Information Protection Policy

Document Number: GRP-PO-IT-01 V.3.0

Effective Date: November 01, 2023

Policy Document Owner

_____

Policy Document Approver

_____

Política de protección de la información

Número de documento: GRP-PO-IT-01 V.3.0

Fecha de entrada en vigor: 1 de noviembre de 2023

Titular del documento normativo

_____

Autorizador de documento normativo

_____

Document Administration

Document Management

Document Owner (Name, Title)	David Rae, President and Chief Executive Officer
Document Administrator (Name, Title)	Matthieu Risgallah, Vice President, Innovation & Technology
Document Approver (Group or Name, Title)	Executive Committee
Adoption Date	May 20, 2018
Effective Date	November 1, 2023
Last Amended Date	August 1, 2023
Next Review Date	July 31, 2026

Version History

Version	Description of Version Changes
1	Initial May 20, 2018
2	Revised June 5, 2020
3	Revision of existing Data Protection Policy (renamed with this revision) to reflect and comply with the *Policy Document Management Standard*, broaden scope, clarify commitments, and align with the *Code of Business Conduct and Ethics.*

Administración de documentos

Gestión de documentos

Titular del documento (Nombre, cargo)	David Rae, presidente y director ejecutivo
Administrador de documentos (Nombre, cargo)	Matthieu Risgallah, vicepresidente de Innovación y Tecnología
Autorizador de documentos (Grupo o Nombre, cargo)	Comité ejecutivo
Fecha de adopción	20 de mayo de 2018
Fecha de entrada en vigor	1 de noviembre de 2023
Fecha de última modificación	1 de agosto de 2023
Fecha de próxima revisión	31 de julio de 2026

Historial de versiones

Versión	Descripción de los cambios de versión
1	Inicial, el 20 de mayo de 2018
2	Revisado, el 5 de junio de 2020
3	Revisión de la *Política de protección de datos existentes* (renombrada durante esta revisión) para reflejar y cumplir con la *Norma de gestión de documentos normativos*, ampliar el alcance, aclarar los compromisos y alinearse con el *Código de Conducta y Ética Empresarial.*

Related Policy Documents

Document Number	Document Title
GRP-PO-LEG-01 V.9.0	*Code of Business Conduct and Ethics*
GRP-PO-LEG-03 V.1.0	*Disclosure and Insider Trading Policy*
GRP-ST-IT-06 V.2.0	*Information Categorization Standard*
GRP-ST-IT-05 V.1.0	*Data Loss Prevention Standard*
GRP-ST-IT-04 V.1.0	*Data Retention, Sanitization and Destruction Standard*
GRP-ST-LEG-17 V.1.0	*Subsidiary Governance Standard*

Documentos normativos relacionados

Número de documento	Título del documento
GRP-PO-LEG-01 V.9.0	*Código de Conducta y Ética Empresarial*
GRP-PO-LEG-03 V.1.0	*Política de divulgación y uso de información privilegiada*
GRP-ST-IT-06 V.2.0	*Norma de categorización de la información*
GRP-ST-IT-05 V.1.0	*Norma de prevención de la pérdida de datos*
GRP-ST-IT-04 V.1.0	*Norma de conservación, depuración y destrucción de datos*
GRP-ST-LEG-17 V.1.0	*Norma de gobernanza de filiales*

Table of Contents

Índice

1. Defined Terms

The following terms and acronyms are integral to the understanding of this Policy and have the meanings assigned within this Section or as referenced herein:

Term	Definition
Board Member(s)	As a group or individually, any member of the DPM Board or any member of the board of directors of any DPM subsidiary or any individual delegated equivalent authority by the shareholder(s) of such entity.

1. Términos definidos

Los siguientes términos y acrónimos son esenciales para la comprensión de esta Política y tienen el significado que se les asigna en esta Sección o al que se hace referencia en ella:

Término	Definición
Miembro/s del Consejo	Como grupo o individualmente, cualquier miembro de la Junta Directiva de DPM o cualquier miembro de la Junta Directiva de cualquier subsidiaria de DPM o cualquier autoridad individual equivalente delegada por el accionista o accionistas de dicha entidad.

