SINTEL GROUP

CORPORATE POLICIES

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

CONTENT

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1 POLICIES

1.1 QUALITY POLICY

It is focused on providing high-quality technological solutions that meet and exceed our customers' expectations. We recognize that quality is essential for the long-term success of our company and for customer satisfaction. To support this commitment, we establish this policy with the following parameters:

1.1.1 Customer Focus

Our main objective is to understand and meet the needs and expectations of our customers, thus seeking to establish long-term relationships based on trust, transparency, and consistent delivery of value.

1.1.2 Excellence in Technological Solutions

We develop innovative and efficient technological solutions that meet the highest quality standards. We seek continuous improvement in our processes and practices to provide solutions that stand out for their performance and reliability.

1.1.3 Compliance with Legal and Regulatory Requirements

We are committed to complying with all laws and regulations applicable to our operations and services, maintaining a management system that ensures compliance with relevant industry standards and regulations.

1.1.4 Commitment to Continuous Improvement

We foster an organizational culture focused on continuous improvement by conducting periodic reviews of our processes and procedures to identify optimization opportunities.

1.1.5 Development and Training of Personnel

We provide ongoing training to our staff to ensure technical competencies and updated skills, fostering an environment that promotes innovation, creativity, and continuous learning.

1.1.6 Collaboration and Effective Communication

We promote effective collaboration among the governing body, management, and departments to ensure consistency in solution delivery, while maintaining open and transparent communication channels with our customers and stakeholders.

1.1.7 Risk Management

We proactively identify and manage risks to ensure the continuity of our services and information security. We implement security measures and controls to protect assets and the confidentiality of information.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1.1.8 Measurement and Performance Evaluation

We establish key performance indicators (KPIs) to measure and evaluate the effectiveness of our processes and customer satisfaction.

1.2 CORPORATE SOCIAL RESPONSIBILITY POLICY

We recognize the importance of integrating socially responsible practices into all our operations and business activities. We are committed to making a positive contribution to society's well-being and sustainable development under the following parameters:

1.2.1 Ethics and Transparency

We operate ethically and transparently in all our business interactions; we promote an organizational culture that values honesty, integrity, and mutual respect.

1.2.2 Inclusion and Diversity

We foster an inclusive environment that celebrates diversity of perspectives, experiences, and skills, implementing hiring and development practices that promote equal opportunities for all employees.

1.2.3 Ethics in the Supply Chain

Our work with suppliers who share our ethical and social values, continuously evaluating the supply chain ensures fair and sustainable practices.

1.2.4 Accountability

We commit to measuring, evaluating, and continuously improving our performance in social responsibility, regularly sharing our achievements and challenges in social responsibility with all stakeholders.

1.3 SOFTWARE DEVELOPMENT POLICY

This policy establishes the standards and guidelines for handling and/or developing software with the aim of ensuring the delivery of high-quality, secure, and efficient technological solutions.

1.3.1 Development Cycle

We adopt an approach based on agile methodologies for software development and/or management; development teams follow interactive and collaborative development practices.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1.3.2 Project Management

We use project management tools to plan, execute, and monitor software development and/or management projects, establishing clear milestones and measurable objectives to assess project progress.

1.3.3 Software Security

Security is a primary consideration throughout the software development and/or management lifecycle, for which regular security analyses and penetration testing of implemented applications are conducted.

1.3.4 Documentation

Comprehensive and up-to-date documentation of the software, architecture, and processes is provided, understandable for different audiences, testers, and support staff.

1.3.5 Testing and Validation

We implement thorough testing, including unit tests, integration tests, and user acceptance testing, and encourage them to enhance software efficiency and quality.

1.3.6 Deployment and Maintenance

We carefully plan the deployment of new software versions. We establish monitoring procedures and proactive maintenance to ensure the stability of the running software.

1.4 BUSINESS CONTINUITY POLICY

This policy establishes the principles and procedures to ensure business continuity in the event of disruptive events, minimizing the impact on operations and ensuring the resilience of the company.

1.4.1 Risk Assessment

Regular risk assessments are conducted to identify potential threats to business continuity, maintaining an updated record of risks and vulnerabilities.

1.4.2 Business Continuity Planning

Detailed business continuity plans will be developed to address various interruption scenarios, including procedures for the recovery of critical systems, data, and functions.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1.4.3 Identification of Critical Activities

Critical activities and processes for the continuous operation of the company are identified and documented, establishing priorities to ensure efficient recovery of essential functions.

1.4.4 Redundant Infrastructure

Measures are taken to ensure redundancy of critical technological infrastructure, establishing agreements with service providers to support business continuity.

1.4.5 Backup and Data Recovery

Regular backups of critical data are performed and stored in secure locations, establishing data recovery procedures to minimize information loss.

1.4.6 Communication and Notification

A communication plan is executed to inform employees, customers, suppliers, and other stakeholders about the interruption and the measures taken, implementing internal and external notification protocols.

