NORTHAM PLATINUM HOLDINGS LIMITED	**DATA PROTECTION COMPLIANCE POLICY**
Title: Data Protection Compliance Policy	**Document No.1**
Effective Date: Exco 28 May 2021	**Next review date: May 2024**
	Approved by: **Chairman of Exco**

1. DEFINITIONS AND INTERPRETATION

"audit and risk committee"	A sub-committee of the board tasked with assisting the board with audit and risk related matters.
"board"	The board of directors of Northam.
"CFO"	The Chief Financial Officer of Northam.
"compliance officer" or "CO" or "information officer"	An employee whose responsibilities include ensuring the group complies with its legal, internal and external regulatory obligations and procedures. All heads of department at Northam ("**HOD's**") are compliance officers, as they are responsible for their respective departments or divisions pertaining to internal policy and external regulatory requirements. The HOD's report any known non-compliances to the CFO through the risk management reports. The risk management reports are submitted to the audit and risk committee and board members for consideration at their respective meetings.
"consent"	Any voluntary, specific and informed expression of will in terms of which permission is given for the processing of personal information.
"CPI"	Children's Personal Information.
"Data Protection Legislation"	means any data protection or data privacy laws applicable to Northam, as such laws are amended from time to time, including but not limited to POPIA, the Electronic Communications and Transactions Act 26 of 2005, the Promotion of Access to Information Act, 2 of 2000, the Consumer Protection Act 68 of 2008;
"data subject"	means the person to whom the personal information relates
"employee"	Any permanent, non-permanent employee / contracting employee, turn key staff or entity working within Northam.
"Exco"	The executive committee of the company.
"Northam" or the "company"	Northam Platinum Holdings Limited and all its subsidiaries, joint arrangements and associates.
"Northam Employee" or "Northam Employees" or "You"	means Northam's directors, employees, contractors, agents and partners involved in the Processing of Personal Information and similar activities
"PAIA"	The Promotion of Access to Information Act 2 of 2008.
''person''	A natural person or a juristic person.

“personal information”	Personal information as defined in POPIA and includes any information relating to an identifiable, living, natural person, and where it is applicable, an identifiable, existing juristic person, including, but not limited to - • race, gender, sex, pregnancy, marital status, nationality, ethnicity or social origin, colour, sexual orientation, age, physical or mental health and well-being; • belief, religion, conscience, culture, language and birth, education, medical information, financial information, criminal or employment history; • an identifying number or symbol; • disability, personal opinions, blood type, biometric information; • views or preferences of a person, correspondence of private or confidential nature, views or opinions of another person; • name of a person if it appears with other personal information; • consumer or purchasing pattern; and • e-mail address and physical address, location information or online identifier and telephone number.
“POPIA”	The Protection of Personal Information Act 4 of 2013.
“privacy manager”	A person appointed as a Northam's privacy manager, being a person responsible for managing POPIA awareness, compliance and information requests within Northam.
‘‘processing’’ / “processed”	As defined in POPIA and includes any operation or activity or any set of operations, whether or not by automatic means, concerning personal information, including: • collection, receipt, recording, organisation, collation and storage; • updating or modification, retrieval and alteration; • consultation; • use, dissemination or distribution; and/or • merging, restriction, destruction or deletion.
‘‘record’’	As defined in POPIA and includes any recorded personal information: • regardless of form or medium, including any of the following: - writing on any material;

	- information produced, recorded or stored by means of any tape-recorder, computer equipment, whether hardware or software or both, or other device, and any material subsequently derived from information so produced, recorded or stored; - label, marking or other writing that identifies or describes anything of which it forms part, or to which it is attached by any means; - book, map, plan, graph or drawing; and - photograph, film, negative, tape or other device in which one or more visual images are embodied so as to be capable, with or without the aid of some other equipment, of being reproduced; • in the possession or under the control of a responsible party; • whether or not it was created by a responsible party; and • regardless of when it came into existence.
‘‘regulator’’	The information regulator established in terms of section 39 of the POPIA.
“responsible party”	As defined in POPIA.
“special personal information”	As defined in POPIA and includes special personal information relating to a person’s: • religious or philosophical beliefs; • race or ethnic origin; • trade union membership; • political persuasion; • health or sex life; • biometric information; or • criminal behaviour.

