INTEGRATED MANAGEMENT SYSTEM
DRUMMOND ENERGY INC.

PERSONAL DATA PROTECTION POLICY

CODE: SIGDEI-0976

	Date	Position
Elaborated by	January 2026	Compliance Systems Coordinator
Reviewed by	February 2026	Data Protection Officer / Legal Manager DLTD / Legal Representative
Approved by	March 2026	Country Manager, Drummond Energy, Inc

TRACK CHANGES		
Version	**Date**	**Summary Description of Change**
1	October 2019	Manual Creation
2	January 2022	Update of principles and purposes
3	March 2026	Separation of the Manual and the Policy

TABLE OF CONTENTS

1. OBJECT

This Policy aims to inform stakeholders and data holders about the processing of personal data that our Company stores in its physical and digital databases, which will be processed in accordance with the principles and duties defined in the Law, during the stages of collection, storage, use, circulation and deletion, whether as controller or processor. It also presents the channels available for data holders to exercise their rights.

2. SCOPE

DRUMMOND ENERGY, INC., identified with NIT 900.786.712-3 and domiciled at Calle 72 No. 10-07, Office 503 of Bogotá DC (hereinafter, "The Company"), recognizes the importance of guaranteeing the security, privacy and confidentiality of the personal data of all counterparties with whom it maintains a contractual, commercial or institutional relationship in the development of its corporate purpose. In compliance with constitutional and legal mandates, the Company adopts this Personal Data Protection Policy, applicable to all its activities involving personal information both nationally and internationally, in accordance with current legislation and applicable international treaties.

The right of access to the data holder's personal data will be guaranteed, after accreditation of his/her identity or that of his/her representative, making his/her personal information available to him/her free of charge, so that the holder can make effective his/her right to rectify, correct or request the deletion of all or part of his/her data. In accordance with the principle of standing to sue, this right may be exercised by:

- Anyone who demonstrates a relationship up to the fourth degree of consanguinity and second degree of affinity, presenting a document that proves legal representation, a notarized power of attorney or the status of heir (ruling or deed of succession) or their successors .
- Whoever proves to be the surviving spouse.
- General attorney or with express authorization to exercise the right of habeas data.
- Legal requirement.

In light of the above, and pursuant to Article 15 of the Constitutional Charter, Law 1581 of 2012 and other regulations that govern or complement it, we hereby list the components for this Policy.

3. DEFINITIONS

- **Authorization:** prior, express and informed consent of the owner to carry out the processing of personal data. Consent may be given in writing, orally, or through unambiguous conduct by the holder that allows the conclusion that authorization was given.

- **Privacy notice:** verbal or written communication generated by the responsible party, addressed to the data holder for the processing of their personal data, through which they are informed about the existence of the information processing policies that will be applicable, how to access them and the purposes of the processing that is intended to be given to the personal data.

- **Database:** an organized set of personal data that is subject to processing.

- **Successor:** person who has succeeded another due to the latter's death (heir or legatee).

- **Surviving spouse:** refers to the surviving spouse.

- **Personal data:** any information linked or that can be associated with one or more specific or identifiable natural persons, who are registered in a database that makes them susceptible to processing.

- **Public data:** data that is not semi-private, private or sensitive, which can be processed by any person, without the need for authorization to do so. Among others, the following are public: data contained in the civil registry of persons (e.g., whether one is single or married, male or female) and those contained in public documents (e.g., contained in Public Deeds), in public records (e.g., the disciplinary record of the Attorney General's Office), in official gazettes and bulletins, and in final judicial judgments that are not subject to confidentiality.

- **Semi-private data:** this is data that, in addition to being of interest to the owner, may be of interest to a sector or group of people, for example: financial and commercial information. This specific type of data is subject to protection under Law 1266 of 2008, and the authority on the matter is the Finance Superintendency.

- **Private data** : data whose knowledge is restricted to the public.