Business Function and Business Function Head	A team of Employees with a designated cost centre, or multiple cost centres, accountable for establishing and maintaining business systems, including through Policy Documents, internal controls, and applications; managing or supporting implementation; and providing ongoing support to other Employees and relevant Third Parties. The Business Function Head thereof is the individual accountable for the Business Function.	Función empresarial y jefe de funciones empresariales	Un equipo de empleados con un centro de costos designado, o varios centros de costos responsables de establecer y mantener los sistemas empresariales, incluso a través de documentos de políticas, controles internos y aplicaciones; de administrar o apoyar la implementación; y de proporcionar apoyo continuo a otros empleados y terceros relevantes. El jefe de funciones empresariales es la persona responsable de las funciones empresariales.
Business Unit and Business Unit Head	DPM and each of its Sites, individually. The Business Head thereof is the individual accountable for the Business Unit.		
Company or Group	DPM and all its directly and indirectly owned subsidiaries, collectively.	Unidad operacional y jefe de unidad operacional	DPM y cada uno de sus sitios, individualmente. El responsable de la unidad operacional de la misma es la persona responsable de la unidad operacional.
		Empresa o grupo	DPM y todas sus subsidiarias de propiedad directa e indirecta, colectivamente.

Company Information	Information, in any medium or format, that is processed by the Company for a specific business purpose determined by the Company. In the context of Company Information, the verb "to process" includes any activity that involves the use of Company Information (whether through manual or automated means) such as the collection, recording, storage, retrieval, use (i.e. organization, adaption, alteration, consultation, alignment, or combination), disclosure (i.e. transmission, dissemination, or otherwise making available), transfer to Third Parties, and destruction of information.	Información de la Compañía	Información, en cualquier medio o formato, que es procesada por la Compañía para un propósito comercial específico determinado por la Compañía. En el contexto de la Información de la Compañía, el verbo "procesar" incluye cualquier actividad que implique el uso de la Información de la Compañía (ya sea por medios manuales o automáticos), como la recopilación, el registro, el almacenamiento, la recuperación, el uso (es decir, la organización, la adaptación, la alteración , consulta, alineación o combinación), divulgación (es decir, transmisión, difusión o puesta a disposición de otro modo), transferencia a terceros y destrucción de información.
Confidential Information	All Company Information that is not generally known to the public.	Información confidencial	Toda la información de la Compañía que no es generalmente conocida por el público.
DPM	Dundee Precious Metals Inc. (the parent company incorporated in Canada) or the Company depending on context.		

Employee	An individual engaged by the Company on a full-time or part-time permanent, fixed term, or temporary basis, as well as a secondment employee, student, intern, or apprentice. For clarity, Employees also include Company Officers. For the definition of "Company Officer", refer to the *Subsidiary Governance Standard.*	DPM	Dundee Precious Metals Inc. (La compañía matriz constituida en Canadá) o tan sólo la Compañía, dependiendo del contexto.
Executive Committee	As a group, the President & Chief Executive Officer and all executive vice presidents and senior vice presidents of DPM.	Empleado	Una persona contratada por la Compañía a tiempo completo o parcial permanente, a plazo fijo o temporal, así como un empleado en comisión de servicio, estudiante, pasante o aprendiz. Para mayor claridad, el término "Empleados" también incluye a los directivos de la Compañía. Para la definición de "directivo de la Compañía", consulte *la Norma de Gobernanza de Filiales.*
Information Breach	The inadvertent or deliberate disclosure of Company Information to Employees, Third Parties, or external parties, who do not have a legitimate business purpose to access such Company Information, and/or the theft of, loss of, or unauthorized access to Company Information because of improper processing (including as a result of deliberate attempts by unauthorized external parties).	Comité ejecutivo	Como grupo, el Presidente y Director Ejecutivo y todos los vicepresidentes ejecutivos y vicepresidentes senior de DPM.
Information Owner	The Head of the Business Function in or from which the Company Information originates.	Violación de la información	La divulgación involuntaria o deliberada de la Información de la Compañía a empleados,