1 INTRODUCTION

1.1 Northam and its affiliates have a significant network of offices and a significant number of employees.

1.2 During the course and scope of its business activities, Northam obtains personal information from a variety of sources including customers, employees, suppliers and various third parties who may engage with Northam, from time to time.

1.3 POPIA governs the processing of personal information, including but not limited to special personal information and imposes certain obligations on Northam in relation to this information and the manner in which it is processed.

1.4 Northam is required to comply with applicable Data Protection Legislation, and Northam can only achieve this if You, as a Northam Employee, comply with the provisions of this Policy.

1.5 Accordingly, Northam wishes to govern, regulate and administer the processing of personal information through this policy in order to comply with the provisions of POPIA.

2 PURPOSE AND OBJECTIVES

2.1 The purpose of this Policy is to assist Northam's Employees to comply with Data Protection Legislation whenever they act on behalf of Northam.

2.2 It is the intent of Northam to adopt this policy in order to:

2.2.1 ensure that personal information and special personal information is treated with the highest degree of security and confidentiality;

2.2.2 reduce the possibility of information loss incidents;

2.2.3 regulate and control the manner in which personal information is processed by all data processors on behalf of Northam;

2.2.4 prescribe rules for processing personal information and special personal information;

2.2.5 protect information in all formats, throughout its lifecycle, as it is a valuable asset;

2.2.6 ensure that Northam, being the responsible party, determines the purpose of and means by which personal information is processed, and complies with this policy for lawful processing of personal information and special personal information; and

2.2.7 enable the monitoring of user activities for compliance with privacy legislation ensuring that personal information is processed in line with data privacy laws and regulations, namely POPIA and PAIA.

3 SCOPE, APPLICATION AND POLICY STATEMENT

3.1 This policy applies to all Northam Employees regardless of seniority and reflects Northam's minimum data privacy requirements. This policy should be read in conjunction with POPIA.

3.2 Northam, its subsidiaries, employees and other officials, agents, and representatives of Northam shall be bound by, observe and implement this policy at all times.

3.3 In the event of any conflict between this policy and any governance document providing for the processing of personal information in relation to Northam, this policy will prevail. Where a business unit requires stricter requirements, those requirements will apply.

3.4 Every Northam Employee will be required to conduct themselves in accordance with this Policy. Accordingly, where Northam is required to do something under this Policy, You must also act in accordance with that requirement. Similarly, where You are required to do something under this Policy, that is because Northam also required to act in a certain manner in terms of applicable Data Protection Legislation.

3.5 Northam processes personal information of its employees (and contractors) in accordance with the Employee Privacy Policy. This policy is maintained by the company. Northam process of the personal information of third parties, including its customers and suppliers, in accordance with its External Privacy Policy, a copy of which is available on the company website.

4 HOW TO USE THIS POLICY

4.1 Northam's Employees are required to:

4.1.1 read through this Policy;

4.1.2 ensure that they understand this Policy; and

4.1.3 take measures to ensure that they adhere to this Policy.

4.2 You must learn: (i) what actions are specifically required or prohibited by Data Protection Legislation; and (ii) to recognise areas where Data Protection Legislation problems may arise and seek guidance from the relevant manager, who may in turn refer matters to the Information Officer.

4.3 This Policy is not a complete statement of the relevant Data Protection Legislation principles. Accordingly, if an Employee has any doubt as to the legality of any course of action or business practice, the relevant manager must immediately be consulted, who may thereafter refer the matter to the Information Officer.

4.4 Any contravention of Data Protection Legislation may have a serious and adverse effect on Northam as well as the individual concerned, including significant fines as well as possible criminal and civil law sanctions. No Employee may act contrary to the provisions of the relevant Data Protection Legislation or authorise others to act in contravention thereof.

5 REVISIONS TO THIS POLICY

The Policy (as well as the Guidelines attached to the Policy) are subject to continuous review by Northam. In the event that there are material changes to Data Protection Legislation or other applicable laws or if Northam wishes to enhance any aspect of this Policy, amendments will be made as necessary.

6 BACKGROUND TO POPIA

6.1 POPIA aims to give effect to the constitutional right to privacy by safeguarding personal information when processed by a responsible party, subject to justifiable limitations. POPIA sets forth various provisions which, *inter alia*, regulate the manner in which personal information may be processed.

