PROTECTION OF PERSONAL INFORMATION POLICY

Dated July 15, 2024

TABLE OF CONTENTS

I. INTRODUCTION

The board of directors (the "**Board**") of G Mining Ventures Corp. ("**GMIN**" or the "**Corporation**") has adopted this protection of personal information policy (this "**Policy**") to affirm and document its commitment to the appropriate use and safeguarding of Personal Information (as defined herein). The objectives of this Policy are to communicate the Corporation's expectations and requirements with respect to the handling of Personal Information, including GMIN Subject Parties' (as defined herein) Personal Information and to facilitate compliance with applicable laws pertaining to privacy and the protection of Personal Information.

II. SCOPE

This Policy applies to all of GMIN's directors, officers, employees, contractors, representatives, service providers and other persons under the direct control of GMIN, irrespective of jurisdiction (collectively, the "**GMIN Subject Parties**"), and for the purposes hereof, references to the Corporation or GMIN are deemed to include references to each of the foregoing.

This Policy is intended to comply with applicable Canadian privacy laws. To the extent any provision herein conflicts with a legal requirement in another jurisdiction, GMIN Subject Parties shall comply with the applicable law.

III. INTERPRETATION

"**Personal Information**" means any information about an identifiable individual, whether factual or subjective, and includes publicly available information. An individual is considered identifiable if it is possible to identify him or her from the information on its own or when combined with other information. This includes information that isn't immediately available (*e.g.*, records held by someone other than GMIN).

Examples of Personal Information include:

- name and contact details (*e.g.*, telephone number, address, email address and social media handle);
- demographic information (*e.g.*, age or date of birth, marital status and gender);
- banking information or payment card information (*e.g.*, credit card numbers);
- government issued identification numbers (*e.g.*, social insurance numbers);
- employment information (*e.g.*, position, wages earned and employment record); and
- behavioural data (*e.g.*, preferences and inferred interests). This type of information is considered Personal Information even if the individual is identified only by a user ID, a device ID, an IP address or any other identifier and not by name.

"**Privacy Officer**" means the vice president, legal affairs & corporate secretary of the Corporation.

IV. ACCESS TO PERSONAL INFORMATION

While working for GMIN, certain GMIN Subject Parties may have access to Personal Information. It is important that they only access Personal Information on a "need to know" basis. This means that GMIN Subject Parties must limit their access to Personal Information to what they are authorized to access by the terms of their employment or contractual agreement with GMIN, or by the nature and/or scope of their duties (*e.g.*, employees having a HR function or managing a payroll), and only to the extent necessary to accomplish the foregoing or another legitimate business purpose. See Section VI for information regarding legitimate business purposes for which Personal Information may be accessed.

GMIN Subject Parties should only access such Personal Information that they need to accomplish their duties and exercise their functions for GMIN.

V. CONSENT

Canadian privacy laws require organizations to obtain informed consent from individuals before collecting, using or disclosing their Personal Information, subject to limited exceptions.

GMIN shall ensure that any and all consents are obtained on a clear, free and informed basis and are given for specific purposes. When the request is made in writing, it must be presented separately from any other information provided to the person concerned. Additionally, individuals must be informed of the purpose for the collection, the means of the collection, and their rights under applicable privacy laws, including the rights set forth in Section XIV.

With respect to the type and necessity of consent required, GMIN Subject Parties should be mindful of the following:

- Express Consent: means that, after having been clearly informed of the intended collection, use or disclosure of his or her Personal Information, the applicable individual has taken an affirmative step to signal his or her consent, such as checking a box, signing his or her name or verbally consenting. Express consent must be sought when the Personal Information being collected is sensitive (*e.g.*, health, financial or credit information, location information or biometric information) or when the individual would not expect the proposed collection, use or disclosure of Personal Information. Express consent may also be required under certain statutes (*e.g.*, to obtain express consent under Canada's anti-spam legislation).
- Implied Consent: means that the intended collection, use or disclosure of Personal Information is obvious in the circumstances and, as a result, it would be reasonable to assume that the individual, by providing his or her Personal Information, has provided

consent (*e.g.*, if an individual contacts the Corporation with a complaint, the consent to use his or her name and contact information to respond to the complaint would be implied).