- **Sensitive data:** is data that affects the privacy of the data holder or whose misuse may lead to discrimination, such as data revealing racial or ethnic origin, political orientation, religious or philosophical beliefs, membership in trade unions, social or human rights organizations or organizations that promote the interests of any political party or guarantee the rights and guarantees of opposition political parties, as well as data relating to health, sex life and biometric data, among others, the capture of still or moving images, fingerprints, photographs, iris, voice recognition, facial or palm recognition, etc.

- **Data processor:** natural or legal person, public or private, who carries out the processing of data on behalf of the controller.

- **Data controller:** natural or legal person, public or private, who decides on the database and the processing.

- **Data holder:** natural person whose personal data is being processed, as well as legal persons when the data of the natural persons that make it up are involved.

- **Processing:** any operation on personal data, such as collection, storage, use, circulation or deletion.

- **Transmission:** communication of data, within or outside the Colombian territory, whose sender is the responsible party and whose receiver is the data processor.

- **Transfer:** sending data, within or outside the national territory, whose sender and, in turn, recipient, is a data controller.

4. GUIDELINES

The Company is committed to protecting information obtained in the ordinary course of its business. For this reason, our Policy and Procedures are based on current regulations regarding the protection of personal data that has been provided to us. Our intention is to collect exclusively the information obtained voluntarily from our Clients, suppliers, employees, former employees, contractors or third parties, on the occasion of the legal, contractual or commercial relationship that binds us, and thus comply with the legal and contractual obligations in the development of our economic activity. In this regard, the present Policy has been developed and adopted, which reflects the requirements of Colombian legislation on the matter.

5. FUNDAMENTAL PRINCIPLES

a) **Principle of legality:** The processing of personal data is a regulated activity that must comply with the provisions of Law 1581 of 2012, Decree 1074 of 2015 and other provisions that modify, add or complement them. Consequently, the Company guarantees that the collection, use and circulation of data will be carried out in strict compliance with current regulations, protecting the fundamental rights of the data holders.

b) **Principle of freedom:** the processing of personal data in the Company can only be carried out with the prior, express and informed consent of the owner. Personal data may not be obtained or disclosed without such authorization, except by legal or judicial mandate that waives the requirement for consent.

In accordance with the Law, authorization will not be necessary when it involves: (i) information required by a public entity in the exercise of its legal functions, (ii) data of a public nature, (iii) cases of medical or health emergency, and (iv) processing of information for statistical, historical or scientific purposes where the owner is not identified.

c) Principle of purpose: the processing of personal data in the Company must be for a legitimate, specific and lawful purpose, which must be framed within the development of its business activities and compliance with its legal obligations. This purpose will be clearly communicated to the holder in advance at the time of requesting their authorization. Consequently, the Company may not use the data for purposes other than those authorized, unless a new authorization is obtained or the Law so permits.

d) Principle of truthfulness or quality: the information subject to processing by the Company must be truthful, complete, accurate, up-to-date, verifiable and understandable. The processing of partial, incomplete, fragmented or misleading data is strictly prohibited.

The Company will take reasonable measures to keep the data up to date; however, the owner assumes the obligation to report any changes to their information. In the case of data from public records, the veracity and quality of this data will be the responsibility of the originating entity or owner, and the Company will be exempt from liability regarding the accuracy of said information.

e) Principle of transparency: the Company guarantees the right of the data holder to obtain, at any time and without restrictions, information about the existence of personal data concerning him or her that is in the Company's databases; the exercise of this right will be free of charge. The above shall be applied in accordance with the exceptions provided for in Article 2 of Law 1581 of 2012, with respect to those databases that, by their nature (e.g. national security, intelligence, personal or domestic use), are excluded from the general scope of application of said rule.

f) Principle of restricted access and circulation: The processing of personal data in the Company is subject to the limits derived from the nature of the data, the provisions of Law 1581 of 2012 and the Political Constitution. Access to the information is restricted exclusively to persons authorized by the owner or those authorized by law.