6.2 POPIA applies to the processing of personal information (i) entered in a record by or for a responsible party by making use of automated or non-automated means or (ii)where the responsible party is either domiciled in South Africa or not domiciled in South Africa, but makes use of the automated or non-automated means in South Africa, unless those means are used only to forward personal information within South Africa.

7 DATA PROCESSING PRINCIPLES

7.1 POPIA prescribes certain conditions for the lawful processing of personal information which are summarised as follows:

7.1.1 *Condition 1 - Accountability*: Northam must ensure that measures are taken which give effect to the conditions set out in POPIA.

7.1.2 *Condition 2 - Processing Limitation*: Personal information must be processed lawfully and in a reasonable manner that does not infringe the privacy of a data subject. Personal information may only be processed if, given the purpose for which it is processed, the processing is adequate, relevant and not excessive. Further, subject to certain exceptions, personal information may only be processed with the consent of a data subject and must be collected directly from a data subject.

7.1.3 *Condition 3 - Purpose Specification:* Personal information must be collected for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party. Personal information may not be kept for longer than is necessary for achieving the purpose for which it is collected or subsequently processed, unless required for historical, statistical and research purposes and only if the responsible party has established appropriate safeguards against the records being used for any other purpose.

7.1.4 *Condition 4 - Further Process Limitation:* Personal information must not be further processed in a way incompatible with a purpose for which it has been collected in the first instance, unless, subject to certain exceptions, consent is obtained from the data subject for such further processing or the information is used for historical, statistical or research purposes and the responsible party ensures that the further processing is carried out solely for such purposes and will not be published in an identifiable form.

7.1.5 *Condition 5 - Information Quality:* Northam must take reasonable practical steps to ensure that the personal information is complete, accurate, not misleading and updated where necessary, having regard to the purpose for which the personal information is collected or further processed.

7.1.6 *Condition 6 - Openness:* Northam must maintain the documentation for all processing operations in accordance with its responsibility in terms of sections 14 and 51 of PAIA. Further, if personal information is collected, the responsible party must take reasonable

practicable steps to ensure that the data subject is, *inter alia*, aware of the information being collected and the purpose for such collection.

7.1.7 *Condition 7 - Security Safeguards*: Appropriate technical and organisational measures must be taken to secure the integrity and confidentiality of personal information by safeguarding against the risk of loss or damage or unauthorised destruction of personal information and against unlawful access to, or processing of, personal information.

7.1.8 *Condition 8 – Data Subject Participation:* A data subject has the right to request confirmation from the responsible party as to whether or not the responsible party holds personal information on the data subject and request record of the personal information (including the identity of the third parties who have or have had access to the information). A data subject may also request a responsible party to correct or delete personal information about the data subject in its possession that is, *inter alia*, inaccurate, irrelevant, incomplete or misleading or destroy or delete a record of personal information about the data subject.

7.2 You are required to process personal information in accordance with these conditions.

8 YOUR OBLIGATIONS WHEN PROCESSING PERSONAL INFORMATION

The following principles must be adhered to and guide the implementation of the minimum requirements as set out in this policy.

8.1 Processing Limitation

8.1.1 Data Protection Legislation restricts the manner in which a person may process personal information. Processing must be adequate, relevant and not excessive given the purpose for which the personal information is processed. These restrictions are not intended to prevent processing, but to ensure that Northam processes personal information lawfully and in a reasonable manner that does not infringe the privacy of the data subject.

8.1.2 Data Protection Legislation allows processing under specific circumstances, some of which are set out below:

8.1.2.1 the data subject consents to the processing;

8.1.2.2 Processing is necessary to carry out actions for the conclusion or performance of a contract to which the data subject is party;

8.1.2.3 Processing complies with an obligation imposed by law on the responsible party;

8.1.2.4 Processing protects a legitimate interest of the data subject;

8.1.2.5 Processing is necessary for the proper performance of a public law duty by a public body; and

8.1.2.6 Processing is necessary for pursuing the legitimate interests of the responsible party or of a third party to whom the information is supplied.

8.1.3 Northam Employees must identify and document the legal ground being relied on for each processing activity.

8.1.4 You may only process personal information when performing your job duties, subject to the other requirements set out in this paragraph 4 being complied with. You cannot process personal information for any reason unrelated to your job duties.