Information Subject	An identified or identifiable natural person to which Personal Information relates.		terceros o terceros externos que no tengan un propósito comercial legítimo para acceder a dicha información de la Compañía, y/o el robo, pérdida de, o acceso no autorizado a la información de la Compañía debido a un procesamiento inadecuado (incluso como resultado de intentos deliberados por parte de terceros no autorizados).
Material Information	Any information relating to the business and affairs of the Company, that results in, or would reasonably be expected to result in a significant change in the market price or value of the Company's securities. Also see Disclosure and Insider Trading Policy for a non-exhaustive list of examples of the types of events or information that may be material.		
Material Non-Public Information	Any Material Information which has not been generally disclosed by dissemination to the public through a news release.		
		Titular de la información	El jefe de la función empresarial en o desde la que se origina la información de la compañía.
		Asunto de la información	Una persona natural identificada o identificable a la que se refiere la información personal.
		Información relevante	Cualquier información relacionada con los negocios y asuntos de la Compañía, que resulte en, o se esperaría

Personal Information	Any information identifying an Information Subject, or information relating to an Information Subject that the Company can identify (directly or indirectly) from that data alone or in combination with other identifiers the Company possesses or can reasonably access. This includes an identifier such as a name, an identification number, location data, an online identifier or factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that Information Subject.		razonablemente que resulte en un cambio significativo en el precio de mercado o el valor de los activos de la Compañía. Consulte también la política de divulgación y uso de información privilegiada para obtener una lista no exhaustiva de ejemplos de los tipos de eventos o información que pueden ser relevantes.
		Información relevante no pública	Cualquier información relevante que no haya sido
Privacy	The protection of Personal Information processed by or on behalf of the Company.		divulgada de forma general mediante su difusión al público a través de un comunicado de prensa.

Privacy Laws	All laws and regulations pertaining to Personal Information privacy, that are applicable to the Company, including but not limited to the *Canadian Personal Information Protection and Electronic Documents Act* (PIPEDA) and the European Union *General Data Protection Regulation* (GDPR).	Información personal	Cualquier información que identifique a un información temática, o información relacionada a una información temática que la Compañía pueda identificar (directa o indirectamente) a partir de esos datos únicamente o en combinación con otros identificadores que la Compañía posea o a los que pueda acceder razonablemente. Esto incluye un identificador como un nombre, un número de identificación, datos de localización, un identificador en línea o factores específicos de la identidad física, fisiológica, genética, mental, económica, cultural o social de dicha información temática.
Site and Site Head	Each and any DPM operation together with directly supporting management service companies, as well as each and any advanced exploration property or development project. The Site Head is the individual accountable for the Site.		
		Privacidad	La protección de la información personal procesada por o en nombre de la Compañía.

Third Party	An individual, company, or other entity, that is interested in entering into or has an existing business relationship with the Company. Third Parties include, but are not limited to, suppliers, contractors, advisors, consultants, agents, brokers, lobbyists, donation and sponsorship beneficiaries, customers, and joint venture, merger, and acquisition partners.	Legislación sobre protección de datos	Todas las leyes y regulaciones relacionadas con la privacidad de la información personal, que son aplicables a la Compañía, incluyendo, pero no limitado a, la *Ley Canadiense de Protección de información personal y Documentos Electrónicos* (PIPEDA) y el *Reglamento General de Protección de Datos de la Unión Europea* (GDPR).
		Sitio y jefe del sitio	Todas y cada una de las operaciones de DPM junto con empresas de servicios de gestión de apoyo directo, así como todas y cada una de las propiedades de exploración avanzada o proyectos de desarrollo. El jefe del sitio es la persona responsable del sitio.

Terceros	Una persona, Compañía u otra entidad que esté interesada en entablar o tenga una relación comercial existente con la Compañía. Los terceros incluyen, pero no se limitan a, proveedores, contratistas, asesores, consultores, agentes, corredores, grupos de presión, beneficiarios de donaciones y patrocinios, clientes y socios de empresas conjuntas, fusiones y adquisiciones.

