Information Protection Policy

Politika zaštite podataka

Document Number: GRP-PO-IT-01 V.3.0
Effective Date: November 01, 2023

Broj dokumenta: GRP-PO-IT-01 V.3.0
Datum stupanja na snagu: 1. novembar 2023.

Policy Document Owner

Vlasnik dokumenta

Policy Document Approver

Dokument odobrava

Document Administration / Administracija dokumenta

Document Management / Upravljanje dokumentom

Document Owner (Name, Title)	David Rae, President and Chief Executive Officer	**Vlasnik dokumenta (Ime, funkcija)**	David Rae, predsednik i generalni direktor
Document Administrator (Name, Title)	Matthieu Risgallah, Vice President, Innovation & Technology	**Administrator dokumenta (Ime, funkcija)**	Matthieu Risgallah, potpredsednik za inovacije i tehnologije
Document Approver (Group or Name, Title)	Executive Committee	**Dokument odobrava (Grupa ili Ime, funkcija)**	Izvršni odbor
Adoption Date	May 20, 2018	**Datum usvajanja**	20. maj 2018.
Effective Date	November 1, 2023	**Datum stupanja na snagu**	1. novembar 2023.
Last Amended Date	August 1, 2023	**Datum poslednje izmene**	1. avgust 2023.
Next Review Date	July 31, 2026	**Datum naredne revizije**	31. jul 2026.

Version History / Pregled izmena

Version	Description of Version Changes	Verzija	Opis izmene
1	Initial May 20, 2018	1	Prvo izdanje 20. maj 2018.
2	Revised June 5, 2020	2	Revidirano 5. juna 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.*	3	Revizija postojeće Politike zaštite podataka (preimenovana ovom revizijom) kako bi odražavala i bila usaglašena sa *Standardom upravljanja dokumentom politike,* proširen opseg, objasni obaveze i uskladi se sa *Kodeksom poslovnog ponašanja i poslovne etike*

Related Policy Documents / Povezani dokumenti politike

Document Number	Document Title	Broj dokumenta	Naziv dokumenta
GRP-PO-LEG-01 V.9.0	*Code of Business Conduct and Ethics*	*GRP-PO-LEG-01 V.9.0*	*Kodeks poslovnog ponašanja i poslovne etike*
GRP-PO-LEG-03 V.1.0	*Disclosure and Insider Trading Policy*	*GRP-PO-LEG-03 V.1.0*	*Politika obelodanjivanja i insajderske trgovine*

GRP-ST-IT-06 V.2.0	*Information Categorization Standard*	*GRP-ST-IT-06 V.2.0*	*Standard kategorizacije podataka*
GRP-ST-IT-05 V.1.0	*Data Loss Prevention Standard*	*GRP-ST-IT-05 V.1.0*	*Standard za sprečavanje gubitka podataka*
GRP-ST-IT-04 V.1.0	*Data Retention, Sanitization and Destruction Standard*	*GRP-ST-IT-04 V.1.0*	*Standard za čuvanje, sanitizaciju i uništavanja podataka*
GRP-ST-LEG-17 V.1.0	*Subsidiary Governance Standard*	*GRP-ST-LEG-17 V.1.0*	*Standard upravljanja podružnicama*

Table of Contents / Sadržaj

1. Defined Terms / Definicije pojmova

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:

Sledeći pojmovi i skraćenice su neophodni za razumevanje ove Politike i imaju značenje dodeljeno u okviru ovog dela ili kako je ovde navedeno:

Term	Definition	Pojam	Definicija
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.	Član(ovi) odbora	Bilo koji član Odbora DPM-a ili bilo koji član odbora direktora bilo koje Podružnice ili bilo koje lice na odgovarajući način ovlašćeno od strane akcionara takvog entiteta, posmatrani kao grupa ili pojedinačno.
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.	Poslovna funkcija i rukovodilac poslovne funkcije	Tim zaposlenih sa određenim troškovnim centrom ili više njih, koji su odgovorni za uspostavljanje i održavanje poslovnih sistema, kroz, između ostalog, Dokumente politike, interne kontrole i primene; upravljanje ili podržavanje implementacije; i pružanje kontinuirane podrške drugim zaposlenima i odgovarajućim trećim licima. Rukovodilac poslovne funkcije je lice odgovorno za poslovnu funkciju.
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.	Poslovna jedinica i rukovodilac poslovne jedinice	DPM i svaka od njegovih lokacija. Rukovodilac poslovne jedinice je lice odgovorno za poslovnu jedinicu.