8.1.5 You may not collect excessive data. Ensure that any personal information collected is adequate and relevant for the intended purposes.

8.1.6 You must ensure that when personal information is no longer needed for specified purposes, it is deleted or de-identified in accordance with Northam's Data Retention Policy.

8.1.7 A data subject consents to the processing of their personal information if they indicate agreement either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are likely to be insufficient.

8.1.8 Data Subjects must be easily able to withdraw consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to process personal information for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

8.1.9 You will need to evidence consent captured and keep records of all Consents (both given and withdrawn by a Data Subject) so that Northam can demonstrate compliance with consent requirements.

8.1.10 Before you Process special personal information, you must ensure that you can identify the lawful basis for Processing such information. For example, Processing of special personal information can take place if:

8.1.11 Processing is carried out with the consent of a Data Subject;

8.1.12 Processing is necessary for the establishment, exercise or defence of a right or obligation in law;

8.1.13 Processing is necessary to comply with an obligation of international public law;

8.1.14 Processing is for historical, statistical or research purposes to the extent that:

8.1.15 the purpose serves a public interest and the Processing is necessary for the purpose concerned; or

8.1.16 it appears to be impossible or would involve a disproportionate effort to ask for consent,

8.1.17 and sufficient guarantees are provided for to ensure that the Processing does not adversely affect the individual privacy of the Data Subject to a disproportionate extent;

8.1.18 information has deliberately been made public by the data subject; or

8.1.19 the specific authorisation requirements set out in applicable Data Protection Legislation are complied with if the information relates to a Data Subject's religious or philosophical beliefs, race or ethnic origin, trade union membership, political persuasion, health or sex life, criminal behaviour, or biometric information.

8.2 **Collection, processing and disclosure of personal information, special personal information and CPI**

8.2.1 Subject to the provisions of paragraph 8.2.3as read with POPIA, all personal information and special personal information relating to a data subject, must be collected directly from that data subject by Northam or an authorised third party operator/outsourced service provider and must be processed in line with the purposes specified by Northam as envisaged below.

8.2.2 All CPI must be collected from the parent or legal guardian or competent person of the child concerned. The parent, legal guardian or competent person of the child must (i) be

informed of the specific purpose for which the CPI is being collected and processed and (ii) consent to the specified and disclosed collection and processing purposes.

8.2.3 Notwithstanding the provision of paragraph 8.1.1 and 8.1.2, personal information need not be collected directly from the data subject in the event that –

8.2.3.1 the personal information is derived from a public record or has been deliberately made public by the data subject and in regard to where the data subject is a child, where such publication was made with the consent of a parent, legal guardian or competent person of the child. A public record is defined in POPIA as a record that is accessible in the public domain and which is in the possession of or under the control of a public body, whether or not it was created by that public body. Examples of public records include deeds office records and the records of the Companies and Intellectual Properties Commission;

8.2.3.2 the data subject or, where the data subject is under the age of 18 (eighteen), his or her parent and/or guardian has consented to the collection of the personal information from another source;

8.2.3.3 the collection of information from another source would not prejudice a legitimate interest of the data subject;

8.2.3.4 the collection of the personal information from another source is necessary –

8.2.3.4.1 to avoid prejudice to the maintenance of the law by any public body, including the prevention, detection, investigation, prosecution and punishment of offences;

8.2.3.4.2 to comply with an obligation imposed by law or enforce legislation concerning the collection of revenue as defined in section 1 of the South African Revenue Service Act 34 of 1997;

8.2.3.4.3 for the conduct of proceedings in any court or tribunal that have commenced or are reasonably contemplated;

8.2.3.4.4 in the interest of national security; or

8.2.3.4.5 to maintain the legitimate interests of Northam or of a third party to whom the information is supplied;

8.2.3.5 compliance would prejudice the lawful purpose of the collection; or

8.2.3.6 compliance it is not reasonably practical in the circumstances of the particular case.