1.4.7 Training and Awareness

Regular training is provided to employees on business continuity procedures, fostering awareness of the importance of business continuity at all levels of the organization.

1.4.8 Coordination with Stakeholders

Coordination mechanisms are established with suppliers, business partners, and other key stakeholders to ensure an efficient response in case of interruption.

1.5 PRIVACY AND DATA PROTECTION POLICY

Describes how we collect, use, disclose, and protect personal information, ensuring the privacy protection and security of personal information of our internal and external collaborators and clients.

1.5.1 Information Collected

Collection of personal information, such as names, email addresses, and phone numbers, is only done when necessary to provide our services and respond to requests.

1.5.2 Use of Information

We use personal information to provide and improve our services, process transactions, and respond to requests. We may use non-identifiable information for analysis and product improvement.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1.5.3 Disclosure to Third Parties

We do not share personal information with third parties, except when necessary to provide services or comply with legal obligations.

1.5.4 Information Security

We implement technical and organizational security measures to protect personal information against unauthorized access, loss, and alteration; we regularly review and update our security procedures.

1.5.5 Legal Compliance

We comply with all applicable data privacy laws and regulations, cooperate with regulatory authorities, and take action to address any data security breaches.

1.6 PERSONAL DATA PROTECTION POLICY

We are fully committed to protecting your information as established by law. The purpose of this Personal Data Protection Policy is to provide information to individuals about what data we collect, why we collect it, and how they can exercise their rights.

1.6.1 Scope

The Personal Data Processing Policy for SINTELINTERNATIONAL S.A.S., hereinafter referred to as "SINTEL," is valid for all personal data collected through the website www.sintel-international.com, digital channels, official social networks, and other means. Its purpose is to inform about the collection, processing, and protection of personal data. This policy is publicly accessible, so any user who visits, explores, or uses the website for informational or interest purposes in the products and services offered can find it in a specific space on the website to easily access it.

1.6.2 Purpose of the Policy

In this Policy, SINTEL establishes guidelines for the collection, recording, processing, administration, storage, and preservation of personal data. Likewise, the procedures that allow data subjects to exercise their rights, such as rectification, updating, access, opposition, deletion, and elimination of the processing of personal data that have been provided to SINTEL under consent and legitimate interest, are detailed.

1.6.3 Definitions

In order to facilitate the understanding of this policy, the definitions specified in the legislation and specialized regulations related to the protection of personal data are presented.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

a) **Consent:** Refers to the expression of the will of the data subject freely, specifically, informed, and unequivocally, through which the data controller authorizes the processing of their personal data.

b) **Database:** An organized set of data, regardless of its form, mode of creation, storage, organization, type of support, treatment, processing, location, or access. These databases can be centralized, decentralized, or distributed functionally or geographically.

c) **Personal data:** Any information related to an identified or identifiable person. This includes, but is not limited to, names, addresses, identification numbers, contact information, biometric data, physical characteristics, location information, health data, online behavior data, or any other detail that allows the unique or indirect identification of a person.

d) **Data Controller:** SINTEL is the data controller and assumes the responsibility to ensure that the processing is carried out in accordance with the applicable data protection laws and regulations of the individuals whose personal data is being processed.

e) **Transfer or Communication:** Refers to the expression, statement, delivery, consultation, interconnection, assignment, transmission, dissemination, or any action involving the disclosure of personal data to a person other than the data subject, data controller, or data processor. It is important to highlight that the shared personal data must be accurate, complete, and up-to-date.

f) **Processing:** Any operation or set of operations performed on personal data, whether by automated, partially automated, or non-automated technical procedures, such as: collection, gathering, obtaining, recording, organization, structuring, storage, adaptation, modification, deletion, indexing, extraction, consultation, use, possession, exploitation, distribution, assignment, communication, or transfer, or any other form of enabling access, comparison, interconnection, limitation, erasure, destruction, and, in general, any use of personal data.

g) **User:** Refers to the natural person whose personal data is susceptible to be processed or treated.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1.6.4 Identity and Contact Information of the Data Controller:

SINTELINTERNATIONAL S.A.S, with RUC: 1793079423001, domiciled in the province of Pichincha, city of Quito, Av. Shyris and Suecia Edificio Renazzo Piso 8, telephone 023331895, and email j.espinoza@sintel-international.com.

1.6.5 Legal Framework for Personal Data Protection:

SINTEL bases the processing of personal data on the following legal instruments, such as those listed below:

- *Constitution of the Republic of Ecuador. - Law on Electronic Commerce, Electronic Signatures, and Data Messages (Law No. 2002-67).*
- *Organic Law on Personal Data Protection, Official Registry Supplement 459 of May 26, 2021.*
- *Art. 7 - Legitimate Processing of Personal Data. - Processing will be legitimate and lawful if one of the following conditions is met:*

  1) By consent of the data subject for the processing of their personal data, for one or more specific purposes;
  2) When carried out by the data controller in compliance with a legal obligation;
  3) When carried out by the data controller, by court order, observing the principles of the present law;
  4) For the execution of pre-contractual measures at the request of the data subject or for the fulfillment of contractual obligations pursued by the data controller, data processor, or by a third party legally authorized;
  5) To satisfy a legitimate interest of the data controller or a third party, provided that the fundamental interests or rights of the data subjects do not prevail.