Term	Definition	Pojam	Definicija
Company or Group	DPM and all its directly and indirectly owned subsidiaries, collectively.	Kompanija ili Grupa	DPM i sve njegove podružnice u direktnom i indirektnom vlasništvu, zajedno.
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.	Podaci o kompaniji	Podaci, u bilo kom mediju ili formatu, koje obrađuje Kompanija za specifične poslovne svrhe koje je Kompanija odredila. U kontekstu Podataka o kompaniji, glagol „obraditi" podrazumeva svaku aktivnost koja obuhvata korišćenje podataka o kompaniji (bilo putem manuelnih ili automatskih sredstava), kao što je prikupljanje, snimanje, skladištenje, preuzimanje, korišćenje (tj. organizacija, prilagođavanje, izmena , konsultovanje, usklađivanje ili kombinovanje), obelodanjivanje (tj. prenos, distribuiranje ili na drugi način stavljanje na raspolaganje), prenos trećim licima i uništavanje podataka.
Confidential Information	All Company Information that is not generally known to the public.	Poverljivi podaci	Svi podaci o kompaniji koji nisu opšte poznati u javnom domenu.
DPM	Dundee Precious Metals Inc. (the parent company incorporated in Canada) or the Company depending on context.	DPM	Dundee Precious Metals Inc. (matična kompanija sa sedištem u Kanadi) ili kompanija u zavisnosti od konteksta.
Employee	An individual engaged by the Company on a full-time or part-time permanent, fixed term, or	Zaposleni	Lice koje zapošljava Kompanija sa punim ili skraćenim radnim vremenom za stalno, na određeno

Term	Definition	Pojam	Definicija
	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.*		vreme ili na privremenoj osnovi, kao i privremeno premešteni zaposleni, student, lice na praksi ili pripravnik. Radi izbegavanja nedoumice, pod pojmom zaposleni takođe se podrazumevaju ovlašćena lica i rukovodioci Kompanije.
Executive Committee	As a group, the President & Chief Executive Officer and all executive vice presidents and senior vice presidents of DPM.	Izvršni odbor	Predsednik i generalni direktor i svi izvršni potpredsednici i viši potpredsednici DPM-a posmatrani kao grupa.
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).	Povreda privatnosti podataka	Nenamerno ili namerno obelodanjivanje podataka o kompaniji zaposlenima, trećim licima ili eksternim licima, koji nemaju legitiman poslovni razlog da pristupe takvim podacima o kompaniji, i/ili krađa, gubitak ili neovlašćeni pristup podacima o kompaniji usled nepravilne obrade (uključujući i kao rezultat namernih pokušaja neovlašćenih eksternih lica).
Information Owner	The Head of the Business Function in or from which the Company Information originates.	Vlasnik podataka	Rukovodilac poslovne funkcije u kojoj je nastao ili iz koje potiče podatak o kompaniji.
Information Subject	An identified or identifiable natural person to which Personal Information relates.	Nosilac podataka	Fizičko lice čiji je identitet utvrđen ili može da se utvrdi, a na koga se podaci o ličnosti odnose.
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	Značajni podaci	Svi podaci koji se odnose na poslovanje i poslove Kompanije, a koji dovode ili bi se razumno očekivalo da će dovesti do značajne promene

Term	Definition	Pojam	Definicija
	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.		tržišne cene ili vrednosti hartija od vrednosti Kompanije. Takođe pogledajte Politiku obelodanjivanja i insajderske trgovine za nepotpunu listu primera tipova događaja ili podataka koji mogu biti od značaja.
Material Non-Public Information	Any Material Information which has not been generally disclosed by dissemination to the public through a news release.	Značajni podaci koji nisu u javnom domenu	Svi značajni podaci koji nisu opšte obelodanjeni javnosti putem distribuiranja saopštenja za javnost.
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.	Podaci o ličnosti	Svaki podatak koji otkriva identitet nosioca podataka, ili podatak koji se odnosi na nosioca podataka čiji identitet Kompanija može da utvrdi (direktno ili indirektno) samo na osnovu tih podataka ili u kombinaciji sa drugim identifikatorima koje Kompanija poseduje ili kojima može opravdano da pristupi. Ovo obuhvata identifikatore kao što su ime, matični broj, podaci o lokaciji, onlajn identifikator ili faktori specifični za fizički, fiziološki, genetski, psihički, ekonomski, kulturni ili društveni identitet tog nosioca podataka.
Privacy	The protection of Personal Information processed by or on behalf of the Company.	Privatnost	Zaštita podataka o ličnosti koje obrađuje Kompanija ili se obrađuju u njeno ime.
Privacy Laws	All laws and regulations pertaining to Personal Information privacy, that are applicable to the Company, including but	Zakoni o zaštiti privatnosti	Svi zakoni i propisi koji se odnose na privatnost podataka o ličnosti, koji važe za Kompaniju, uključujući, između ostalog, *kanadski*