8.2.4 No person shall be entitled to process the special personal information of a data subject, unless –

8.2.4.1 the data subject has provided his or her consent to the processing of such information;

8.2.4.2 processing is necessary for the establishment, exercise or defence of a right or obligation in law;

8.2.4.3 processing is for historical, statistical or research purposes to the extent that –

8.2.4.3.1 the purpose serves a public interest and the processing is necessary for the purpose concerned; or

8.2.4.3.2 it appears to be impossible or would involve a disproportionate effort to ask for consent,

and sufficient guarantees are provided for to ensure that the processing does not adversely affect the individual privacy of the data subject to a disproportionate extent;

8.2.4.4 information has deliberately been made public by the data subject; or

8.2.4.5 the necessary authorisations contemplated in POPIA have been complied with.

8.3 **Personal information must be collected for a specific purpose.**

8.3.1 You may only collect, store, update, destroy or otherwise process personal information for a specific, explicitly defined and lawful purpose related to a function or activity of the responsible party.

8.3.2 Therefore:

8.3.2.1 the purpose(s) for which Northam collects and processes personal information must be clearly identified and communicated to the data subject concerned at or before the time that the personal information is collected; and

8.3.2.2 subject to paragraph 8.4.1, Northam's business units may not use the personal information for anything other purpose outside the specified purpose unless the further, legally required consent is obtained from the data subject in relation to the additional previously unmentioned purpose.

8.4 **Further Processing**

8.4.1 Notwithstanding the provisions of paragraph 8.2.2, further processing of personal information may be undertaken if it is compatible with the purpose for which the information was originally collected.

8.4.2 To establish whether further Processing is compatible with the purpose of collection, consider:

8.4.2.1 the nature of the information concerned;

8.4.2.2 the manner in which the information has been collected; and

8.4.2.3 any contractual rights and obligations between the Data Subject and Northam.

8.4.3 You cannot use personal information for new, different or incompatible purposes from that disclosed when it was first collected unless You have informed the Data Subject of the new purposes and they have Consented where necessary.

8.5 **Data subject participation**

8.6 Data Subjects have rights when it comes to how Northam handles their personal information. These include, depending on the Data Subject's location, the right to:

8.6.1 be notified that personal information is being collected;

8.6.2 be notified of a personal information breach;

8.6.3 access personal information held by Northam;

8.6.4 request the correction, destruction or deletion of personal information;

8.6.5 object to processing;

8.6.6 restrict Northam's processing of the Data Subject's personal information;

8.6.7 object to direct marketing;

8.6.8 request that Northam transfers their personal information to a third party in an easily accessible format;

8.6.9 object to automated decision making; and

8.6.10 submit a complaint to the appropriate Regulator.

8.6.11

8.7 **Outsourced service providers**

The transfer of personal information to a third party or vendor without first notifying the data subject concerned about the transfer would be deemed unlawful, thus measures must be put in place by the governance team to ensure that any transfer of personal information is legally implemented. Therefore:

8.7.1 no personal information may be passed onto any third party or vendor without informing the data subject in advance and, where required, obtaining their consent;

8.7.2 no personal information particular to persons outside Northam may be collected from vendors or any other third party without written confirmation of whether consent was obtained by the vendor or third party from the data subject(s); and

8.7.3 Northam business units must ensure that when outsourcing any processes, the vendor or third party has or will be contractually required to comply with this policy as well as related third party vendor standards and that the vendor has appropriate security measures in place for such purposes.

8.8 **Minimality**

To avoid claims against the excessive, irrelevant or inaccurate processing of personal information, You must ensure that:

8.8.1 only personal information that is relevant for the purposes for which it is being collected is obtained from the data subject(s);

8.8.2 regular reviews must be conducted and coordinated by the CO in order to ensure consistency with the primary purposes of collection of personal information; and

8.8.3 Northam business units must not process personal information unnecessarily or ask for more information than needed for the purposes for which they are collecting it (even if the information would be useful to know).

8.9 **Ensure the quality of personal information.**

To protect Northam's employees and business partners from the adverse consequences that may result from using or disclosing inaccurate, incomplete or out of date personal information, You must ensure that:

8.9.1 all reasonable steps are taken to ensure that any personal information collected, processed, stored and disclosed is accurate, complete and up to date. This is particularly important when this personal information is collected from a third party source; and

8.9.2 Northam business units must update their records when a person informs them that their details have changed and must continuously review and assess the quality of their records.