Personal data, except for information of a public nature, will not be available on the internet or other means of mass dissemination, unless technical control measures are implemented that guarantee restricted access only to the owners or authorized third parties. The Company will ensure that access profiles to its information systems respect this principle, limiting the circulation of data according to the purpose for which it was collected.

g) **Security Principle:** The Company, in its capacity as controller and/or processor, will implement the necessary technical, human and administrative measures to ensure the security of personal data, preventing its alteration, loss, consultation, use or unauthorized or fraudulent access.

To this end, the Company will adopt security protocols, technological protection tools and administrative controls applicable to both electronic repositories and physical files, guaranteeing the integrity, availability and confidentiality of information in accordance with information security standards and best practices.

h) **Principle of confidentiality:** all persons involved in the processing of personal data in the Company are obliged to guarantee the confidentiality of the information, even after their employment or contractual relationship has ended. This duty implies the commitment not to disclose to third parties personal, commercial, accounting, technical or any other type of information to which they have access in the exercise of their functions.

The Company will require its employees, contractors, and strategic partners to sign confidentiality agreements or confidentiality clauses in their respective contracts. The provision or communication of personal data will only be appropriate when it corresponds to the development of activities authorized by the owner or by the Law, always maintaining due diligence in the custody of the information.

i) **Principle of necessity and proportionality:** the processing of personal data in the Company will be limited to those data that are strictly necessary, adequate and relevant to fulfill the legitimate purposes informed to the owner.

Under this principle, the Company will avoid collecting excessive or unnecessary data. Likewise, personal data will only be kept for the reasonable and necessary time to fulfill the purpose that justified its processing and to comply with the relevant legal, accounting or administrative obligations, proceeding to its deletion or anonymization once said purpose has been exhausted.

j) **Principle of temporality or expiry:** the period of permanence of personal data in the Company's information systems will be strictly necessary to fulfill the purpose informed to the holder in the authorization.

Once the purpose of the processing has been fulfilled, and provided that there is no legal, contractual or accounting mandate that obliges its retention (such as statute of limitations for legal actions or mandatory document retention periods), the Company will proceed to delete the data or anonymize it, ensuring that it cannot be used to identify the owner or be holder to

unauthorized access.

In accordance with the fundamental principles, the Company declares:

- To be responsible for the personal information in its possession.
- To inform in advance and expressly the purpose of the collection of personal data.
- To process personal data, only with prior, express and informed consent from the data holder.
- To limit the amount and type of personal information collected, solely to fulfill the processing purposes presented here and authorized by the data holders.
- To use and share the personal data it may have, only for the purposes authorized by the owner.
- To update the personal information that it may have in its possession or control and, in any case, respond to requests for updating or deletion within the legal terms.
- To protect personal data with reasonable security measures, taking into account the nature of the personal information being collected.
- To guarantee to the holders of personal data that, at any time and in accordance with the legal terms, it will respond to requests for information submitted to it.

6. AUTHORIZATION

The Company will request authorization in such a way that the data holder gives their prior, express and informed consent to the processing to which their personal data is subject.

Authorization may also be obtained from unequivocal conduct of the data holder, which reasonably allows the conclusion that he/she gave his/her consent for the processing of his/her information. Such actions must clearly express the will to authorize the processing.

The data holder's consent may be obtained by any means that can be subsequently verified, such as written, verbal, virtual communication or unambiguous conduct.

By virtue of its nature and corporate purpose, the Company receives, collects, registers, keeps, stores, modifies, reports, consults, delivers, transmits, transfers, shares and deletes personal information, for which it obtains the prior authorization of the owner.