- Consent Not Required: There are situations where GMIN may collect, use or disclose Personal Information without informed consent, such as in emergency situations when someone's life or health is threatened, in the context of an investigation into a breach of law or contract by an applicable individual, or when required by law or court order. Any decision to rely on these exceptions must be made in consultation with the Privacy Officer.
- Optional Consent: An individual cannot be required to consent to a collection, use or disclosure of his or her Personal Information for a purpose that is not necessary in the circumstances. For instance, an individual cannot be required to consent to receiving marketing communications as a condition to submitting a complaint or question online. Similarly, an individual cannot be required to provide his or her gender as a condition of participating in a sweepstakes or promotion, since this information is not necessary in the circumstances. Consent for non-essential collections, uses or disclosures of Personal Information must be optional, and the optional nature of the consent must be communicated to the applicable individual.

VI. COLLECTING, USING AND DISCLOSING PERSONAL INFORMATION

A. Limit Collection of Personal Information to What is Necessary

The amount and type of Personal Information that is collected must be limited to what is necessary in the circumstances of such collection. The purpose for collecting Personal Information must be determined in advance. "**Necessary**" means that the information is essential to the purpose for which Personal Information is collected (*e.g.*, collection of a bank account number to set up direct deposit for payroll purposes).

Non-essential information may still be requested, so long as it is not unreasonable and is provided on a voluntary or optional basis. For instance, requesting demographic information from participants in a sweepstake cannot be required because this information is not necessary to administer the sweepstake. However, it is reasonable to collect and use this information for market research purposes. Accordingly, non-essential information can be requested from participants on a voluntary or optional basis, provided that the purposes for which the information will be used (if provided) are made clear.

Personal Information may never be collected, used or disclosed for purposes that a reasonable person would consider to be inappropriate, even if consent for such collection is obtained. GMIN Subject Parties should consult with the Privacy Officer if they have concerns about a planned collection, use or disclosure of Personal Information.

B. Collect Personal Information Directly from the Individual or Verify Authority for Indirect Collections

To the fullest possible extent, Personal Information should be collected directly from the individual about whom the information relates. However, there may be situations where it is necessary to collect Personal Information indirectly from another source. For instance, GMIN Subject Parties may collect Personal Information about an employee applicant from a reference, previous employer or through a background check provider, and individuals may provide Personal Information about their spouse or dependents in connection with benefits enrolment or administration. When Personal Information is collected indirectly, GMIN Subject Parties must take steps to ensure that appropriate consents have been obtained (*e.g.*, by obtaining consent from the individual to collect the Personal Information from the other source or by obtaining confirmation from the individual that he or she has all necessary consents to provide such Personal Information).

C. Collect, Use and Disclosure of Personal Information with Consent

As further discussed in Section V, Personal Information may only be collected, used, and disclosed with informed consent, subject to very limited exceptions.

GMIN Subject Parties are expected to familiarize themselves with the various policies and related documentation of the Corporation, including the internal privacy notice, so that they understand the purposes for which Personal Information is generally collected, used and disclosed by GMIN. However, it is important to note that a mere description of a collection, use or disclosure of Personal Information in a policy does not imply that an individual has consented to such collection, use or disclosure. Accordingly, prior to collecting, using or disclosing Personal Information for a particular purpose, GMIN Subject Parties must ensure that appropriate consents have been obtained.

GMIN Subject Parties involved in the collection of Personal Information must be able to provide a rationale with respect to the purposes for which such Personal Information will be used and disclosed. Any questions or complaints with respect to the collection, use or disclosure of Personnel Information must be promptly referred to the Privacy Officer.