2. Purpose and Scope

The purpose of the *Information Protection Policy* (this Policy) is to facilitate the protection of Company Information in accordance with applicable legal requirements and Company internal commitments.

The Policy defines the Company's approach to protecting Company Information, including Personal Information and sets out the Company's information protection framework. This Policy is applicable across the Group to all Company Information. All Board Members, Employees and Third Parties who process Company Information are required to follow this Policy.

2. Propósito y alcance

El propósito de la *Política de Protección de la Información* (en adelante, esta Política) es facilitar la protección de la Información de la Compañía de acuerdo con los requisitos legales aplicables y los compromisos internos de la Compañía.

La Política define el enfoque de la Compañía para proteger la Información de la Compañía, incluida la información personal y establece el marco de protección de la información de la Compañía. Esta Política es aplicable en todo el Grupo a toda la Información de la Compañía. Todos los miembros de la junta directiva, empleados y terceros que procesan

3. Information Protection Principles

Company Information is an important asset, on which the Company relies to empower activities and decision making that help fulfil the Company's strategic objectives. It is a key resource for meeting regulatory requirements, achieving transparency, making informed decisions and staying competitive.

The Company is committed to protect the integrity, confidentiality, and availability of Company Information by various means including categorization, sensitivity labeling, technical safeguarding, and response strategies, which will be used during Information Breach or information systems failure. Information protection at the Company is based on risk-aware decision making, which ensures consideration of the full potential of the surrounding threats, the current level of protection and the costs that will be incurred in case adverse effects materialize.

All Company Information will be treated as Confidential Information. A non-exhaustive list of basic actions which Board Members, Employees and Third Parties can take to safeguard Confidential Information is provided in Appendix A – Guidelines for Safeguarding Confidential Information.

Material Non-Public Information is one of the subcategories of Confidential Information. As such, it is protected by this Policy and managed by the Disclosure and Insider Trading Policy, which governs confidentiality, disclosure and trading requirements and restrictions, applicable to Material Information.

información de la Compañía deben seguir esta política.

3. Principios de protección de la información

La información de la Compañía es un activo importante, en el que la Compañía se basa para potenciar las actividades y la toma de decisiones que ayudan a cumplir los objetivos estratégicos de la Compañía. Es un recurso clave para cumplir con los requisitos regulatorios, lograr transparencia, tomar decisiones informadas y mantenerse competitivo.

La Compañía se compromete a proteger la integridad, confidencialidad y disponibilidad de su información por varios medios, incluyendo la categorización, el etiquetado de confidencialidad, la salvaguarda técnica y las estrategias de respuesta que se utilizarán durante la violación de la información o el fallo de los sistemas de información. La protección de la información en la Compañía se basa en la toma de decisiones conscientes del riesgo, lo que garantiza la consideración de todo el potencial de las amenazas circundantes, el nivel actual de protección y los costos en los que se incurrirá en caso de que se materialicen efectos adversos.

Toda la información de la Compañía se tratará como información confidencial. Una lista no exhaustiva de las acciones básicas que los miembros de la junta directiva, los empleados y los terceros pueden tomar para salvaguardar la información confidencial se proporciona en el Apéndice A – Directrices para salvaguardar la información confidencial.

La información relevante no pública es una de las subcategorías de información confidencial. Como tal, está protegida por esta Política y