The Company will keep proof of such authorizations in an appropriate manner, ensuring and respecting the principles of privacy and confidentiality of information.
To inform employees of the updated personal data protection policy, the Company will issue an internal statement which will be shared via email and other authorized channels for their information. The updated Personal Data Protection Policy will be disseminated to employees through internal communications and corporate channels. For third parties and the general public, changes will be notified through a privacy notice posted on our official website.

The data holder may at any time revoke their consent for the processing of their data, provided that it is legally and contractually permitted, by sending a communication or request through the customer service channels provided for this purpose, providing a copy of their identification document.

If a third party exercises these rights, they must:

- **Successor of the holder:** prove such status according to the current means of proof to legitimize their cause.
- **The representative and/or agent of the holder:** upon prior accreditation of the representation or power of attorney.

Furthermore, the general public is informed that authorization for data processing is not required in the following cases:

- Information required by a public or administrative entity in the exercise of its legal functions or by court order.
- Data of a public nature.
- Medical or health emergency.
- Processing of information authorized by law for historical, statistical or scientific purposes.
- Data related to civil registration.
- Databases and files whose purpose is the prevention, detection, monitoring and control of money laundering and the financing of terrorism, in accordance with Article 2 of Law 1581 of 2012.
- Databases and archives of journalistic information and other editorial content.

7. COLLECTION METHODS

The Company wishes to inform that it will have various means to obtain authorization from the data holders, and may also store personal data through physical or electronic files, for the preservation of proof of the authorization granted by the data holders.

Furthermore, it will comply at all times with the technical and legal controls to establish applicable and reasonable security conditions, in order to prevent access, loss, alteration or fraudulent use of the data.

The personal data that the Company has collected, or that it collects in the course of its commercial, contractual and/or social activity, strictly corresponds to the following categories, in accordance with the authorization granted by the data holder and the need for each process:

- **Identification and contact information**: name, ID number, address, telephone, email address, marital status, date of birth.
- **Employment and professional data**: position, work history, academic background, professional experience, functions, start and end dates, type of contract, promotion history, job performance.
- **Education data:** level of studies, degrees obtained, educational institutions, certifications and professional licenses.
- **Financial, asset and economic data**: bank accounts, income, expenses, credit history (generally consulted in risk bureaus), payment information, withholdings, income declaration, salary, deductions, payroll and benefits information, properties, assets and liabilities.
- **Background information** : judicial, disciplinary, fiscal and list reports.
- **Family and beneficiary data:** only when necessary for social security, welfare or contractual benefits purposes.
- **Demographic data:** date and place of birth, age, sex, nationality.
- **Health data:** medical conditions, disabilities, results of occupational examinations necessary for OSH management, occupational health history, information on diseases, data on sexual life.
- **Affiliation data:** affiliation with unions, family compensation funds, pension and severance funds, health and social protection entities, funeral and banking services.
- **Biometric data:** fingerprints, facial and voice recognition. The provision of this type of data is optional on the part of the data holder.
- **Image and audio data:** photographs, video recordings and voice recordings (in customer service or security calls).
- **Browsing data:** IP address, browser type, operating system, time and date of access to websites.
- **Geolocation data:** geographic location.
- **Session data:** information generated by the use of applications, login credentials, encrypted passwords.
- **Data of minors:** data of children or dependents of employees will only be processed for the purposes of benefits and social security.
- **Data of minors from the communities:** only personal data of children and adolescents belonging to the communities of influence of the Company will be processed, within the development of its corporate social responsibility programs with prior authorization of the legal representative of the minor.

The collection of new categories of personal data will only be carried out after updating this Policy and obtaining a new express authorization from the data holder.

The Company has adopted information security policies and a technological infrastructure that reasonably protects the personal information collected, limiting its access, as far as possible, exclusively to persons who have an interest in it and who have been authorized to access it, in accordance with this Policy and current regulations.

The Company will make ongoing efforts to improve the security standards that protect the personal information it has collected.

