external parties.
- Minor corrections and wording changes

Request No. 16518