Одобрил: _____ **Approved by:**

проф. д-р инж. Илия Гърков / Hon. Prof. Iliya Garkov, MSc PhD

Старши вицепрезидент „Оперативни дейности в Европа“/ Senior Vice President, European Operations

Дата: _____ **Date:**

Information Protection Policy	*Политика за защита на информацията*
Document Number: GRP-PO-IT-01 V.3.0	Код на документа: GRP-PO-IT-01 V.3.0
Effective Date: November 1, 2023	В сила от: 01 ноември 2023 г.

Policy Document Owner: _____	Собственик: _____
Policy Document Approver: _____	Утвърдил: _____

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.*

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

Администриране на документа

Управление на документи

Собственик на документа (име и длъжност)	Дейвид Рей, Президент и Главен изпълнителен директор
Администратор на документа (име и длъжност)	Матийо Ризгала, Вицепрезидент “Иновации и Технологии”
Утвърдил (групов орган или име и длъжност)	Изпълнителен комитет
Приет на	20 май, 2018
В сила от	1 ноември, 2023
Дата на последното изменение на документа	1 август, 2023
Дата на следващия преглед на документа	31 юли, 2026

Предишни версии

Версия	Описание на промените във версиите
1	Първа версия: 20 май, 2018
2	Редактирана версия: 5 юни, 2020
3	Настоящият документ представлява редактирана версия на съществуващата Политика за защита на данните (с ново име в настоящата версия), целяща отразяване и съответствие със *Стандарт за управление на фирмените политики (документи)*, разширяване на обхвата, изясняване на ангажиментите и синхронизиране с *Правилника за бизнес етика и поведение.*

Свързани фирмени политики

Код на документа	Наименование
GRP-PO-LEG-01 V.9.0	Правилник за бизнес поведение и етика
GRP-PO-LEG-03 V.1.0	Политика за оповестяване на информация и търговия с ценни книжа от страна на лица, разполагащи с вътрешна информация
GRP-ST-IT-06 V.2.0	Стандарт за категоризиране на информацията

GRP-ST-IT-05 V.1.0	Data Loss Prevention Standard	GRP-ST-IT-05 V.1.0	Стандарт за предотвратяване загубата на данни
GRP-ST-IT-04 V.1.0	Data Retention, Sanitization and Destruction Standard	GRP-ST-IT-04 V.1.0	Стандарт за съхранение, санитизиране и унищожаване на данни
GRP-ST-LEG-17 V.1.0	Subsidiary Governance Standard	GRP-ST-LEG-17 V.1.0	Стандарт за управление на дъщерните дружества

Table of Contents

Съдържание

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:

1 Дефиниции на термини

Термините и съкращенията са важни за правилното разбиране на настоящата Политика. Кратките им дефиниции са дадени по-долу:

Term	Definition	Срок на договора	Дефиниция
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.	Член/-ове на Борда	Заедно или поотделно – всяко лице в състава на Съвета на директорите на ДПМ или на някое от дъщерните ѝ дружества, както и всяко лице, на което акционер(-и) на тези дружества са възложили еквивалентни правомощия.
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.	Бизнес функция и Ръководител на бизнес функция	Екип от работници/служители с отделен разходен център или с няколко разходни центрове, чиито отговорности включват изграждане и поддържане на бизнес системи, включително чрез фирмени политики, вътрешни мерки за контрол и различни приложения; управление и съдействие за внедряване; оказване на подкрепа на други работници/служители и трети страни. Отговорността за Бизнес функцията се носи от нейният Ръководител.
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.	Бизнес единица и ръководител на бизнес единица	ДПМ и всяко от дъщерните ѝ дружества поотделно. Отговорността за Бизнес единицата се носи от нейният Ръководител.
Company or Group	DPM and all its directly and indirectly owned subsidiaries, collectively.	Компания или Група	ДПМ и всички дъщерни дружества, чиито капитал компанията притежава пряко и непряко, взети заедно.