- *Organic Law of the National System of Public Data Registry, published in the Official Registry Supplement No. 162 of March 31, 2010; Article 4 - "Responsibility for information."*

- *The public and private sector institutions and natural persons that currently or in the future administer databases or registries of public data are responsible for the integrity, protection, and control of the records and databases under their charge. Such institutions shall be responsible for the truthfulness, authenticity, custody, and proper conservation of the records. The responsibility for the truthfulness and authenticity of the registered data lies exclusively with the declarant when he or she provides all the information (...)."*

  Article 6 of the aforementioned Law determines: "Accessibility and confidentiality. - Personal data, such as: ideology, political or union affiliation, ethnicity, health status, sexual orientation, religion, migratory status, and other data concerning personal privacy and especially information whose public use

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

violates human rights enshrined in the Constitution and international instruments (...)."

- *ORGANIC CODE OF SOCIAL ECONOMY OF KNOWLEDGE, CREATIVITY, AND INNOVATION - COESCCI, General Provisions, TWENTY-SEVENTH.- "(...) The processing of personal data, including actions such as the collection, systematization, and storage of personal data, will require the prior and informed authorization of the owner (...)."*

1.6.6 Origin and Processing of Personal Data

In order to enhance the quality of the experience in the provision of products and services, it is imperative that personal data requested through various channels, such as the website, digital platforms, social networks, or adhesion contract forms, be provided voluntarily, explicitly, informed, and unequivocally by the user; such data are covered by the POLICY FOR THE PROCESSING OF PERSONAL DATA and include:

- Names and Surnames
- Identification Number
- Cell phone number and/or WhatsApp
- Email address
- Date of birth
- Location data: city, address, and georeferencing
- Browsing behavior on the website
- Access IP address
- Username and password
- Date and time of access

SINTEL reserves the right to share information and personal data with entities, whether natural or legal persons, both public and private, in order to comply with requests related to accessing the products and services offered by SINTEL, always in accordance with personal data protection regulations.

1.6.7 Purposes of Personal Data Processing

SINTEL will use the information and personal data for the following purposes:

- **Processing of data for own commercial purposes:** The text indicates that SINTEL is authorized to use the user's personal data for the purpose of offering commercial offers, information about products and services related to internet access, iCloud services, antivirus, browsing platforms, among others. These communications will be carried out through the contact channels provided by the user in forms, digital channels, and/or social networks.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

- **Processing of data for third-party communications purposes:** SINTEL is authorized to use the user's identifying personal data, such as names, surnames, email, and/or telephone number. This data will be processed by processors in order to receive commercial offers of products or services from third parties, with whom SINTEL has alliances and/or agreements to provide benefits in service and/or related products.

- **Processing of data for statistical and analytical purposes:** SINTEL, by having authorization for the use of the user's personal data, may use it to carry out market studies that cover commercial preferences and interests, as well as the evaluation of service quality, satisfaction, and effectiveness of the products and services provided. The information obtained will be used to improve the equipment, personnel, and overall provision of SINTEL's services. Authorization also covers situations such as inquiries, requests, claims, loyalty, and service cancellation. The user acknowledges that refusing to grant this authorization could affect the indicators.

1.6.8 Information about cookies and data storage and/or retrieval devices:

This website collects standard logging information, such as IP address, browser type, language, access times, and website addresses. In order to ensure effective administration and improve the browsing experience, we or our service providers may use cookies or data storage and/or retrieval devices to obtain aggregated data. For more details on the use of cookies and other tracking technologies, as well as to learn about control options, please refer to our Cookies and Data Storage and/or Retrieval Devices Policy.

1.6.9 Conservation

The retention of personal data will only be carried out for the time necessary to fulfill the purposes described in the Personal Data Protection Policy, or up to a maximum of 6 years. After this period, the data will be deleted.

1.6.10 Transfer and communication of personal data:

SINTEL will transfer your personal data, either locally or internationally, to any member of the company; likewise, if necessary to comply with obligations or requirements of the competent authority, personal data may be disclosed to governmental, regulatory authorities, or other third parties. SINTEL will ensure that the third parties to whom this data is transferred comply with appropriate standards of confidentiality, protection, and security, especially when located in countries without data protection legislation that meets the criteria established by applicable regulations in each jurisdiction.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1.6.11 Security

The website implements security measures aimed at safeguarding the personal information provided by its visitors, in order to prevent unauthorized access, disclosure, destruction, or misuse.