VII. PRIVACY AND NEW PROJECTS

GMIN Subject Parties are expected to comply with this Policy in respect of all handling of Personal Information. However, it is particularly important to take privacy into account in connection with new tools, applications and software programs and new vendors (collectively, "**New Projects**"). If a New Project involves access to Personal Information under GMIN's control, or the collection, use, or disclosure of Personal Information, the privacy implications of the New Project must be assessed through a privacy impact assessment to ensure compliance with this Policy and applicable privacy laws. GMIN Subject Parties should consult with the Privacy Officer in respect of all New Projects.

VIII. TRANSFERS OUTSIDE OF QUÉBEC

Before communicating Personal Information outside of the Province of Québec, GMIN Subject Parties must conduct an assessment of privacy-related factors. GMIN Subject Parties should consult with the Privacy Officer in respect of all transfers of Personal Information outside of Québec.

IX. PROFILING

If GMIN collects Personal Information using technology that includes functions allowing the person concerned to be identified, located or profiled, GMIN Subject Parties must first inform the individual of the use of the technology and the means available to activate the function that allows the individual to be identified, located or profiled. "Profiling" means the collection and use of Personal Information to assess certain characteristics of a natural person, in particular for the purpose of analyzing that person's work performance, economic situation, health, personal preferences, interest or behaviour.

X. AUTOMATED PROCESSING

If GMIN renders a decision concerning one person based exclusively on automated processing (*e.g.*, no human intervention), GMIN Subject Parties must inform such person accordingly no later than at the time it informed him or her of such decision.

XI. SAFEGUARDING PERSONAL INFORMATION

GMIN Subject Parties play a critical role in maintaining the security and confidentiality of Personal Information. GMIN Subject Parties are expected to familiarize themselves with the Corporation's policies with respect to information technology ("IT"), including the code of ethics and business conduct, and to participate in all mandatory information security training.

In addition, GMIN Subject Parties are expected to follow basic information security best practices, as set forth below:

1. ensure that filing cabinets containing Personal Information remain locked and keep keys in a secure location;
2. choose a strong password that is at least eight characters long and made up of multiple types of characters, including lower case letters, uppercase letters, numbers and symbols, and change such password periodically;
3. keep password secure, never write it down and never share it with anyone;
4. lock computer screens when stepping away from computer, even if just for a few minutes;
5. never store Personal Information on portable devices, such as laptops or thumb drives and always use remote access to access Personal Information stored in GMIN systems; however,

if Personal Information must absolutely be stored on a portable device, ensure that the information is strongly encrypted and securely deleted once it is no longer needed;

6. when deleting, discarding or destroying documents and records, ensure to do so securely and consult with the IT department of the Corporation (the "IT Department") to further ensure secure erasure; paper files must be shredded and electronic files permanently erased;

7. exercise a high degree of caution before clicking on a link or attachment in an email (*e.g.*, verify that the email is legitimate before clicking a link or opening an attachment) and never provide a username and password if prompted to do so after clicking a link or attachment; when in doubt, contact the sender by phone to confirm or contact the IT Department; and

8. never install software or applications on a GMIN computer or device, as such software or applications may contain malware or viruses or may permit third parties to access information in GMIN systems without GMIN's knowledge; obtain prior approval for all such installations by the IT Department.

XII. SUSPECTED CONFIDENTIALITY INCIDENT

A "Confidentiality Incident" means any loss or theft of, or unauthorized access, use or disclosure of Personal Information. Examples of Confidentiality Incidents include:

- emailing, faxing or mailing Personal Information to the wrong recipient;
- losing a phone, laptop or other device that contains or could contain Personal Information;
- losing a physical file containing Personal Information; or
- a technology issue that has resulted or could have resulted in unauthorized access to Personal Information (*e.g.*, a secure website that is inadvertently made accessible to the public or a cybersecurity incident).

If GMIN Subject Parties suspect that a Confidentiality Incident has or may have occurred, or if they identify any other concerns with respect to the security of Personal Information, they must immediately notify the Privacy Officer, who will follow the protocols set forth in the Corporation's cyber incident response plan.