8. PURPOSES

The Company will process the personal data of the data holders, provided that it has their prior, express and informed authorization, in accordance with the legal stipulations. Therefore, the purposes for which this processing will be carried out as controller and/or processor, according to the legal or contractual relationship that links it to the data holder, are presented below:

8.1. General purposes applicable to all data holders

a) **Legal and contractual compliance:** to execute the obligations arising from contractual, commercial, labor or any other type of relationship established with the data holder, as well as to comply with the legal duties imposed by the Colombian legal system (including the provision of information to judicial or administrative authorities), as well as to carry out internal and external audits to verify compliance with the Company's operational processes.
b) **PQR and judicial management:** attend to and process petitions, inquiries, complaints, claims (PQR), and information requests from judicial or administrative authorities.
c) **Transfer and transmission:** supply, transfer and/or transmit the data to third-party contractors (processors) or third parties (controllers) national or foreign with whom the Company establishes commercial or contractual relationships, for the development of its operations.
d) **Compliance systems:** conduct due diligence, consult and verify the holder's information in public and private databases and binding and restrictive lists, for the prevention of risks associated with compliance systems.
e) **Security and control:** ensuring the safety of people and property through access control to facilities, the use of video surveillance systems (CCTV) and the management of biometric data (fingerprints, face) for individualization purposes.
f) **Risk management:** conducting risk analysis, statistical and market studies, monitoring and improving the conditions of internal processes and the commercial or contractual relationship.
g) **Direct communication:** contacting the holder via physical mail, email, landline or mobile phone (including text messages or messaging applications), to send communications, notices or contact in case of emergency.
h) **Publications:** Publication of the Company's activities through the media.

i) **Accounting, tax and administrative management:** handling and monitoring of requests from judicial or administrative authorities and compliance with court rulings or administrative resolutions.
j) **Invitations:** contacting the data holders to send invitations to events or programs related to the purpose initially informed to each data holder.

8.2. Specific purposes for employees, former employees, and expatriates

a) **Pre-contractual or contractual management:** conduct reliability and security studies for positions that require it according to the risk profile.
b) **Labor relations management:** administering payroll, making salary payments, social benefits, social security and parafiscal contributions, granting benefits, administering extra-legal benefits such as humanitarian funds, housing programs and specific aid. This process includes the collection of personal data of the employee and their family unit, including minors.
c) **Occupational Health and Safety (OHS):** manage the OHS system, including the performance of occupational medical examinations (pre-employment, periodic and exit), management of medical records, prevention of occupational risks, development of promotion and prevention programs, health control and care by health professionals.
d) **Training and development:** develop training, education, social welfare and promotion of healthy lifestyles activities.
e) **Staff training:** training and development of human resources.
f) **Promotion and selection:** promotion and selection of personnel (includes interns and apprentices).
g) **Registration of entry and exit of documents:** issuance of certifications, records or copies requested by the holder, a duly authorized third party or by administrative or judicial order.

8.3. Purposes for suppliers and contractors

a) **Contracting and evaluation:** evaluate supplier compliance and performance, conduct reference management, and execute due diligence and knowledge processes to mitigate risks**.**
b) **Payments and credit:** perform accounting, tax and administrative management, including the payment of obligations and the management of portfolio and collections.
c) **Handling requests:** issuance of certificates, records or copies requested by the holder, a duly authorized third party or by administrative or judicial order.
d) **Training and development:** carry out training and development activities.

8.4. Purposes for domestic clients

a) **Check background:** commercial, reputational and potential risks associated with money laundering, terrorist financing and financing of the proliferation of weapons of mass destruction,

corruption, bribery, transactional bribery.

b) **Register in management systems:** perform registration for the development of the commercial, accounting, logistical and financial procedures of the operation.
c) **Formalize the contractual relationship:** to control the full execution of the obligations assumed.
d) **Evaluate performance and behavior:** to strengthen the procedures for hiring and commercial management.
e) **To allow the operation of DEI's security systems** on its premises and outside of them when appropriate, given the functions performed.
f) **Disclosure and communication:** that DEI may use, reproduce, disclose and publish, without any limitation, the activities, events, products, services, brands, logos and images that involve my client within the framework of our business relationship.
g) **Develop and validate compliance with the functions, duties and responsibilities assigned,** under the contract entered into with DEI, as well as for the exchange of information that may take place under said link or by legal provision, whether internal or with authorities.