1.6.12 Rights of access, rectification, updating, deletion, suspension, and opposition:

SINTEL acts in accordance with the Organic Law of Data Protection, so the data subject has the right to exercise the rights of rectification, updating, opposition, limitation, portability, or deletion of the data provided to the company as established in the articles detailed below.

CHAPTER I

COMPREHENSIVE SCOPE OF APPLICATION

Art. 1.- Object and purpose. - The object and purpose of this law are to guarantee the exercise of the right to the protection of personal data, which includes access and decision-making regarding information and data of this nature, as well as their corresponding protection. For this purpose, it regulates, foresees, and develops principles, rights, obligations, and protection mechanisms.
CHAPTER III

RIGHTS

Art. 13.- Right of access. The data subject has the right to know and obtain, free of charge, from the data controller access to all their personal data and the information detailed in the preceding article, without the need to provide any justification. The data controller must establish reasonable methods to allow the exercise of this right.

Art. 14.- Right of rectification and updating. The data subject has the right to obtain from the data controller the rectification and updating of their inaccurate or incomplete personal data. For this purpose, the data subject must provide the relevant justifications, when applicable.

Art. 15.- Right of erasure. The data subject has the right for the data controller to erase their personal data when:

- The processing does not comply with the principles established in this law;
- The processing is not necessary or relevant for the fulfillment of the purpose;
- The personal data have fulfilled the purpose for which they were collected or processed;
- The retention period for personal data has expired;
- The processing affects fundamental rights or individual freedoms.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

Art. 16.- Right to object. The data subject has the right to object to or refuse the processing of their personal data in the following cases:

- Where fundamental rights and freedoms of third parties are not affected, the law permits it, and it does not concern public information, public interest, or data processing ordered by law.
- When the processing of personal data is for direct marketing purposes; the data subject shall have the right to object at any time to the processing of personal data concerning them, including profiling; in which case, personal data shall no longer be processed for such purposes.
- When consent for processing is not necessary due to the presence of a legitimate interest, as provided in Article 7, and it is justified in the specific personal situation of the data subject, provided that a law does not stipulate otherwise.
- The data controller shall cease processing personal data in these cases, unless it can demonstrate compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject, or for the establishment, exercise, or defense of legal claims.

The purpose of this law is to guarantee the exercise of the right to the protection of personal data, including access and decision-making regarding information and data of this type, as well as their proper protection. To this end, it regulates, foresees, and develops principles, rights, obligations, and protection mechanisms.

1.6.13 Process and form to exercise the rights of access, rectification, updating, deletion, and opposition:

This process can be carried out through the following steps:

The data subject can contact SINTEL to exercise their rights through the institutional email protecciondatos@sintel-international.com.

When submitting the request, at least the following personal data must be included: names, surnames, ID number, email, and telephone number, as well as the specific right that is desired to be exercised (access, rectification, updating, limitation, opposition, or deletion) as specified in the form.

SINTEL, through the certified Personal Data Protection Officer, will assess the relevance of the request and classify it as appropriate or not. The assigned customer service representative will notify the resolution within the deadlines established by the Organic Law on Personal Data Protection (LOPDP) and communicate the decision to the email or telephone number of the data subject who submitted the request.

SINTEL reserves the right to make changes and updates to its Personal Data Processing Policy as necessary or in response to provisions or updates in personal data protection

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

regulations. Data subjects can consult the website for the latest information on updates to the Personal Data Processing Policy.

1.6.14 Right to data portability:

You have the right to require the data processor to deliver your personal data in a format that is compatible, up-to-date, structured, common, interoperable, and machine-readable, maintaining its characteristics, or to transfer it to other data controllers.

1.6.15 Procedure to exercise the right to data portability:

To request the portability of your data, it is necessary to send a request to the contact email of the data controller, indicated in section 2 of this policy. In the request, the data to be received and/or transferred must be specified, as well as the destination, format, and necessary characteristics to carry out said exercise.

1.6.16 Existence of automated assessments and the right not to be subject to a decision based solely or partially on automated assessments:

With the data collected through our website, no automated assessments are conducted. The right not to be subjected to a decision based solely or partially on assessments that are the product of automated processes, including profiling, which produce legal effects on the individual or that infringe upon their fundamental rights and freedoms, is acknowledged.

There are certain exceptions in which we may reject a request not to be subject to a decision based solely or partially on automated assessments, for example, when personal data is necessary for compliance with the law or in connection with claims.

1.6.17 Process to enforce the right not to be subject to a decision based solely or partially on automated assessments:

To exercise the right not to be subject to decisions based entirely or in part on automated evaluations, it is required to send a request to the contact email of the data controller, detailed in section 2 of this policy.

1.6.18 Implications of providing or denying the provision of data:

Providing the data will enable the fulfillment of the objectives detailed in section 5 of this policy. If the data subject refuses to provide them, we will not be able to communicate with them to offer our services, and in general, we will not be able to fulfill the purposes of the processing.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1.6.19 Consequences of providing incorrect or inaccurate information:

Providing incorrect or inaccurate data impacts the quality of the services we offer through the website.