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.	Информация на Компанията	Информация, независимо от нейния формат или среда, която се обработва от Компанията с определена от нея конкретна бизнес цел. В контекста на фирмената информация глаголът „обработвам” включва дейност с фирмена информация (ръчна или автоматизирана) като събиране, записване, съхранение, извличане и използване (например за организационни цели, адаптиране, изменение, консултации, синхронизиране или комбинация от тези цели), оповестяване (като например излъчване, разпространение или предоставяне по друг начин), предаване на Трети страни и унищожаване на информацията.
Confidential Information	All Company Information that is not generally known to the public.	Конфиденциал на информация	Цялата информация на Компанията, която не е публично достъпна.
DPM	Dundee Precious Metals Inc. (the parent company incorporated in Canada) or the Company depending on context.	ДПМ	„Дънди Прешъс Металс“ Инк. (компанията-майка, учредена в Канада) или Компанията, в зависимост от контекста.
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.*	Работник/служител	Лице, нает от Компанията по трудово правоотношение на пълно или непълно работно време със срочен или безсрочен договор, включително и командировано на друго работно място или временно нает студент, стажант или практикант. За повече яснота, категорията работник/служител, включва и членовете на висшето ръководство/ длъжностните лица на Компанията. За целите на дефиницията “Длъжностно лице на Компанията”, прави препратка към *Стандарт за управление на дъщерните дружества.*
Executive Committee	As a group, the President & Chief Executive Officer and all executive vice presidents and senior vice presidents of DPM.	Изпълнителен комитет	Заедно - Президентът и Главният изпълнителен директор на ДПМ, както и всички Изпълнителни вицепрезиденти и Старши вицепрезиденти на компанията.

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).	Неоторизирано разкриване на информация	Непреднамерено или умишлено разкриване на информация за Компанията пред работници/служители, Трети страни или външни страни, които нямат основателни бизнес причини за достъп до такава информация, и/или кражба, загуба, или неоторизиран достъп до нея поради неправилна обработка, включително в резултат от нарушение на изисквания към сигурността (например в резултат от умишлени опити на неоторизирани външни лица).
Information Owner	The Head of the Business Function in or from which the Company Information originates.	Собственик на информацията	Ръководителят на Бизнес функция, в която или от която произлиза информация на Компанията.
Information Subject	An identified or identifiable natural person to which Personal Information relates.	Субект на информация	Идентифицирано или възможно за идентифициране физическо лице, за което се отнася определени лични данни.
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.	Съществена информация	Всяка информация, която се отнася за бизнеса и дейността на Компанията, чийто резултат с основание може да се очаква, че ще причини значителни промени в пазарната цена или стойността на ценните книжа на Компанията. Освен това, вижте *Политиката за оповестяване на информация и търговия с ценни книжа от страна на лица, разполагащи с вътрешна информация*, в която има списък с *Примери за информация, която може да е Съществена*.
Material Non-Public Information	Any Material Information which has not been generally disclosed by dissemination to the public through a news release.	Съществена непублична информация	Всяка съществена информация, която не е била оповестена чрез разпространение в публичното пространство чрез прессъобщение.

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.	Лични данни	Всяка информация, която идентифицира Субекта на информацията, или информация, свързана с този Субект, която Компанията може да идентифицира (директно или индиректно) от самите данни или в комбинация с други идентификатори, които Компанията притежава или до които може да има достъп. Това включва идентификатори като име, идентификационен номер, данни за местоположение, онлайн идентификатор и фактори, които конкретно се отнасят за физическата, физиологичната, генетична, психическа, икономическа, културна и социална идентичност на Субекта на информацията.
Privacy	The protection of Personal Information processed by or on behalf of the Company.	Неприкосновеност на информацията	Представлява защита на Личните данни, които се обработват от или от името на Компанията.
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).	Закони за неприкосновеност на личните данни	Всички закони и наредби, касаещи защита на личните данни, които Компанията трябва да спазва, включително, но не само, канадския *Закон за защита на личните данни и електронните документи* и *Общия регламент за защита на личните данни* (GDPR) на ЕС.
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.	Дружество и Ръководител на дружество	Всяко дружество на ДПМ заедно с дружествата, които пряко предоставят управленски услуги, както и дружествата в напреднал етап на реализация на проучвателни дейности или инвестиционни предложения. Ръководителят на дружество е лицето, което носи отговорността за него.