	administrada por la política de divulgación y uso de información privilegiada, que rige los requisitos y restricciones de confidencialidad, divulgación y comercio, aplicables a la información relevante.
## 4. Information Protection Framework The information protection framework is organized by pillar along the lines of information categorization, breach prevention, and retention, all of which apply to all categories of Company Information. Additionally, special considerations are given to Personal Information pursuant to the Personal Information Privacy pillar and the Privacy principles discussed below. To meet the requirements of the information protection framework, all Company Information is assigned an Information Owner.	## 4. Marco de protección de la información El marco de protección de la información está organizado por pilares en función de la categorización y conservación de la información y la prevención de violaciones, y dichos pilares se aplican a todas las categorías de la información de la Compañía. Además, se dan consideraciones especiales a la información personal de conformidad con los pilares de privacidad de la información personal y los principios de privacidad que se describen a continuación. Para cumplir con los requisitos del marco de protección de la información, toda la información de la Compañía se asigna a un titular de la información.
### 4.1 Information Categorization Information categorization involves the classification of Company Information based on disclosure requirements, sensitivity, impact in the event of Information Breach, and volume. Information categorization allows visibility over the business value of Company Information and helps reduce the negative impact of information loss by tailored application of relevant protection measures. The requirements for Company Information categorization are further specified in the Information Categorization Standard.	### 4.1 Categorización de la información La categorización de la información implica la clasificación de esta en la Compañía en función de los requisitos de divulgación, la confidencialidad, el impacto en caso de violación de la información, así como su volumen. La categorización de la información permite la visibilidad sobre el valor empresarial de la información de la Compañía y ayuda a reducir el impacto negativo de la pérdida de información mediante la aplicación personalizada de las medidas de protección pertinentes. Los requisitos para la categorización de la información de la Compañía se especifican en la Norma de categorización de la información.

4.2 Information Breach Prevention

Information Breach prevention involves manual and automated activities and controls, which are designed and implemented to prevent, reduce the likelihood of, or detect and address Information Breach while facilitating access and retrieval. Information Breach prevention rules will be designed and applied based on the Company Information category and in accordance with the principles of risk-aware information protection. Information Breach prevention requirements are further specified in the Data Loss Prevention Standard.

4.3 Information Retention

Information retention involves the storage, recovery, and disposal of Company Information to support information availability and disposal of information that is no longer needed. Information retention requirements are further specified in the Data Retention, Sanitization and Destruction Standard.

Requirements for backup and information disaster recovery are designed to meet the Company's business continuity objectives while minimizing the adverse effect on safety and avoiding operational downtime and failure to meet Company commitments.

To satisfy the need for timely destruction of Company Information, retention periods will be identified for all Company Information in all media and formats. Retention periods will be defined for each Business Unit based on prevailing regulatory, licensing and business requirements. Company Information will be retained for no longer than its predetermined retention period after which it will be destroyed, and relevant media sanitized, if applicable.

4.2 Prevención de la violación de la información

La prevención de la violación de la información implica actividades y controles manuales y automatizados, diseñados y aplicados para prevenir, reducir la probabilidad o detectar y abordar la violación de la información, facilitando al mismo tiempo el acceso y la recuperación. Las reglas de prevención de violación de la información se diseñarán y aplicarán en función de la categoría de información de la Compañía y de acuerdo con los principios de protección de la información consciente de riesgos. Los requisitos de prevención de violaciones de la información se especifican en la Norma de prevención de la pérdida de datos.

4.3 Conservación de la información

La conservación de la información implica el almacenamiento, la recuperación y la eliminación de la información de la empresa para respaldar su disponibilidad y la eliminación de la que ya no es necesaria. Los requisitos de conservación de la información se especifican además en la Norma de retención, depuración y destrucción de datos.

Los requisitos en materia de copias de seguridad y recuperación de la información en caso de catástrofe están diseñados para cumplir los objetivos de continuidad de la actividad de la Compañía, minimizando al mismo tiempo el efecto adverso sobre la seguridad y evitando el tiempo de inactividad operativa y el incumplimiento de los compromisos de la Compañía.

Para satisfacer la necesidad de eliminación oportuna de la información de la Compañía, se identificarán períodos de conservación para dicha información en todos los medios y formatos. Los períodos de conservación se

Personal Information will be stored for only as long as necessary to fulfil the purpose(s) for which it was collected and while stored, will be accessible by Information Subjects as explained below.

definirán para cada unidad operacional en función de los requisitos normativos, de licencias y empresariales vigentes. La información de la Compañía se conservará durante un período de retención no superior al predeterminado, después del cual se destruirá y se depurarán los medios relevantes, de ser el caso.

La información personal se almacenará solo durante el tiempo que sea necesario para cumplir con el fin o fines para los que se recopiló y, mientras se almacena, será accesible para el Sujeto de la Información, como se explica a continuación.