1.6.20 Withdrawal of consent:

At any time, you have the option to request the cessation of the processing of your personal data. To make this request, it is necessary to notify us through the email indicated in section 2 of this policy.

1.6.21 Links to third-party websites:

Our website may contain links to third-party websites for your convenience. We are not responsible for the privacy policies or practices of third parties. Any information you provide to a third party will be subject to its privacy policy. Upon leaving the SINTEL website, where this notice is published, or being redirected to a third-party website, application, or other online service, we recommend that you read and become familiar with the privacy terms or policies applicable to that third party.

1.6.22 Children and Adolescents:

We do not seek to obtain information from children under the age of 12. In situations where information is provided about children under the age of 12, the express consent of their legal guardian will be required. Adolescents aged 12 or older have the capacity to give their consent directly.

1.6.23 Social Media

SINTEL's profiles on Instagram, Facebook, and LinkedIn are exclusively intended to provide information and disseminate content. They should not be used as appropriate channels to submit complaints, claims, or legal inquiries related to the protection of personal data. Such inquiries should be directed to the email address protecciondatos@sintel-international.com, following the requirements established in the applicable regulations.

The responses provided through SINTEL's profiles are of an informative nature, and SINTEL reserves the right not to respond individually to messages or comments received through these channels.

The graphical, audio, and/or video elements shared on these profiles are the property of SINTEL and are protected by intellectual property laws. Some publications may include links to third-party websites considered of interest. SINTEL does not assume responsibility for the content of these pages.

SINTEL follows other profiles and accounts on these platforms, and this fact does not necessarily imply any kind of affiliation with them.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

SINTEL reserves the right to modify or delete messages, whether its own or from third parties, published on its profiles at any time and without prior notice.

1.6.24 How to contact us?

If you wish to obtain more information about how your personal data is managed, please contact us using the contact information provided in section 2 of this policy.

1.6.25 Modifications to our personal data protection policy:

We reserve the right to modify or amend this Personal Data Protection Policy when necessary, and we will inform you of such changes through our website. The revision date will be updated in the event of modifications, and the new provisions will take effect from that date. Therefore, we recommend that you regularly review this Policy to be aware of the protection procedures implemented by SINTEL.

1.7 INFORMATION SECURITY POLICY

The purpose of this policy is to implement a set of measures aimed at preserving the confidentiality, integrity, and availability of information, which are essential elements of information security.

a) ***Confidentiality:*** Restricted access to sensitive information is ensured, limited only to authorized personnel, as a fundamental part of our information security policy. Additionally, encryption measures are implemented both in data storage and transmission to safeguard the confidentiality of the information.

b) ***Integrity:*** Ensuring the accuracy and completeness of information is essential for the integrity of our data. To achieve this, rigorous validation controls and procedures will be established to ensure the quality and truthfulness of the information at each stage of its handling. Also, as a preventive measure against potential contingencies, regular backup systems are implemented to prevent both data loss and corruption of critical data.

c) ***Availability:*** Ensuring the continuity of such systems by implementing measures that ensure their constant operability. This involves establishing contingency procedures and disaster recovery plans to minimize downtime in the event of incidents.

d) ***Responsibility:*** Defined roles and authority limits are established so that each team member is aware of their specific responsibilities in this area. In addition to fostering awareness and training in security among all employees, it is essential to create an organizational culture oriented towards information protection.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

e) Legal and Regulatory Compliance: Strict compliance with all relevant laws and regulations, thus guaranteeing the integrity and confidentiality of the data. To ensure continuous compliance, it is imperative to keep security controls updated, adjusting them according to modifications in regulatory requirements.

f) Risk Management: A proactive approach is taken that involves the regular identification, assessment, and mitigation of risks associated with information security. To ensure the effectiveness of the implemented measures, regular audits are conducted to assess the degree of compliance with established security policies.

g) Procedures and Guidelines: Effective implementation of security controls with the establishment of detailed procedures and specific guidelines covering fundamental aspects such as access management, event monitoring, and incident management, among others; the clarity and specificity of these protocols are essential to ensure consistent and efficient application of security measures.

h) Review and Update: This process is carried out regularly to adapt the policy to dynamic changes in the technological environment. This practice not only reflects a continuous commitment to security but also allows for the improvement of the effectiveness of the implemented security controls.

i) Responsibility: Each employee is responsible for adhering to this policy and for reporting any incidents related to information security.