Term	Definition	Pojam	Definicija
	not limited to the *Canadian Personal Information Protection and Electronic Documents Act* (PIPEDA) and the European Union *General Data Protection Regulation* (GDPR).		*Zakon o zaštiti podataka o ličnosti i elektronskim dokumentima* (PIPEDA) i *Opštu uredbu Evropske unije o zaštiti podataka o ličnosti* (GDPR).
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.	Lokacija i Rukovodilac lokacije	Svaka aktivnost kompanije DPM zajedno sa kompanijama za pružanje usluga upravljanja kojima pruža direktnu podršku, kao i svaki posed za unapređeno istraživanje ili razvojni projekat. Rukovodilac lokacije je osoba koja je odgovorna za lokaciju.
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.	Treće lice	Lice, kompanija ili drugi subjekt, koji je zainteresovan za zasnivanje ili ima postojeći poslovni odnos sa Kompanijom. Treća lica uključuju, ali nisu ograničena na, dobavljače, izvođače, savetnike, konsultante, agente, brokere, lobiste, korisnike donacija i sponzorstava, klijente, kao i partnere u zajedničkim ulaganjima, spajanjima i pripajanjima.

2. Purpose and Scope / Svrha i područje primene

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.

Svrha *Politike zaštite podataka* (ova Politika) je da olakša zaštitu podataka o kompaniji u skladu sa važećim zakonskim zahtevima i internim obavezama Kompanije.

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.

Politika definiše pristup koji Kompanija ima u vezi sa zaštitom podataka o Kompaniji, uključujući podatke o ličnosti i utvrđuje okvir za zaštitu podataka Kompanije. Ova politika se primenjuje u celoj Grupi na sve podatke o Kompaniji. Svi članovi odbora, zaposleni i treća lica koji obrađuju podatke o Kompaniji dužni su da poštuju ovu Politiku.

3. Information Protection Principles / Principi zaštite podataka

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

Podaci o Kompaniji su važna imovina na koju se Kompanija oslanja da bi unapredila aktivnosti i donošenje odluka koje pomažu u ispunjavanju strateških ciljeva Kompanije. To je ključni resurs za ispunjavanje regulatornih zahteva, postizanje transparentnosti, donošenje informisanih odluka i održavanje konkurentnosti.

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.

Kompanija je posvećena zaštiti integriteta, poverljivosti i dostupnosti podataka o kompaniji na različite načine, uključujući kategorizaciju, označavanje osetljivih podataka, tehničku zaštitu i strategije odgovora, koje će se koristiti u slučaju povrede privatnosti podataka ili kvara informacionog sistema. Zaštita podataka u Kompaniji zasniva se na donošenju odluka uz postojanje svesti o riziku, što obezbeđuje sagledavanje punog potencijala rizika koji postoje u okruženju, postojećeg nivoa zaštite i troškova koji će nastati u slučaju nastanka štetnih posledica.

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

Svi podaci o Kompaniji se tretiraju kao poverljivi podaci. Nepotpuna lista osnovnih mera koje članovi Odbora direktora, zaposleni i treća lica mogu da preduzmu u cilju zaštite poverljivih

Confidential Information is provided in Appendix A – Guidelines for Safeguarding Confidential Information.

podataka data je u Prilogu A – Smernice za zaštitu poverljivih podataka.

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.

Značajni podaci koji nisu u javnom domenu su jedna od potkategorija poverljivih podataka. Kao takvi, zaštićeni su ovom Politikom i njima se upravlja na osnovu Politike obelodanivanja i insajderske trgovine, koja reguliše zahteve i ograničenja u vezi sa poverljivošću, obelodanjivanjem i trgovinom, a koji važe za značajne podatke.

4. Information Protection Framework / Okvir za zaštitu podataka

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.

Okvir za zaštitu podataka organizovan je po stubovima u skladu sa kategorizacijom podataka, prevencijom kršenja i zadržavanjem, što se sve odnosi na sve kategorije podataka o Kompaniji. Pored toga, posebna pažnja se posvećuje podacima o ličnosti u skladu sa stubom privatnosti ličnih podataka i principima privatnosti o kojima se govori u nastavku. Da bi se ispunili zahtevi okvira za zaštitu podataka, svim podacima o Kompaniji se dodeljuje Vlasnik podataka.