4.4 Personal Information Protection

Personal Information will be safeguarded from breach and retained as described above. In addition, the Company will process Personal Information fairly, lawfully, for specified purposes and in a transparent manner in relation to the Information Subject. In particular:

- Personal Information will be requested from the Information Subject together with a clearly identified purpose(s) for collection and use;
- Personal Information will be processed only on the basis of applicable legal grounds (i.e., the Information Subject has given their consent; the processing is necessary for the performance of a contract with the Information Subject; to meet the Company's legal compliance obligations; to protect the vital interests of the Information Subject or to pursue the legitimate interests of the Company);
- To the extent feasible, the Company will inform the Information Subject of the processing of their Personal Information;
- Personal Information will be processed only for the purpose(s) identified by the Company,

4.4 Protección de la información personal

La información personal se salvaguardará de la violación y se conservará como se describe anteriormente. Además, la Compañía procesará la información personal de manera justa, legal, para fines específicos y de manera transparente en relación con el Sujeto de la Información. En particular:

- Se solicitará información personal del Sujeto de la Información junto con propósitos claramente identificados para la recopilación y el uso;
- La información personal se procesará únicamente sobre la base de los causales de ley aplicables (es decir, el Sujeto de la Información ha dado su consentimiento; el procesamiento es necesario para la ejecución de un contrato con el Sujeto de la Información; para cumplir con las obligaciones legales de cumplimiento de la Compañía; para proteger los intereses vitales de dicho sujeto o para perseguir los intereses legítimos de la Compañía);

except with the consent of the Information Subject, or as required by law;
- Personal Information will be kept accurate, complete, and up-to-date and corrected or deleted when inaccurate;
- Information Subjects will be provided with access to the Company's procedures related to the management of Personal Information;
- Information Subjects will be informed of the existence, use, and disclosure of their Personal Information and will be given access to and the ability to correct that information; and
- Information Subjects will be provided with information on their rights when it comes to how the Company process their Personal Information.

5. Role Relationships, Authorities, and Accountabilities

To facilitate compliance with this Policy, certain roles are defined in Section 1: Defined Terms, and related relationships and accountabilities are prescribed herein as regards the owners and users of Company Information.

5.1 Business Unit Head

Business Unit Heads are accountable to ensure that processes and controls, designed in compliance with

- En la medida de lo posible, la Compañía informará al Sujeto de la Información sobre el procesamiento de su Información Personal;
- La información personal se procesará solo para los fines identificados por la Compañía, excepto con el consentimiento del Sujeto de la Información, o según lo requiera la ley;
- La información personal se mantendrá precisa, completa y actualizada, y se corregirá o eliminará cuando sea inexacta;
- Los Sujetos de la Información tendrán acceso a los procedimientos de la Compañía relacionados con la gestión de la Información Personal;
- Se informará a los Sujetos de la Información sobre la existencia, el uso y la divulgación de su información personal y se les dará acceso y la capacidad de corregir dicha información; y.
- Los interesados recibirán información sobre sus derechos en relación con el tratamiento de sus datos personales por parte de la Compañía.

5. Relaciones de funciones, autoridades y responsabilidades

Para facilitar el cumplimiento de esta Política, ciertas funciones se definen en la Sección 1: Los términos definidos y las relaciones y responsabilidades relacionadas se prescriben aquí en lo que respecta a los propietarios y usuarios de la Información de la Compañía.

5.1 Jefe de la unidad operacional

Los jefes de las unidades operacionales son responsables de garantizar que los procesos y