XIII. RETENTION OF GMIN SUBJECT PARTIES' PERSONAL INFORMATION

GMIN retains Personal Information in accordance with its records retention policy. Such policy is designed to ensure that Personal Information is retained only for as long as necessary to fulfil the purposes for which the Personal Information was collected, in accordance with prudent business practices on general document retention or as required by law. Personal Information must be kept sufficiently accurate, complete, and up-to-date as necessary to minimize the risk that inaccurate information will be used to make a decision about an individual.

XIV. INDIVIDUAL RIGHTS WITH RESPECT TO PERSONAL INFORMATION

GMIN must make information about its policies and practices with respect to the handling of Personal Information available upon request. For GMIN Subject Parties, this information is set forth in Sections XV to XX. For members of the public, this information is made available through the privacy policy available on the Corporation's website at [insert link].

Privacy laws grant individuals certain rights with respect to their Personal Information. The available rights will depend on applicable privacy laws, but may include:

- the right to request access to Personal Information in the control of GMIN or request a copy of such information for the GMIN Subject Party's own use;
- the right to request information about the purposes for which GMIN has used Personal Information and the third parties to whom the Personal Information has been disclosed and for what purposes;
- the right to request that inaccurate or incomplete information be corrected or supplemented;
- the right to withdraw consent to the collection, use or disclosure of Personal Information or restrict its use;
- the right to make a complaint to GMIN or a supervisory authority about the Corporation's practices with respect to the management of Personal Information; and
- the right to require that Personal Information be deleted if retaining the Personal Information is not authorized by law and to request that GMIN cease disseminating certain information.

These rights are not absolute and are subject to certain contractual and legal restrictions.

If GMIN Subject Parties receive a rights request or a question with respect to how to make such a request from a member of the public, they must forward the request to the Privacy Officer. Upon receipt of such request, the Privacy Officer will take the appropriate measures to verify the identity of the requestor prior to sharing Personal Information.

GMIN Subject Parties can access and update certain Personal Information by contacting the Privacy Officer.

Upon receipt of such request, the Privacy Officer will proceed in accordance with the Corporation's personal information requests policy.

XV. COLLECTION OF PERSONAL INFORMATION FROM GMIN SUBJECT PARTIES

In relation to their appointment, employment or other contractual relationship, GMIN may collect, use, and disclose Personal Information of GMIN Subject Parties for business purposes consistent with applicable laws. The Personal Information collected includes, where appropriate:

- name and contact information (personal and business);
- next of kin, marital status, emergency contact information, age, date of birth and gender;
- information provided in an application, through references or authorized background checks, including educational background, work experience, languages spoken, ID verification and credit checks;
- information relating to health conditions, disabilities or accommodation requirements;
- information required for administration of payroll (including direct deposit information), insurance, pension and benefit plans, including date of birth, social insurance number, beneficiaries and dependent information, and banking information;
- information collected through or for the purposes of security and workplace monitoring systems, including photographs;
- information collected through GMIN monitoring technology; and
- information collected to advance and measure diversity at GMIN, including in accordance with the Corporation's diversity policy.

Personal Information may be collected directly from GMIN Subject Parties, indirectly through monitoring technology or premises, and/or from third parties, including from, where appropriate:

- individuals providing references;
- third parties responding to authorized background checks;
- workplace monitoring mechanisms;
- third parties sending email, mail or other forms of communication to GMIN Subject Parties;
- individuals conducting investigations into suspected unlawful or inappropriate activity or investigations into breaches of contract, including employment or services agreements; and
- professional indemnity insurers regarding claims.

XVI. PURPOSES FOR USING, PROCESSING AND DISCLOSING PERSONAL INFORMATION OF GMIN SUBJECT PARTIES

The purposes for which GMIN uses, processes and discloses Personal Information are as set forth below:

- to comply with applicable legal and regulatory requests and obligations, including investigations in connection therewith;
- to establish or defend legal claims and allegations;
- for security purposes or to prevent, detect, or investigate fraud, suspected or actual illegal activity, violations of the Corporation's policies or rules, or other forms of misconduct;
- to seek advice and/or services from legal counsel, auditors and other professional advisors;
- to administer employee benefits and insurance plans, pension plans, professional indemnity insurance plans and professional memberships, and maintain records relating thereto; and
- for any other legitimate purpose identified by GMIN.