8.5. Purposes for social management

a) **Inclusion and support:** include the holders in cultural, social, academic, educational, recreational, instructional, medical, psychological, legal support activities or any other type of activity carried out in the exercise of social functions or contributions to the community in general.
b) **Associative, cultural, recreational, sporting and social activities:** social assistance, various activities with the communities in the area of influence of the mining project.
c) **Education and culture:** scholarships and aid to students from communities in the area of influence of the mining project.
d) **Training:** for the communities in the area of influence of the mining project.
e) **Data update campaigns and information on changes in the processing of personal data:** updating and exchanging data with the entities that are part of the social projects carried out by the Company.

8.6. Purposes for visitors and facility control

a) **Ensuring the safety of people, property and facilities:** through the recording of information in the control of entry and exit of people.
b) **Referencing and scheduling:** private investigations and consultation of public and private data sources, for individuals who require access to the Company's facilities, in order to mitigate the potential risks they may generate.

The Company may process such information as the controller and processor of personal data and other data to which it is given access. Likewise, the holder undertakes to keep the personal data provided

updated, especially when he/she has exercised any of his/her rights of access, rectification, deletion or opposition before the Company.

9. FINAL PROVISION

9.1. Applicant databases

The personal data of applicants for employment with the Company, who are not selected for the position, are stored indefinitely in the Company's database, while the physical documents are eliminated, in order to maintain an easily accessible digital history and avoid duplication of processes in future calls for applications.

9.2. Databases of employees, former employees, and expatriates

Employees' personal data will be kept by the Company during and after the termination of the employment relationship. This is due to the fact that the Company must comply with legal obligations; therefore, the final disposition, understood as the suppression or elimination of the data, will be subject to what is indicated by Colombian labor legislation.

9.3. Shareholder databases

This is managed directly by the Headquarters, which will comply with its internal and legal policies.

9.4. National customer databases

The personal information of national clients will be kept by the Company during the business relationship between the parties and after its termination, until the fulfillment of the specific purpose of its authorization or for the time required by any legal obligation, this in order to comply with regulatory provisions.

9.5. International customer databases

This is managed directly by the Headquarters, which will comply with its internal and legal policies.

9.6. Databases of contractors and suppliers

The personal information of suppliers will be kept by the Company during the business relationship between the parties and after its termination until the fulfillment of the specific purpose of its authorization or for the time required by any legal obligation, this in order to comply with regulatory

provisions.

9.7. Third-party databases involved in activities in the areas of social management

Personal data collected within the framework of Corporate Social Responsibility programs will be kept for the duration of the benefit or participation of the holder in said activities, and for an additional period necessary for monitoring social impact and compliance with legal obligations or audits.

9.8. Databases for facility access and control

The images and recordings from the video surveillance system will be kept for a maximum term of ninety (90) days, after which the system will perform a deletion process by automatically overwriting the oldest information.

Visitor identification data, photographs and references will only be kept for the time necessary to comply with security and operational audit protocols. Once this purpose has been fulfilled, and if there is no legal obligation or requirement from an authority that demands its preservation, it will be safely disposed of or anonymized.