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.	Трета страна	Физическо или юридическо лице със стопанска или друга цел, което е в бизнес отношения или има интерес да установи такива отношения с Компанията. Категорията включва, но не се ограничава до доставчици, подизпълнители, съветници, консултанти, агенти, брокери, лобисти, бенефициенти на дарения и спонсорство, клиенти и партньори в съвместни предприятия, сливания и придобивания.

2 Purpose and Scope	2 Цел и обхват
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.	Целта на *Политиката за защита на информацията* (настоящата Политика) е да осигурява защита на информацията на Компанията съгласно приложимите законови изисквания и вътрешните ангажименти на Компанията.
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.	Целта на тази Политика е да определи подхода на Компанията към защитата на информацията на Компанията, включително на Личните данни, и да зададе рамката за защита на фирмената информация. Тази политика важи за цялата Група и цялата информация на Компанията. Всички членове на Борда, работници/служители и Трети страни, които обработват информация на Компанията са длъжни да спазват тази Политика.
3 Information Protection Principles	**3 Принципи на защита на информацията**
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.	Информацията на Компанията е важен актив, на който Компанията разчита за осигуряване на дейностите и взимане на решения, така че да се реализират стратегическите цели на Компанията. Информацията е ключов ресурс за спазване на регулаторни изисквания, за постигане на прозрачност, взимане на информирани решения и поддържане на конкурентоспособността.
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.	Компанията се ангажира да защитава интегритета, конфиденциалността и наличността на информацията си чрез различни средства, включително категоризиране, отбелязване на чувствителността на данните, технически защити и стратегии за реакция, които да се използват при Неоторизирано разкриване на информация или срив на информационните системи. Защитата на информацията в Компанията е базирана на ориентирано към риска взимане на решения, което осигурява разглеждане на пълния потенциал на заплахите, настоящото ниво на защита, както и разходите, които биха възникнали, ако се реализират такива заплахи със значителен негативен ефект.
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.	Цялата информация на Компанията се третира като Конфиденциална. В Приложение А – Насоки за защита на Конфиденциалната информация е даден неизчерпателен списък с основните дейности, които трябва да се предприемат от съответните членове на Борда, работници/служители и Трети страни за защита на Конфиденциалната информация

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.	Съществената непублична информация е една от подкатегориите Конфиденциална информация. В това си качество, тя е защитена от настоящата Политика и се управлява съгласно Политиката за оповестяване на информация и търговия с ценни книжа от страна на лица, разполагащи с вътрешна информация, която определя изискванията относно конфиденциалността, оповестяването, търговията с ценни книжа и съответните ограничения, които са приложими за Съществената информация.
## 4 Information Protection Framework	## 4 Рамка за защита на информацията
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.	Рамката за защита на информацията е организирана около следните няколко стълба - категоризиране на информацията, предотвратяване на неоторизиран достъп и съхранение, които важат за всички категории информация на Компанията. Освен това се отделя специално внимание на Личните данни съгласно изискванията и принципите за Неприкосновеност на личните данни, които са детайлизирани долу. С оглед на спазване на рамката за защита на информацията, Компанията е определила собственик на всяка фирмена информация.
### 4.1 Information Categorization	### 4.1 Категоризиране на информацията
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.*	Категоризирането на информацията включва класифициране съгласно изискванията за оповестяване, чувствителност в случай на Неоторизирано разкриване, и обем. Категоризирането на информацията визуализира бизнес стойността на информацията на Компанията и намалява негативното въздействие от загубата на информация чрез прецизно прилагане на мерки за защита. Изискванията за категоризиране на информацията са детайлизирани в *Стандарта за категоризиране на информацията.*
### 4.2 Information Breach Prevention	### 4.2 Предотвратяване на Неоторизирано разкриване на информация
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.*	Предотвратяването на Неоторизирано разкриване на информация представлява ръчни или автоматизирани дейности и контроли, чиято цел е да предотвратяват и намаляват вероятността от или да засичат и реагират на Неоторизирано разкриване на информация чрез осигуряване на достъп до информацията и нейното възстановяване. Правилата за предотвратяване на Неоторизирано разкриване са базирани и следва да бъдат прилагани въз основа на категорията на информацията и в съответствие с принципите на защита, основана на съобразените рискове. Изискванията за предотвратяване на Неоторизирано разкриване са детайлизирани в *Стандарт за предотвратяване на загуба на данни.*