the requirements of the pillars of the information protection framework set out in this Policy, are implemented, and enforced in their respective Business Units. The Business Unit Head is accountable for the custody and protection of Company Information in physical format.	controles, diseñados de acuerdo con los requisitos de los pilares del marco de protección de la información establecidos en esta Política, se implementen y apliquen en sus respectivas unidades operacionales. El jefe de la unidad operacional es responsable de la custodia y protección de la información de la Compañía en formato físico.
### 5.2 Information Owner The Information Owner is accountable for the compliance with the requirements of this Policy, including but not limited to Information Owner oversight of the Employees within the respective Business Function and the Third Parties, dealing with the respective Business Function.	### 5.2 Titular de la información El Titular de la Información es responsable del cumplimiento de los requisitos de esta Política, incluyendo pero no limitado a la supervisión del Propietario de la Información de los empleados dentro de la Función de Negocio respectiva y de los Terceros, que se ocupan de la Función de Negocio respectiva.
## 6. Effective Date and Review of this Policy Board Members, Employees and Third Parties must comply with all requirements described within this Policy as of the Effective Date. This Policy will be reviewed every three years and updated as necessary.	## 6. Fecha de entrada en vigor y revisión de esta política Los miembros de la junta directiva, los empleados y los terceros deben cumplir con todos los requisitos descritos en esta política a partir de la fecha de entrada en vigor. Esta Política se revisará cada tres años y se actualizará, según sea necesario.

7. Compliance with this Policy Document

Failure to comply with this Policy may subject a Board Member, Employee or Third Party to corrective action by the Company as described in the *Code of Business Conduct and Ethics*.

8. Appendices

The following appendices are integral to the understanding of this Policy Document:

- Appendix A – Guidelines to Safeguard Confidential Information

Appendix A: Actions to Safeguard Confidential Information

The following is a non-exhaustive list of basic actions that can be taken to safeguard Confidential Information:

- Confidential Information should be discussed only in places where the discussion cannot be overheard.
- Documents or electronic files including Confidential Information should be read or viewed only in places where such documents or electronic files cannot be inadvertently viewed.
- Documents and electronic files containing Confidential Information should be kept in a safe place to which access is restricted.
- Transmission of Confidential Information by electronic means, including by email or through the internet, should be made only where it is reasonable to believe that the transmission can be made and received under secure conditions.
- Documents or electronic files containing Confidential Information should not be copied unless necessary.

7. Cumplimiento de este documento normativo

El incumplimiento de esta Política puede someter a un Miembro de la Junta Directiva, Empleado o Tercero a una medida correctiva por parte de la Compañía, como se describe en el Código de Conducta y Ética Empresarial.

8. Apéndices

Los siguientes apéndices son parte integral de la comprensión de este documento normativo:

- Apéndice A – Directrices para salvaguardar la información confidencial

Apéndice A: Acciones para salvaguardar la información confidencial

La siguiente es una lista no exhaustiva de las acciones básicas que se pueden tomar para proteger la información confidencial:

- La información confidencial debe discutirse solo en lugares donde la conversación no pueda ser escuchada.
- Los documentos o archivos electrónicos, incluida la información confidencial, deben leerse o verse solo en lugares donde dichos documentos o archivos electrónicos no se puedan ver accidentalmente.
- Los documentos y archivos electrónicos que contengan información confidencial deben guardarse en un lugar seguro al que se restrinja el acceso.
- La transmisión de Información Confidencial por medios electrónicos,

• Documents or electronic files containing Confidential Information should be promptly removed from meeting/conference rooms and work areas after meetings have concluded. • Documents or electronic files containing Confidential Information should not be discarded or left where others can retrieve them; extra copies of such documents or electronic files should be shredded or otherwise destroyed. Services provided by Third Parties engaged to process Company Information should be governed by formal confidentiality and data processing agreements.	incluso por correo electrónico o a través de Internet, debe realizarse solo cuando sea razonable creer que la transmisión puede realizarse y recibirse en condiciones seguras. • Los documentos o archivos electrónicos que contengan información confidencial no deben copiarse a menos que sea necesario. • Los documentos o archivos electrónicos que contengan información confidencial deben eliminarse inmediatamente de las salas de reuniones/conferencias y de las áreas de trabajo una vez concluidas las reuniones. • Los documentos o archivos electrónicos que contengan información confidencial no deben desecharse ni dejarse donde otros puedan recuperarlos; las copias adicionales de dichos documentos o archivos electrónicos deben triturarse o destruirse de otro modo. Los servicios prestados por terceros comprometidos con el procesamiento de la información de la Compañía deben regirse por acuerdos formales de confidencialidad y procesamiento de datos.