1.8 INFORMATION SECURITY, HEALTH, AND ENVIRONMENT POLICY

SINTEL ensures the well-being of its employees through the implementation of control measures that prevent risks and minimize potential environmental impacts resulting from the company's activities. Therefore, we are committed to:

- Complying with regulations, internal policies, and other applicable legal and regulatory requirements, both for internal personnel and third parties linked to the company, such as suppliers, contractors, and business partners.
- Identifying, evaluating, and managing risks and opportunities arising from the company's activities.
- Fostering innovation and increasing productivity with profitability, efficiency, sustainability, safety, health, and asset integrity criteria.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

- Establishing objectives and goals to improve the company's performance and ensuring their achievement through the allocation of necessary technical, human, and material resources, as well as the adoption of the best available technology.
- Ensuring transparency in the information provided to stakeholders through internal processes, controls, and protocols that guarantee its reliability and rigor, and preserving the confidentiality of such information.
- Providing training and information to ensure that staff understand and know the rules and commitments necessary to perform their duties.
- Implementing processes of participation, dialogue, and consultation with stakeholders to meet their needs and expectations, foster shared value creation, and consolidate Enagás's recognition as a leading company in the field.
- Fostering a culture of excellence and people's participation by promoting teamwork, internal communication, knowledge management, talent development, equal opportunities, and recognition of achievements.
- Maintaining a culture of resilience to properly manage crises, threats, or disruptive situations that may arise.
- Documenting, implementing, and maintaining the Integrated Management System.
- Ensuring a high level of security in facilities and work, ensuring safe conditions in the design, operation, and maintenance of facilities, processes, and equipment.
- Establishing emergency measures and actions for crisis situations in different centers and workplaces, aimed at ensuring the protection of people, assets, and the environment during their activities.
- Planning, controlling, and managing risks arising from or related to modification projects of the installation or operational changes to prevent foreseeable emergency situations.
- Eliminating hazards and reducing risks to safety and health at work, in order to prevent occupational diseases and accidents.
- Promoting physical and emotional health and well-being through awareness and sensitization campaigns.
- Ensuring information, consultation, and participation of workers in occupational safety and health issues.

1.1. COOKIES AND DATA STORAGE AND/OR RETRIEVAL DEVICES POLICY

The Cookies and Data Storage and/or Retrieval Devices Policy aims to provide information to users of the website https://www.sintel-international.com about the handling of cookies and data storage and/or retrieval devices on their devices. In general terms, the use of cookies is linked to the processing of personal data, so it is advisable to review the Personal Data Protection Policy available on the website for detailed and accessible information on this topic.

What is a Cookie or data storage and/or retrieval device?

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

Small text files or data storage and/or retrieval devices include:

- Small text files.
- Other similar technologies for installation and/or data collection on or about your device (such as web beacons, bugs, pixels, HTML5, SDK).
- Techniques used for device identification information combination (fingerprinting).

These elements are stored by the website https://www.sintel-international.com on your computer, tablet, smartphone, or similar device. They contain information about your browsing or usage for the purpose of providing functionalities and tools to the website and the user. Additionally, they facilitate navigation, enhance user experience, and allow the website to understand how people interact with it, as well as to offer own or third-party advertising.

It is important to highlight that cookies and data storage and retrieval devices do not harm your devices.

What cookies or data storage and/or retrieval devices do we use?
Below are the categories of cookies or data storage and/or retrieval devices we use, and it will depend on your choice what type of cookies and data storage and/or retrieval devices we place.

Functionality cookies or storage and/or retrieval devices:
These cookies or storage and/or retrieval devices allow web pages and applications to retain information to personalize the customer or user experience, offering distinctive features. They are essential for the operation of web pages and applications, and their non-acceptance prevents access to or use of our products or services.

Navigation cookies or storage and/or retrieval devices:
Navigation cookies or storage and/or retrieval devices store information about the user's visit, facilitating future interactions and making the visit more practical. Non-acceptance of these cookies may result in slow performance or inappropriate recommendations.

Security cookies or storage and/or retrieval devices:
These cookies or storage and/or retrieval devices help authenticate users, prevent fraud, and protect user interaction with the service. Their non-acceptance may expose users to security risks or be used to compromise the security of the Cooperativa de Ahorro y Crédito Policía Nacional Ltda.

Session cookies or storage and/or retrieval devices:
Session cookies or storage and/or retrieval devices aim to assign the user a specific session. Non-acceptance of these cookies prevents customers or users from accessing functional areas of web pages or applications.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

Analysis cookies or storage and/or retrieval devices:
Analysis cookies or storage and/or retrieval devices quantify the number of users, sections visited, and interaction on various platforms, allowing measurement and analysis of the use of web pages and applications anonymously.

Behavioral advertising cookies or storage and/or retrieval devices:
Behavioral advertising cookies or storage and/or retrieval devices determine the continued behavior of users or customers, creating specific profiles to display personalized advertising. Non-acceptance of these cookies may reduce the effectiveness of advertising spaces.

How can I manage the use of Cookies on this website?
It is relevant to note that the Cookies used on our web platform are exclusively those necessary for the core processes and security of our members.

If you are browsing online, you have the option to disable the use of Cookies in your browser. This ability to prevent the use of Cookies is available at any time and can be executed at your discretion.

