TERANGA GOLD CORPORATION
DATA PROTECTION AND PRIVACY POLICY

1. Introduction

The Board of Directors (the "**Board**") of Teranga Gold Corporation ("**Teranga**")[1] has determined that Teranga should formalize its policy on protecting the privacy and security of Personal Data. All capitalized terms not otherwise defined herein shall have the meanings ascribed to them in Schedule "A".

2. Application and Objectives of the Policy

Teranga's Data Protection and Privacy Policy (the "**Policy**") applies to all employees, directors and officers of Teranga, including, temporary staff, agents, consultants, contractors, vendors and service providers (collectively "**Representatives**") in their Processing of Personal Data (as defined below) on behalf of Teranga. The Policy is intended to set out the minimum requirements to ensure compliance by Teranga and its Representatives with applicable privacy and data protection laws and regulations ("**Data Protection Requirements**").

3. Data Protection and Privacy Principles

Teranga's data protection and privacy principles are set out below. All Representatives must:

(a) Process Personal Data only for specified, explicit, lawful, and legitimate purposes and only: (i) with the valid consent of the individual to whom the Personal Data relates (each, an "**Individual**"); or (ii) where otherwise permissible under Data Protection Requirements;

(b) Process Personal Data fairly and lawfully in compliance with Data Protection Requirements and the rights of the Individual;

(c) Process Sensitive Personal Data using special care, as it is subject to additional Data Protection Requirements (see Section 5 below);

(d) ensure that Personal Data is adequate, relevant, accurate, complete, kept up to date, as appropriate, and not excessive in relation to the purposes for which the Personal Data is Processed;

(e) not keep Personal Data in an identifiable form for longer than necessary;

(f) use appropriate technical and organizational measures in relation to Personal Data; and

(g) only transfer Personal Data from one jurisdiction to another where allowed by Data Protection Requirements. For example, transfers of Personal Data from certain European countries to other jurisdictions is allowed only if the receiving jurisdiction is considered to have an adequate level of protection or an exemption applies.

[1] The Policy applies to Teranga and each of its subsidiaries. Accordingly, the Policy will refer to Teranga Gold Corporation and its subsidiaries as "Teranga".

4. Legal Grounds for Processing

Teranga shall only Process Personal Data if one or more of the following criteria are met and if such Processing is:

(a) consented to in writing by the Individual. This consent must be a freely given, specific, informed, unambiguous and active indication that an Individual agrees to the Processing of his or her Personal Data. The Individual has the right to withdraw consent at any time and must be informed of this right;

(b) necessary for the performance of, or to take steps to enter into, a contract with the Individual (e.g. an employment contract);

(c) necessary to comply with a legal obligation; and/or

(d) necessary for the legitimate interests of Teranga (or third parties to whom the Personal Data must be disclosed), except where such interests are overridden by the fundamental rights and freedoms of the Individual.

5. Sensitive Personal Data

Teranga will generally only be able to Process Sensitive Personal Data where, for example:

(a) the Individual has given his or her explicit consent; or

(b) the Processing is necessary and specifically authorized or required by law.

The Processing of Sensitive Personal Data must be kept to a minimum and only as strictly necessary. Where it is possible to Process Sensitive Personal Data anonymously or as aggregated data, Teranga will endeavor to do so. Due to the sensitivity of Sensitive Personal Data:

(a) it must be Processed in accordance with the highest of security standards; and

(b) access to Sensitive Personal Data should be restricted to only those Representatives who require it to complete their tasks.

6. Disclosure of Personal Data to Data Processors and Other Third Parties

If Teranga engages a supplier or service provider and it is anticipated that such supplier or service provider will Process Personal Data on behalf of and in accordance with instructions from Teranga (i.e. it will become a Data Processor and Teranga the Data Controller), then Teranga shall not provide any Personal Data to such supplier or service provider unless: (i) a written agreement has been entered into which includes specific data protection provisions; and (ii) Teranga can ensure that appropriate safeguards are in place in connection with the Processing of such Personal Data.

Teranga's standard purchase order terms and conditions and template contracts contain data protection provisions. Please consult with the Legal Department if you are in discussions with a potential supplier who may have access to Personal Data in the course of their engagement and who wish to modify or negotiate any such provisions. The Legal Department will assist in the review and/or preparation of any such amendments.

In the event Teranga is required to disclose Personal Data to a third party who is not acting as a Data Processor (for example, disclosures in response to a request made by the police or a regulator) and such third party Process such Personal Data, then Teranga will take reasonable and appropriate steps to maintain the level of data protection and privacy as required by this Policy. The Legal Department and, if specifically related to an employee of Teranga, the Corporate Human Resources Department, should be

consulted prior to making any such disclosures to ensure that any additional legal requirements have been addressed.