4.1 Information Categorization / Kategorizacija podataka

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.

Kategorizacija podataka podrazumeva klasifikaciju podataka o Kompaniji na osnovu zahteva za obelodanjivanjem, osetljivosti podataka, posledica u slučaju povrede privatnosti podataka i obima. Kategorizacija podataka omogućava uvid u poslovnu vrednost podataka o Kompaniji i pomaže u smanjenju negativnih posledica usled gubitka podataka prilagođenom primenom odgovarajućih mera zaštite. Zahtevi za kategorizaciju podataka o Kompaniji su navedeni dalje u tekstu u Standardu za kategorizaciju podataka.

4.2 Information Breach Prevention / Sprečavanje povrede privatnosti podataka

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.

Sprečavanje povrede privatnosti podataka podrazumeva manuelne i automatske aktivnosti i kontrole, koje su dizajnirane i implementirane da spreče, smanje verovatnoću ili otkriju i rešavaju pitanje povrede privatnosti podataka, a istovremeno olakšavaju pristup i preuzimanje podataka. Pravila za sprečavanje povrede privatnosti podataka izrađuju se i primenjuju na osnovu kategorije podataka o Kompaniji i u skladu sa principima zaštite podataka uz svest o riziku. Zahtevi za sprečavanje povrede privatnosti podataka su navedeni dalje u tekstu u Standardu za sprečavanje gubitka podataka.

4.3 Information Retention / Čuvanje podataka

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.

Čuvanje podataka podrazumeva skladištenje, spašavanje i odlaganje podataka o Kompaniji kako bi se podržala dostupnost informacija i odlaganje podataka koji više nisu potrebni. Zahtevi za čuvanje podataka su navedeni dalje u tekstu u Standardu za čuvanje, sanitizaciju i uništavanje podataka.

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.

Zahtevi za rezervne kopije i spašavanje podataka u slučaju katastrofe su izrađeni da ispune ciljeve Kompanije u pogledu kontinuiteta poslovanja, istovremeno minimizirajući negativne posledice na bezbednost i izbegavajući zastoje u radu i neispunjavanje obaveza Kompanije.

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.
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.

Da bi se zadovoljila potreba za blagovremenim uništavanjem podataka o Kompaniji, periodi čuvanja se definišu za sve podatke o Kompaniji u svim medijima i formatima. Period čuvanja se definiše za svaku poslovnu jedinicu na osnovu preovlađujućih regulatornih, licencnih i poslovnih zahteva. Podaci o Kompaniji se čuvaju ne duže od prethodno određenog perioda čuvanja nakon čega se uništavaju, a odgovarajući mediji se podvrgavaju sanitizaciji, ako je primenljivo.
Lični podaci se čuvaju samo onoliko dugo koliko je potrebno da se ispuni svrha(e) za koju su prikupljeni i dok se čuvaju, dostupni su nosiocima podataka kao što je objašnjeno u nastavku.

4.4 Personal Information Protection / Zaštita podataka o ličnosti

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, 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.

Podaci o ličnosti su zaštićeni od povreda i čuvaju se na gore opisan način. Pored toga, Kompanija obrađuje podatke o ličnosti na pravičan i zakonit način, u određene svrhe i transparentno u odnosu na nosioca podataka. Naročito:

- Podaci o ličnosti se traže od nosioca podataka zajedno sa jasno defnisanom(im) svrhom(ama) prikupljanja i korišćenja;
- Podaci o ličnosti se obrađuju samo na osnovu važećih zakonskih osnova (tj. nosilac podataka je dao svoju saglasnost; obrada je neophodna za izvršenje ugovora sa nosiocem podataka; da bi se ispunile obaveze Kompanije u pogledu usaglašenosti sa zakonima; da bi se zaštitili vitalni interesi nosioca podataka ili ostvarili legitimni interesi Kompanije);
- U meri u kojoj je to izvodljivo, Kompanija obaveštava nosioca podataka o obradi njegovih ličnih podataka;
- Podaci o ličnosti se obrađuju samo u svrhu(e) koju je definisala Kompanija, osim uz saglasnost nosioca podataka, ili u skladu sa zakonom;
- Podaci o ličnosti treba da budu uvek tačni, potpuni i ažurirani i ispravljeni ili obrisani kada su netačni;
- Nosiocima podataka je omogućen pristup procedurama Kompanije u vezi sa upravljanjem podacima o ličnosti;
- Nosioci podataka su obavešteni o postojanju, korišćenju i obelodanjivanju njihovih ličnih podataka i dozvoljen im je pristup i data mogućnost da te podatke isprave; i

Nosiocima podataka se pružaju informacije o njihovim pravima kada je u pitanju način na koji Kompanija obrađuje njihove podatke o ličnosti.