Who uses the information stored in Cookies?
The information stored in the cookies of our web pages and applications is used exclusively by our organization, except for third-party cookies. The latter are used and managed by other entities for the purpose of providing us with services aimed at enhancing the experience of our customers or users during their use.

Cookies and similar tracking technologies are used to track activity on Our Service and store certain information. The tracking technologies used include beacons, tags, and scripts to collect and track information and improve and analyze Our Service. The technologies we use may include:

Cookies or Browser Cookies. A cookie is a small file placed on your device. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. However, if you do not accept cookies, you may not be able to use some portions of our Service. Unless you have adjusted your browser setting so that it will refuse cookies, our Service may use cookies.

Web Beacon. Certain sections of our Service and our emails may contain small electronic files known as web beacons (also referred to as clear gifs, pixel tags, and single-pixel gifs) that enable the Company, for example, to count users who have visited those pages or opened an email and for other related website statistics (for example, recording the popularity of a certain section and verifying system and server integrity).

Cookies can be "Persistent" or "Session" cookies. Persistent cookies remain on your personal computer or mobile device when you go offline, while session cookies are deleted as soon as you close your web browser.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

We use both session and persistent cookies for the purposes set out below:

- Necessary/Essential Cookies
- Type: Session Cookies
- Managed by: Us

Purpose: These cookies are essential to provide you with services available through the website and to enable you to use some of its features. They help to authenticate users and prevent fraudulent use of user accounts. Without these Cookies, the services that you have asked for cannot be provided, and we only use these Cookies to provide you with those services.

- Cookies Policy / Cookie Acceptance Notice
- Type: Persistent Cookies
- Managed by: Us
- Purpose: These Cookies identify if users have accepted the use of cookies on the Website.
- Functionality Cookies
- Type: Persistent Cookies
- Managed by: Us

Purpose: These cookies allow us to remember choices you make when you use the website. The purpose of these Cookies is to provide you with a more personal experience and to avoid you having to re-enter your preferences every time you use the website.

1.9 POLICY FOR PROTECTION OF PERSONAL DATA BY VERTICALS

a) Electronic Security Solutions

It provides responses to its clients' technological demands. In a context of insecurity affecting the country, not only related to organized crime but also to the lack of access controls and the notification of alarms for security protocol violations, which could affect both personnel and commercial assets, Electronic Security addresses this issue by understanding:

- Safecam
- CCTV
- Safe Entry
- Fire detection
- Alarm and Intrusion System
- Access control

b) Transit Solutions

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

It installs high-tech devices in the road infrastructure, as well as security products for monitoring and control. The company has a comprehensive understanding of this process.

- Mobile Bus
- BodyCams
- Speed cameras
- GPS Tracking
- Dashcam
- MDVR

1.10 ANTI-BRIBERY POLICY

The purpose of this policy is to openly manifest the commitment to ethical and transparent conduct towards stakeholders, as well as to carry out commercial operations responsibly and sustainably, applying a philosophy of zero tolerance towards actions contrary to organizational principles.

a) Commitment of Executives:

This goes beyond compliance with legal requirements; it implies the permanent management of an ethical culture rooted at all levels of the company. As leaders, they maintain this commitment to act as role models guiding others with their ethics and integral conduct. Their firm stance against corruption sends a clear message about the values the company holds in general.

b) Transparent Procedures:

Transparent procedures are managed to safeguard SINTEL's integrity in conducting due diligence when selecting personnel, business partners, contractors, and suppliers; allowing for a thorough assessment of the suitability and integrity of the parties involved in operations, ensuring adherence to established ethical and legal standards. By incorporating transparency into the selection processes, the company not only significantly reduces the risks associated with potential misconduct but also reinforces its commitment to ethical practices.

c) Whistleblower Channel:

This channel provides a secure means to report possible cases of corruption or bribery without fear of reprisals. By offering the possibility of making anonymous reports, our company encourages active participation in the detection and prevention of misconduct. This not only strengthens internal integrity but also acts as a deterrent against corrupt practices by demonstrating the organization's commitment to accountability and justice.

d) Training and Awareness:

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

Regular training is provided on anti-corruption and anti-bribery policies. These sessions not only offer detailed information on key principles and practices but also serve to enhance collective understanding of ethical implications in the work environment in compliance with regulations and internal policies.

e) Audits and Monitoring:

Internal audits provide us with a detailed view of the effectiveness of internal controls, while external audits provide an impartial and objective perspective. By proactively monitoring compliance and the effectiveness of anti-corruption policies, our company can address any deviations early on and strengthen its prevention mechanisms.

f) Sanctions and Discipline:

Sanctions are established for employees who violate the policies of our company, emphasizing our strong intolerance towards any form of corruption. Disciplinary actions, which may vary depending on the severity of the infraction, range from internal corrective measures to, in extreme cases, legal actions.

g) Cooperation with Authorities:

We maintain a total willingness to cooperate openly and transparently with the competent authorities, if required, demonstrating our clear commitment to the fight against corruption in accordance with current legal regulations.