4.3 Information Retention	4.3 Съхранение на информацията
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.*	Съхранението на информацията включва нейното запазване, извличане и унищожаване с цел да се осигури наличност на информацията, която е необходима и унищожаване на тази, която вече не е необходима. Изискванията към съхранение на информацията са детайлизирани в *Стандарт за съхранение, санитизиране и унищожаване на данни.*
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.	Изискванията за бекъп и възстановяване на информацията при бедствия и авари са дефинирани, така че да отговарят на изискванията за непрекъснатост на бизнеса, да минимизират негативните ефекти върху сигурността, да се избегнат престоите в производството и да се спазят ангажиментите на Компанията.
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.	С оглед на навременното унищожаване на информацията на Компанията, за всяка информация се определят периоди за съхранение, за съответните формати и среда на съхранение. Периодите за съхранение на данни се определят за всяка Бизнес единица съгласно нормативните, лицензионни и оперативни изисквания. Информацията на Компанията се съхранява не по дълго от указания период за съхранение, след което се унищожава и съответната среда се санитизира/почиства, ако това е необходимо.
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.	Личните данни се съхранява само за времето, което е необходимо за постигане на целта, за която се събират и съхраняват. Тази информация е достъпна за Субекта на информацията, както е обяснено долу.
4.4 Personal Information Protection	4.4 Защита на личните данни
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:	Личните данни се защитава от неоторизирано оповестяване и се съхраняват, както е описано по-горе. Освен това, Компанията обработва личните данни справедливо, законно, за конкретни цели и по прозрачен начин по отношение на Субекта на информацията. Конкретно:
• Personal Information will be requested from the Information Subject together with a clearly identified purpose(s) for collection and use;	• Личните данни се изискват от Субекта на информация, като се посочва ясна цел/цели за нейното събиране и ползване.
• 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);	• Личните данни се обработват само съгласно приложимите законови основания (т.е., с декларирано съгласие на Субекта на информацията; когато обработката е необходима за изпълнение на договор с този Субект; за да се спазят законодателни изисквания към Компанията; за защита на жизнените интереси на Субекта или за защита на законните интереси на Компанията);
• To the extent feasible, the Company will inform the Information Subject of the processing of their Personal Information;	• Доколкото е практически възможно, Компанията информира Субекта на информация за неговите лични данни;

