# *Information Protection Policy*

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

Effective Date: November 01, 2023

Policy Document Owner

DocuSigned by:
3BE3B4987360496...

Policy Document Approver

DocuSigned by:
3BE3B4987360496...

# 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* |
| *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* |

# Table of Contents

Document Administration ..... 2
Document Management ..... 2
Version History ..... 2
Related Policy Documents ..... 2
1. Defined Terms ..... 4
2. Purpose and Scope ..... 6
3. Information Protection Principles ..... 6
4. Information Protection Framework ..... 6
4.1 Information Categorization ..... 6
4.2 Information Breach Prevention ..... 7
4.3 Information Retention ..... 7
4.4 Personal Information Protection ..... 7
5. Role Relationships, Authorities, and Accountabilities ..... 8
5.1 Business Unit Head ..... 8
5.2 Information Owner ..... 8
6. Effective Date and Review of this Policy ..... 8
7. Compliance with this Policy Document ..... 9
8. Appendices ..... 9
Appendix A: Actions to Safeguard Confidential Information ..... 10

## 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. |
| 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. |
| 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. |
| 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. |
| Confidential Information | All Company Information that is not generally known to the public. |
| 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.* |
| Executive Committee | As a group, the President & Chief Executive Officer and all executive vice presidents and senior vice presidents of DPM. |
| 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). |

| Term | Definition |
|---|---|
| Information Owner | The Head of the Business Function in or from which the Company Information originates. |
| Information Subject | An identified or identifiable natural person to which Personal Information relates. |
| 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. |
| 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. |
| Privacy | The protection of Personal Information processed by or on behalf of the Company. |
| 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). |
| 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. |
| 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. |

## 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.

## 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.

## 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.

### 4.1 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.

## 4.2 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.

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.

## 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, 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 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.

## 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.

# 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.

## 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.
- 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.