10. SENSITIVE DATA

The Company only obtains information classified as "sensitive" by regulations in the following events:

- The data holder has given explicit consent to such processing, except in cases where the granting of such consent is not required by law.
- The processing is necessary to safeguard the vital interests of the data holder, and the data holder is physically or legally incapable of giving consent. In these events, legal representatives must grant authorization.
- The processing is carried out in the course of legitimate activities and with due safeguards by a foundation, NGO, association or any other non-profit body whose purpose is political, philosophical, religious or trade union, provided that they relate exclusively to its members or to persons who maintain regular contact by reason of its purpose. In these events, the data may not be provided to third parties without the authorization of the owner.
- The processing refers to data that is necessary for the recognition, exercise or defense of a right in a judicial process.
- The treatment has a historical, statistical, or scientific purpose. In this event, measures must be taken to suppress the identity of the holders.

11. DATA ON MINORS

The processing of personal data of children and adolescents is prohibited as a general rule. However, and only in the cases provided for by law, the legal representative of the child or adolescent may authorize their treatment by the Company. The minor's legal representative must ensure compliance with the provisions of Article 12 of Decree 1377 of 2013.

Authorization is not required when the data is of a public nature, or in cases of medical or health emergency. Except for the exceptions provided for by the regulations, and within the legitimate purposes of the business and the attention to its requirements, in no case does the Company supply, distribute, market, share or exchange collected information; nor does it carry out activities in which the confidentiality and protection of minors is compromised. The data collected may only be shared with third parties in the event of prior, express and informed consent and authorization from the owner.

12. RIGHTS OF THE HOLDER

In accordance with the provisions of Article 8 of Law 1581 of 2012, the owner of personal data has the following rights:

a) To know, update and rectify your personal data before the Company, in its capacity as controller or processor.
b) Request proof of the authorization granted to the Company in its capacity as controller or processor.
c) To be informed by the Company upon request, regarding the use given to your personal data.
d) To file complaints with the Superintendency of Industry and Commerce (SIC) for violations of the provisions of Law 1581 of 2012, once the consultation or claim process before the data controller has been exhausted.
e) Revoke authorization and/or request the deletion of data when the processing does not respect the constitutional and legal principles, rights and guarantees.
f) Access his/her personal data that has been processed, free of charge.

13. OBLIGATIONS OF THE CONTROLLER OR PROCESSOR

The Company's duties as the data controller include:

a) To guarantee the holder at all times the full and effective exercise of the right of habeas data through the channels enabled for this purpose.
b) Request and keep, under the conditions provided in this document and in the Law, a copy of the respective authorization granted by the data holder during its processing.
c) Inform the data holder clearly and sufficiently about the purpose of collecting their personal

data and the rights they have by virtue of the authorization granted.

d) Keep the information under the necessary security conditions to prevent its alteration, loss, consultation, use or unauthorized or fraudulent access.
e) Ensure that the information provided to the data controller is truthful, complete, accurate, up-to-date, verifiable and understandable, in case the Company decides to appoint a data controller for the processing of personal data.
f) Update the information, promptly communicating to the data controller all changes regarding the data previously provided and take other necessary measures to ensure that the information provided to the controller remains up-to-date.
g) Correct the information when it is incorrect and communicate the relevant information to the data controller.
h) Provide the data processor, as applicable, only with data whose processing has been previously authorized in accordance with the provisions of the Law.
i) Require the data controller to respect, at all times, the security and privacy conditions of the data holder's information.
j) To process inquiries and complaints made by the owners of personal data, or their successors, in accordance with the terms set out in Law 1581 of 2012 and ratified in this Policy.
k) Inform the data holder, upon request, about the use given to their data.
l) Adopt specific procedures to ensure proper compliance with the Law and, in particular, to address inquiries and complaints.
m) Inform the data controller when certain information is under discussion by the data holder, once the complaint has been filed and the respective process has not yet been completed.
n) Inform the data protection authority (Superintendence of Industry and Commerce) when violations of security codes occur and there are risks in the management of the information of the holders.
o) Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce as the data protection authority.