In addition to the foregoing, GMIN may disclose or transfer Personal Information to:

- service providers who administer or provide products, services or information on behalf of GMIN, including, but not limited to, payroll, pension and benefits administrators, information technology contractors, human resource information systems and employee assistance providers; and
- regulatory (including self-regulatory) or governmental authorities as requested or required for the purpose of fulfilling the Corporation's mandates or responsibilities.

XVII. DATA TRANSFER OF GMIN SUBJECT PARTIES PERSONAL INFORMATION

Personal Information of GMIN Subject Parties is processed and stored by GMIN or its service providers in Canada. If such service providers are located outside of Canada, GMIN will ensure that appropriate safeguards are in place as required by applicable laws.

XVIII. GMIN SUBJECT PARTIES RIGHTS WITH RESPECT TO PERSONAL INFORMATION

Privacy laws grant individuals certain rights with respect to their Personal Information. The available rights will depend on applicable privacy laws, but may include:

- the right to request access to Personal Information in the control of GMIN or request a copy of such information for the GMIN Subject Party's own use;

- the right to request information about the purposes for which GMIN has used Personal Information and the third parties to whom the Personal Information has been disclosed and for what purposes;
- the right to request that inaccurate or incomplete information be corrected or supplemented;
- the right to withdraw consent to the collection, use or disclosure of Personal Information or restrict its use;
- the right to make a complaint to GMIN or a supervisory authority about GMIN's practices with respect to the management of Personal Information; and
- the right to require that Personal Information be deleted if retaining the Personal Information is not authorized by law and to request that GMIN cease disseminating certain information.

GMIN Subject Parties may submit a request directly or authorize an agent to submit a request for accessing, correcting, or deleting their Personal Information. To the extent an agent is authorized, such agent will need to provide written proof of his or her permission to act on the applicable GMIN Subject Party's behalf. Failure to provide such evidence will result in the denial of the request in order to safeguard the Personal Information.

These rights are not absolute and are subject to certain contractual and legal restrictions.

Upon receipt of a rights request with respect to Personal Information, the Privacy Officer will proceed in accordance with the Corporation's personal information requests policy.

XIX. COMMENTS, QUESTIONS AND/OR CONCERNS

GMIN is responsible for the Personal Information under its control. Responsibility for ensuring compliance with this Policy and applicable privacy laws rests with the Privacy Officer.

If any GMIN Subject Party has any comments, questions and/or concerns with respect to the subject-matter covered by this Policy, such individual should contact the Privacy Officer at mdagenais@gminingventures.com.

XX. COMPLIANCE

All GMIN Subject Parties are expected to review and understand this Policy and attend mandatory privacy training.

GMIN may monitor and verify compliance with this Policy using a variety of methods, such as periodic walk-throughs, video and network monitoring, business tool reports, internal and external

audits, and other formal or informal methods of measuring and documenting compliance, subject to applicable privacy laws.

Any GMIN Subject Party found to have violated this Policy may be subject to disciplinary action, up to termination, including for serious fault, or resiliation of contract for serious reason.

GMIN Subject Parties must promptly report any violation or suspected violation of this Policy to the Privacy Officer, either directly or by email at the following address: mdagenais@gminingventures.com. In the event that the Privacy Officer may be involved in the violation or suspected violation, the reporting individual must so report at the following address: ethics@gminingventures.com.

XXI. REVIEW

On an as-needed basis, the environment, social & governance committee of the Board (the "**ESG Committee**") shall review this Policy, including by assessing its effectiveness, and recommend any changes to this Policy to the Board. The Board may also amend this Policy, as required.

The Privacy Officer shall monitor the implementation of this Policy and shall periodically provide reports and, as applicable, make recommendations to the ESG Committee with respect to any recommended changes thereto.

Any amendments to this Policy must be communicated with diligence to GMIN Subject Parties.

XXII. EFFECTIVE DATE

This Policy was adopted by the Board on July 15, 2024.