8.10 **Only retain personal information as required**

In order to ensure that a person's rights with respect to the retention of their personal information is in line with the law, Northam must ensure that personal information which is no longer required for the purposes for which it was collected or where the legal obligations for retention have expired (unless such information is retained for historical, statistical or research purposes where the responsible party has established appropriate safeguards against the records being used for any other purpose), is destroyed *via* secure means such as cross cut shredding (for paper records) or permanent erasure *via* suitable and agreed mechanisms (for electronic records) or in any other manner that prevents the reconstruction of such personal information.

8.11 **Ensure transparency of and accessibility to personal information**

8.11.1 Northam must adopt an open and transparent approach to dealing with the processing of personal information. Northam should recognise the rights of data subjects to gain access to all the personal information that Northam may hold in respect of such data subject. To this end:

8.11.1.1 Any employee of Northam who becomes aware of a security compromise relating to personal information must notify the relevant CO or Privacy Manager thereof. Such CO or Privacy Manager must immediately notify Exco of such security compromise;

8.11.1.2 a data subject is entitled to provide Northam with a written request to –

8.11.1.2.1 correct or delete the personal information of the data subject in Northam's possession or control which is inaccurate, irrelevant, excessive, out of date, incomplete, misleading or obtained unlawfully; or

8.11.1.2.2 destroy or delete a record of personal information of the data subject which Northam is no longer authorised to retain;

8.11.1.3 a set of procedures designed to facilitate a data subject(s) request for access or changes to its personal information substantially similar to those set out in Northam's PAIA process, must be defined, agreed and communicated to all relevant data subjects;

8.11.1.4 reasons for denying access or refusing to correct personal information must be provided to the data subject(s) concerned based on appropriate and documented exceptions and/or regulations. Any disputes relating to the withholding of personal information should be referred to, and the resolution thereof facilitated by, Exco;

8.11.1.5 You must take reasonable steps to ensure that the data subject is aware of various matters related to the collection of personal information, including but not limited to:

8.11.1.5.1 the type of personal information collected,

8.11.1.5.2 the source from which it is collected;

8.11.1.5.3 Northam's details;

8.11.1.5.4 the purpose for which the personal information is collected;

8.11.1.5.5 whether the supply of the personal information is voluntary or mandatory;

8.11.1.5.6 the consequences for failing to provide the personal information;

8.11.1.5.7 any law, including Data Protection Legislation, which requires the collection of the personal information;

8.11.1.5.8 whether Northam intends to transfer the personal information to another country and the level of protection afforded to that personal information in that country;

8.11.1.5.9 the recipients of the personal information;

8.11.1.5.10 the Data Subject's right to access, rectify, or object to the collection or processing of the personal information; and

8.11.1.5.11 the right to lodge a complaint with the appropriate Regulator.

8.12 **Ensure the security of personal information**

To secure the integrity of personal information in Northam's possession or under its control and to prevent unauthorised access, business disruptions, legal liabilities and abuses of such personal information, the following must be applied:

8.12.1 suitable measures to prevent and detect unauthorised entry to premises where personal information may be stored or processed must be adopted; and

8.12.2 suitable measures to protect computer systems and networks used for storing, processing and transmitting personal information from unauthorised access, modification and disclosure must be taken.

8.13 Northam will endeavour to identify all reasonably foreseeable internal and external risks to personal information in Northam's possession or under its control. Northam will develop, implement and maintain safeguards appropriate to its size, scope and business, Northam's available resources, the amount of personal information that it owns or maintains on behalf of others and identified risks. Northam will regularly evaluate and test the effectiveness of those safeguards to ensure the security of its processing of personal information, and update them when new risks are identified. In this regard, it is important that You are responsible for protecting the personal information that is processed by Northam (to the extent that You are involved in the processing of this personal information).

8.14 You must adhere to the security measures put in place by Northam and exercise care when processing personal information.

8.15 **Cross border transfer**

8.15.1 Subject to the provisions paragraph 8.15.2, Northam shall not be entitled to transfer the personal information of a data subject to a third party who does not reside within South Africa.