• Personal Information will be processed only for the purpose(s) identified by the Company, except with the consent of the Information Subject, or as required by law;	• Личните данни се обработват само за целите, които са посочени от Компанията, освен със съгласие на Субекта на информацията, както се изисква от законодателството;
• Personal Information will be kept accurate, complete, and up-to-date and corrected or deleted when inaccurate;	• Личните данни се поддържат точни, пълни и актуални и се коригират или изтриват, когато са неточни;
• Information Subjects will be provided with access to the Company's procedures related to the management of Personal Information;	• Субектите на информация получават достъп до процедурите на Компанията, свързани с управлението на Личните данни
• 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	• Компанията информира Субектите на информация за съществуването, използването и оповестяването на техните Лични данни, и им дава достъп до тях и възможност да ги коригират; и
• Information Subjects will be provided with information on their rights when it comes to how the Company process their Personal Information.	• Компанията информира Субектите на информация за техните права по отношение на техните Лични данни, които Компанията обработва.
5 Role Relationships, Authorities, and Accountabilities	**5 Взаимодействия, правомощия и отговорности, свързани с ролите**
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.	Някои роли са дефинирани в Раздел 1, за да се осигури съответствие с настоящата Политика. Тук са дадени дефинирани термини, отговорности и отношения между собствениците и ползвателите на информация на Компанията.
5.1 Business Unit Head	5.1 Ръководител на бизнес единица
Business Unit Heads are accountable to ensure that processes and controls, designed in compliance with 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.	Ръководителите на бизнес единици носят отговорност за това процесите и контроли мерки в съответната Бизнес единица да са разработени в съответствие с изискванията на рамката за защита на информацията, определена в настоящата Политика. Освен това, Ръководителите носят отговорност и за внедряване и изпълнение на разработените процеси и контроли в съответните Бизнес единици. Ръководителят на Бизнес единицата носи отговорност за попечителството и защитата на информацията на Компанията във физически формат.
5.2 Information Owner	5.2 Собственик на информацията
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.	Собственикът на информацията носи отговорност за спазването на настоящата Политика, включително но не само за контрол върху работниците/служителите в съответната Бизнес функция и върху Трети страни, които имат отношения с тази Бизнес функцията.
6 Effective Date and Review of this Policy	**6 Дата на влизане в сила и прегледи на настоящия Политика**
Board Members, Employees and Third Parties must comply with all requirements described within this Policy as of the Effective Date.	Членовете на Борда, работниците/служители и Трети страни са длъжни да спазват всички изисквания, описани в настоящата Политика от датата на влизането ѝ в сила.

This Policy will be reviewed every three years and updated as necessary.	Настоящата Политика се преразглежда на всеки три години и при необходимост се актуализира.
## 7 Compliance with this Policy Document	## 7 Съответствие с настоящия документ
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*.	За неспазване на настоящата Политика може да бъдат наложени корективни мерки на член на Борда, работник/служител или Трета страна съгласно *Правилника за бизнес етика и поведение*.
## 8 Appendices	## 8 Приложения
The following appendices are integral to the understanding of this Policy Document:	Изброените долу приложения са важни за по-доброто разбиране на настоящата Политика:
• Appendix A – Guidelines to Safeguard Confidential Information	• Приложение А – Насоки за защита на Конфиденциалната информация

Appendix A: Guidelines to Safeguard Confidential Information	Приложение А: Насоки за защита на Конфиденциалната информация
The following is a non-exhaustive list of basic actions that can be taken to safeguard Confidential Information:	Долу е даден неизчерпателен списък с основните действия, които трябва да се предприемат за защита на Конфиденциалната информация:
• Confidential Information should be discussed only in places where the discussion cannot be overheard.	• Конфиденциална информация се обсъжда само на места, на които други лица не могат да чуят обсъждането.
• 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.	• Документите и електронните файлове, които включват Конфиденциална информация, се четат/ извеждат на екран само на места, където други лица не могат случайно да ги видят.
• Documents and electronic files containing Confidential Information should be kept in a safe place to which access is restricted.	• Документите и дигиталните копия (файлове) с Конфиденциална информация се държат на безопасно място с ограничен достъп.
• 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.	• Изпращането/ прехвърлянето на Конфиденциална информация по електронен път, включително по и-мейл и Интернет се прави само когато с основание може да се счита, че информацията ще бъде получена по безопасен начин.
• Documents or electronic files containing Confidential Information should not be copied unless necessary.	• Документите и дигиталните копия с Конфиденциална информация не трябва да се копират, освен когато това е наложително.
• Documents or electronic files containing Confidential Information should be promptly removed from meeting/conference rooms and work areas after meetings have concluded.	• Документите и дигиталните копия с Конфиденциална информация трябва своевременно да се отстраняват от зали за срещи и работни места след приключване на срещите.
• 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.	• Документите и дигиталните копия с Конфиденциална информация не се изхвърлят и не се оставят на места, на които някой може да ги намери и използва; допълнителните копия от такива документи и дигитални копия се шредират или се унищожават по друг начин.
Services provided by Third Parties engaged to process Company Information should be governed by formal confidentiality and data processing agreements.	Услугите, предоставени от Трети страни, които обработват информация на Компанията трябва да се управляват на базата на сключени договори за конфиденциалност на информацията и обработката на данни.