1.11 COMMISSION POLICY

Through this policy, the company acknowledges the effort and commitment of its employees in business-related activities, covering various aspects that are essential for the fair operation of a compensation system based on the principles of transparency and honesty.

A variable for commission payment will be considered for personnel in any of the following categories:

- Employees under an employment relationship
- Professional service personnel
- Collaborators under occasional service agreements

Objetivo

To promote the improvement of performance, efficiency, productivity, and income of its workers through incentives linked to the projects being carried out.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

In this regard, SINTEL has established a specific commission policy according to the type of commission agent and the scope of the project under the following guidelines:

		AMOUNT		COMMISSION RANGE	
		FROM	TO	% MIN	% MAX.
SALES	EMPLOYEES UNDER DEPENDENCY	$ -	$ 50.000,00	5%	10%
		$ 50.001,00	$ 100.000,00	3%	8%
		$ 100.001,00	HENCEFORTH	1%	3%
	SERVICES PROVIDED	$ -	$ 50.000,00	5%	10%
		$ 50.001,00	$ 100.000,00	3%	8%
		$ 100.001,00	HENCEFORTH	1%	3%
	OCCASIONAL SERVICES	$ -	$ 50.000,00	3%	5%
		$ 50.001,00	$ 100.000,00		
		$ 100.001,00	HENCEFORTH		
INVESTMENT PROJECTS	EMPLOYEES UNDER DEPENDENCY	$ -	HENCEFORTH	8%	
	SERVICES PROVIDED				

GUIDELINES

a. All projects must be socialized and registered on the project platform, indicating client data, project context, and the problem and solution to be offered.
b. The commission agent will provide SINTEL with all the information regarding the development in a timely manner and is committed to monitoring and reporting on progress in negotiations with the prospect.
c. The commission agent will handle only the information, prices, and conditions through the digital tool GOOGLE DRIVE, where all respective backups of all project stages must be stored.
d. Commissions will be paid individually when the project warrants it, and the collaborator's involvement is unique and direct in signing the contract.
e. Commissions will be charged for each purchase order issued by the client, regardless of the breakdown of operations.
f. Commission payments will be made once the project contract is closed, and the amount of the commission will be according to the following table:

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

g. Commission payment will be 100% if the client has made the agreed-upon disbursement for the project, and it will be reflected in the next payroll for employees under dependence or for professional services or within 30 days for workers under occasional services.
h. Payment will be subject to the final payment method of each client; that is, if a sufficient cash payment is made to cover the commission, the payment will be made in cash.
i. Commissions will be paid on the value of the profit.

Update of the ranges of this Policy

If it is desired to modify what is established in this Policy, the General Manager must convene the board where the modification will be presented and approval will be requested from the shareholders' meeting, and it will be registered and become effective from the date of subscription. Once the Policy is adjusted, an email will be sent to the involved parties for socialization.

Avenida de los Shyris N35-174 y Suecia
Edificio Renazzo Plaza, Of. 807
Telf.: 02 225 2050

1.12 ANNEXES

REQUEST FOR DATA PROTECTION RIGHTS	Code:	SIN-001-PD
	Edition:	First
	Page:	1 de 1
Date of Request:	DD-MM-YY	

APPLICANT'S INFORMATION	
Full Name: (first name and last name)	
Identification Number	
Address:	
Province:	
City:	

I request that all administrative acts resulting from this procedure be notified to my email address.

YES ☐ NO ☐

If the response is positive, please indicate the email address: _____

In accordance with the provisions of the Organic Law on Personal Data Protection, I request:

CHECK WITH AN (X) THE RIGHTS OF PERSONAL DATA SUBJECTS YOU WISH TO EXERCISE:	
ACCESS (request to obtain and know what personal data are held and for what purpose they are used).	x
RECTIFICATION and UPDATING (request the correction of inaccurate or incomplete personal data).	☐
DELETION (request the deletion of personal data that are no longer necessary for the purpose for which they were collected).	☐
OBJECTION (request to object to the processing of your personal data).	☐
SUSPENSION (request the suspension of the processing of my personal data).	☐

PLEASE SPECIFY THE TYPE OF PERSONAL DATA:

_____
_____
_____

Signature: _____

SINTELINTERNATIONAL S.A.S ensures the security and confidentiality of the personal data provided, and thus, in accordance with the provisions of the Organic Law on Personal Data Protection and its Regulations, the user is informed and gives consent to the incorporation of their data into automated and non-automated Personal Data Files, as well as to the processing of these, for the purpose of exercising their rights.
The Personal Data Protection Policy of SINTELINTERNATIONAL S.A.S guarantees the adoption of the necessary technical, organizational, and legal measures to ensure the confidential treatment of such data.
Delivery Instructions:
1. All requested information must be provided in the corresponding spaces.
2. The document should be sent to the email address protecciondatos@sintel-latam.com
3. You must attach the original copy of your ID document and include a copy of it with your request.