7. Transfers of Personal Data

Transfers of Personal Data from certain jurisdictions (e.g. the European Union) to other jurisdictions is allowed only if the receiving jurisdiction is considered to have an adequate level of protection (e.g. Canada is considered a jurisdiction with an adequate level of protection) or an exemption applies (e.g. consent is obtained, model contracts or provisions are adopted, etc.).

Please consult with the Legal Department and the Corporate Human Resources Department (if specifically related to an employee of Teranga) if you may be transferring Personal Data from one jurisdiction to another, as certain prohibitions on these transfers may apply. The Legal Department will assist in determining whether any action is required to effect the transfer.

8. Rights of Individuals

Individuals have certain rights under Data Protection Requirements (subject to limitations and/or restrictions), including the right to:

(a) be informed about the collection and use of their Personal Data;

(b) request access to and correct or delete their Personal Data;

(c) restrict or object to Processing of their Personal Data;

(d) data portability (i.e. have their Personal Data available in a structured, commonly used, machine-readable and interoperable format that allows the transfer of the Personal Data to another controller; and

(e) not be subject to a decision based solely on automated Processing, including profiling, which produces legal effects concerning the Individual or significantly affects the Individual.

9. Marketing Activities

Subject to applicable laws and Teranga's policies and guidance on promotional activities, Personal Data may only be Processed to send marketing information to an Individual (including any employee) where specific consent has been received from the Individual.

If Teranga or any of its affiliates or Representatives wish to send marketing information to an Individual, they should first contact Investor Relations before sending any such communications to ensure adequate consent has been or will be obtained.

10. Data Security

Appropriate physical, technical, and organizational measures must be maintained to protect Personal Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, having regard to the cost of implementation, the nature of the data, and the risks to which they are exposed.

Employees who are required to Process Personal Data as part of their job duties will receive training and guidance on how to maintain the security of Personal Data. However, Teranga expects all of its employees to be aware of the basic security principles as set out in this Policy and Teranga's other policies, as applicable.

It is the responsibility of all employees to report all security breaches, or suspected security breaches, relating to loss of, or unauthorized access to or disclosure of Personal Data, as soon as possible to the

Legal Department as well as the Corporate Human Resources Department if specifically related to an employee of Teranga.

11. Communication of the Policy

Copies of this Policy are made available to Representatives, either directly or by posting of the Policy on the Teranga website at www.terangagold.com. This Policy may be revised at any time and Representatives will be informed whenever significant changes are made through appropriate mechanisms. New Representatives will be provided with a copy of this Policy or directed to the website to obtain a copy.

12. Administrative Responsibility

Teranga's Legal Department will be responsible for overseeing Teranga's compliance with Data Protection Requirements and ensuring adherence to this Policy.

The General Counsel will be the individual primarily responsible for ensuring that Teranga complies with all Data Protection Requirements, including:

(a) monitoring compliance with this Policy;

(b) initiating, with input and advice from the other members of senior management, the implementation of data protection and privacy procedures in accordance with the principles set out in this Policy; and

(c) dealing with any issues which may be raised from time to time by applicable regulatory authorities.

13. Dealing with Regulators

If a data protection or privacy authority or regulator, as applicable, requests information from or contacts a Representative for any reason, the Legal Department and the Corporate Human Resources Department must be contacted immediately and will handle such request and respond accordingly.

14. Consequences of Non-Compliance with Policy

Failure to comply with this Policy may result in severe consequences, which could include internal disciplinary action or termination of employment or consulting arrangements without notice. The violation of this Policy may also violate Data Protection Requirements worldwide, and if it appears that a director, officer or employee may have violated such laws or regulations, then Teranga may refer the matter to the appropriate regulatory authorities, which could lead to penalties, fines or even possibly imprisonment.

15. Review of Policy

The Board of Directors of Teranga shall annually review and evaluate this Policy to determine whether the Policy is effective in ensuring compliance with Data Protection Requirements and that appropriate measures are taken to ensure the protection and privacy of Personal Data.

16. Queries

If you have any questions about how this Policy should be followed in a particular case, please contact the General Counsel of Teranga.

Dated: August 1, 2018
Approved by: Board of Directors

SCHEDULE "A"

As used in this Policy, the following terms have the meanings set out below:

"**Data Controller**" means the natural or legal person, public authority, agency or any other body which alone, or jointly with others, determines the purposes and means of the Processing of Personal Data.

"**Data Processor**" means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of a Data Controller.

"**Personal Data**" means any information relating to an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

"**Processing**" means any operation or set of operations performed upon Personal Data or sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, and "Process(es)" and "Processed" will be interpreted accordingly.

"**Sensitive Personal Data**" includes Personal Data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, actual or alleged criminal offences or criminal convictions, data concerning health or sex life and sexual orientation, and genetic data or biometric data.