8.15.2 Personal information of a data subject may be transferred outside of South Africa where –

8.15.2.1 the third party concerned is subject to a law, binding corporate rules or a binding agreement which provides an adequate level of protection that –

8.15.2.1.1 effectively upholds principles for reasonable processing of the information that are substantially similar to the conditions for the lawful processing of personal information relating to a data subject who is a natural person and, where applicable, a juristic person; and

8.15.2.1.2 includes provisions, that are substantially similar to this paragraph 8.15, relating to the further transfer of personal information from the recipient to another third party who is in a foreign country;

8.15.2.2 the data subject consents to the transfer;

8.15.2.3 the transfer is necessary for the performance of a contract between the data subject and the relevant company within the Northam group, or for the implementation of pre-contractual measures taken in response to the data subject's request;

8.15.2.4 the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between Northam and a third party; or

8.15.2.5 the transfer is for the benefit of the data subject, and –

8.15.2.5.1 it is not reasonably practical to obtain the consent of the data subject to that transfer; and

8.15.2.5.2 if it were reasonably practical to obtain such consent, the data subject would be likely to give it.

8.15.3 In the event of a transfer of personal information as contemplated in this paragraph 8.15 taking place, the person responsible for such transfer shall be required to provide the CO or Privacy Manager with details pertaining to the transfer, including but not limited to whether the consent to the transfer was obtained from the data subject and proof of such consent.

9 NON-COMPLIANCE

9.1 All employees are required to comply with this policy, and where requested, to demonstrate such compliance. Any violations of this policy may result in disciplinary action and will be dealt with under the appropriate Northam disciplinary policy, and/or may result in civil or criminal legal action against an employee, contractor or third party, as applicable.

9.2 Northam reserves the right to audit and/or monitor compliance with this policy, and any other related policies, guidelines or standards at any time.

9.3 Northam reserves the right to suspend or permanently remove access to its information assets and processing facilities based on non-compliance with this policy.

9.4 Any exceptions to this policy must be fully motivated and documented by those seeking the exception, and agreed to by the relevant person(s) tasked with risk management around the particular area(s) affected by the exception and will be reviewed at least annually.

9.5 You are obliged to report any violation of this Policy by another Employee to the Information Officer as soon as possible.

10 ROLES AND RESPONSIBILITIES

10.1 Business units and line managers have overall accountability for making their employees aware of this policy and ensuring that they comply with the principles and rules contained herein.

10.2 Every employee is responsible for complying with this policy and must notify line managers, the CO or Privacy Manager if he/she suspects any violation of this policy.

10.3 The CO and/or Privacy Manager(s) are responsible for developing and over-seeing related privacy practices, standards and policies, and has the mandate to ensure adherence to this policy as well as related privacy procedures in order to ensure that appropriate controls are adopted across Northam.

10.4 The CO acts as the appointed information officer as defined in PAIA.

10.5 The CO will, *inter alia*, be responsible for initiating and facilitating:

10.5.1 compliance by Northam and all its data processors with the provisions of the POPIA, any other applicable privacy related legislation and this policy;

10.5.2 appointing of privacy representatives within each business unit of Northam;

10.5.3 authorising of collection, processing and/or destruction of personal information in hard copy, soft copy and any other format used by Northam;

10.5.4 managing the personal information on Northam owned databases, mobile devices, hardcopy documents and stored hard and soft copy data that is the property of Northam

and ensuring the integrity of the data is delegated to the Privacy Manager(s), who will manage the respective data processors of Northam;

10.5.5 the CO and Privacy Manager(s) of Northam are responsible for data processors and are accordingly responsible for the maintenance of Northam's personal information. Data integrity responsibilities are delegated to the user level where data is generated or processed by the data processors. The CO and Privacy Manager(s) shall ensure the security clearance and profile of the user handling the data is in line with the security classifications of the data. Access to data shall be allocated on a need-to-know basis and as authorised;

10.5.6 the CO or Privacy Manager(s) should report to and update Exco at least once every 6 (six) months on all privacy related issues; and

10.5.7 the CO or Privacy Manager(s) should also liaise with Exco on any new developments or amendments relating to the drafting, implementing and operationalisation of Northam data privacy standards.

11 DISCIPLINARY ACTION

Disciplinary action may be taken against any employees who do not comply with this policy. Where such non-compliance constitutes gross misconduct it may result in dismissal.

12 GOVERNANCE

This policy should be reviewed by Exco at least once every 3 (three) years to ensure compliance with the latest corporate governance best practice.