5. Role Relationships, Authorities, and Accountabilities / Odnosi, ovlašćenja i odgovornosti pozicija

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.

Da bi se olakšala usklađenost sa ovom Politikom, određene pozicije su definisane u Odeljku 1: Definicije pojmova, a povezani odnosi i odgovornosti su ovde propisani u vezi sa vlasnicima i korisnicima podataka o Kompaniji.

5.1 Business Unit Head / Rukovodilac poslovne jedinice

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.

Rukovodioci poslovnih jedinica su odgovorni da obezbede da se procesi i kontrole, kreirani u skladu sa zahtevima stubova okvira za zaštitu podataka navedenih u ovoj Politici, sprovode i izvršavaju u njihovim poslovnim jedinicama. Rukovodilac poslovne jedinice je odgovoran za čuvanje i zaštitu podataka o Kompaniji u fizičkom formatu.

5.2 Information Owner / Vlasnik podataka

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.

Vlasnik podataka je odgovoran za usklađenost sa zahtevima ove Politike, uključujući, ali ne ograničavajući se na, nadzor vlasnika podataka nad zaposlenima u okviru odgovarajuće poslovne funkcije i trećim licima koje se bave odgovarajućom poslovnom funkcijom.

6. Effective Date and Review of this Policy / Datum stupanja na snagu i revizija ove politike

Board Members, Employees and Third Parties must comply with all requirements described within this Policy as of the Effective Date.

Članovi Odbora, zaposleni i treća lica moraju da poštuju sve zahteve opisane u ovoj Politici od datuma stupanja na snagu.

This Policy will be reviewed every three years and updated as necessary.

Ova Politika mora da se revidira svake tri godine i da se po potrebi ažurira.

7. Compliance with this Policy Document / Postupanje u skladu sa ovim dokumentom politike

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*.

Nepostupanje u skladu sa ovom Politikom može podrazumevati primenu korektivnih mera Kompanije protiv člana Odbora, zaposlenog ili trećeg lica, kako je opisano u *Kodeksu poslovnog ponašanja i poslovne etike*

8. Appendices / Prilozi

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

- Appendix A – Guidelines to Safeguard Confidential Information

Sledeći prilozi su neophodni za razumevanje ovog dokumenta Politike:

- Prilog A – Smernice za čuvanje poverljivih podataka

Appendix A: Actions to Safeguard Confidential Information / Prilog A: Mere za čuvanje poverljivih podataka

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.
- 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.

U nastavku je nepotpuna lista osnovnih mera koje se mogu preduzeti da bi se zaštitili poverljivi podaci:

- Poverljivi podaci treba da budu predmet razgovora samo na mestima gde takav razgovor ne mogu čuti druga lica.
- Dokumenti ili elektronske datoteke koji sadrže poverljive podatke treba da se čitaju ili pregledaju samo na mestima gde takvi dokumenti ili elektronske datoteke ne mogu da budu izloženi slučajnim pogledima.
- Dokumenti i elektronske datoteke koji sadrže poverljive podatke čuvaju se na bezbednom mestu sa ograničenim pristupom.
- Prenos poverljivih podataka elektronskim putem, uključujući e-poštu ili putem interneta, vrši se samo u slučajevima kada se opravdano veruje da prenos može da se izvrši i primi pod bezbednim uslovima.
- Dokumenti ili elektronske datoteke koji sadrže poverljive podatke ne smeju da se kopiraju osim ako je neophodno.
- Dokumenti ili elektronske datoteke koji sadrže poverljive podatke moraju odmah da se uklone iz sala za sastanke/konferencijskih sala i radnih prostorija nakon završetka sastanaka.
- Dokumenti ili elektronske datoteke koji sadrže poverljive podatke ne smeju da se odbace ili ostave na mestima gde druga lica mogu da ih pronađu; dodatne kopije takvih dokumenata ili elektronskih datoteka treba da budu uništene u mašini za uništavanje dokumenata (šreder) ili na drugi način.

Usluge koje pružaju treća lica angažovana za obradu podataka o Kompaniji treba da budu regulisane formalnim ugovorima o poverljivosti i obradi podataka.