The Company's duties, as the data controller, include:

a) To guarantee the holder, at all times, the full and effective exercise of the right of habeas data.
b) Keep the information under the necessary security conditions to prevent its alteration, loss, consultation, use or unauthorized or fraudulent access.
c) Update, rectify or delete data in a timely manner in accordance with Law 1581 of 2012 and other related and current regulations.
d) Update the information reported by the data controllers within five (5) business days from receipt.
e) To process inquiries and complaints made by the holders in accordance with the terms set out in this Policy.
f) Adopt an internal manual of policies and procedures to ensure proper compliance with the Law

and, in particular, to address inquiries and complaints from data holders.

g) Register the phrase “claim in process” in the databases in the manner regulated by the Law.
h) Insert the legend “information under judicial discussion” into the database once you are notified by the competent authority about judicial proceedings related to the quality of the personal data.
i) Refrain from circulating information that is being disputed by the owner and whose blocking has been ordered by the Superintendency of Industry and Commerce.
j) Allow access to information only to people who are authorized to access it.
k) Inform the data protection authority (Superintendence of Industry and Commerce) when violations of security codes occur and there are risks in the management of the information of the holders.
l) Verify that the data controller has the authorization to process the data holder's personal data.
m) Comply with the instructions and requirements issued by the Superintendency of Industry and Commerce as the data protection authority.

14. SUPPORT CHANNELS AND ACTIONS

The rights of consultation, correction, updating of data and claims may be exercised by the owner or whoever is legitimizing the cause, as follows:

Inquiries: The owner of the personal data may consult their information in the databases managed by the Company; the inquiry made by the owner will be addressed within a maximum of ten (10) business days from the date of receipt of the request. If it is not possible to address the inquiry within that timeframe, the interested party will be informed, stating the reasons for the delay and indicating the date on which their inquiry will be addressed, without exceeding five (5) business days following the expiration of the first timeframe.

For the purpose of exercising their right to consultation, the holders may send an email to the channels mentioned in section 2. SCOPE, these requirements are handled by the user support area in conjunction with those responsible for the databases.

Complaints: The data holder who believes that the information contained in any database managed by the Company should be corrected, updated or deleted, may file a complaint with the Company. This claim must be made through an application that includes the identification of the holder and a description of the facts that give rise to the claim, attaching any documents that he/she wishes to provide as evidence. If the claim is incomplete, the interested party will be informed within the following five (5) business days to correct the deficiencies. After two (2) months from the date of the request without the applicant providing the requested information, it will be understood that he/she has withdrawn the claim. Once the complete claim is received, within a period of no more than two (2) business days, a legend stating "claim in process" and the reason for it will be included in the

database. This legend must be maintained until the claim is decided. The maximum term to address the claim will be fifteen (15) business days counted from the day following the date of its receipt. When it is not possible to address the claim within that period, the interested party will be informed of the reasons for the delay and the date on which their claim will be addressed, which in no case will exceed eight (8) business days following the expiration of the first period.

15. NATIONAL DATABASE REGISTRY

In accordance with Article 25 of Law 1581 of 2012 and its regulatory decrees, the Company will register its databases together with this Personal Data Processing Policy, in the National Database Registry administered by the Superintendency of Industry and Commerce, in accordance with the procedure established for this purpose.

16. VALIDITY

The Company may modify this Personal Data Protection Policy at any time it deems necessary. In the event that any changes or modifications are made to this policy, the Company will communicate the changes to the holder. Therefore, we respectfully invite you to periodically review this policy on the Company's website: *https://drummondenergy.com/nuestra-compania/quienes-somos/nuestras-politicas/*, in order to stay informed about the security mechanisms implemented for the protection of personal information.

17. REFERENCE DOCUMENTS

This Policy is aligned with the following regulations applicable to the Company:

- Articles 15 and 20 of the Political Constitution (right to privacy and right to information, respectively)
- Law 1581 of 2012 - General framework for the protection of personal data in Colombia
- Decree 1377 of 2013 - Rules for the protection of personal data in Colombia