



AUSTIN GOLD CORP. INFORMATION TECHNOLOGY POLICY

Access to Austin Gold Corp.'s (the "Company") computers, networks, communications systems and other information technology ("IT") systems is provided to employees and consultants (together "**Employees**") to promote effective communication and working practices within our organization. This policy outlines the standards Employees must observe when using these systems, the circumstances in which the Company will monitor their use, and actions that may be taken when this policy is breached.

This policy applies to all Employee access to and use of IT and communications systems owned by or available through the Company, including any access or use of those systems by Employees through their own resources. These systems include, but are not limited to:

- Email systems and email accounts.
- The Company's intranet.
- Internet access.
- Instant messaging services.
- Telephones and voicemail systems, including landline and mobile telephones, smartphones and pagers.
- Printers, photocopiers and scanners.
- Fax machines.
- All computers, computer networks, computer storage devices (including hard drives, flash drives, and external hard drives), peripheral equipment, and software.
- Cameras.

This policy applies to all the Company's Employees, and to any contractors, who have access to the Company's IT and communication systems.

Equipment Security and Passwords

Each Employee is responsible for the security of the IT and communications equipment allocated to or used by them and must not allow that equipment to be used by anyone other than the Employee except in accordance with this policy.

Each Employee is responsible for the security of any computer used by the Employee. Employees should lock the computer or log off when leaving it unattended, including when leaving the office, to prevent unauthorized users accessing the Company's systems.

Employees must use passwords on all IT and communications systems in accordance with guidelines provided by the Company's management.

System and Data Security

The Company operates computer, data and communications networks and related systems to support all of its business functions. To protect these networks, and the information accessible through them, Employees must adhere to the terms of this policy and any guidelines issued by management of the Company.

Employees must not access the Company's systems using the password or login information of another Employee or permit another person to access the Company's systems using the Employee's own password or login information.

Employees must not access, alter, or delete any document or other data stored on the Company's systems unless authorized to do so in performance of the Employee's duties.

Employees must not delete, destroy or modify existing systems, programs, information or data held on the Company's computers, telephones, tablets, or other devices unless authorized to do so in performance of the Employee's duties.

Employees must not download or install software from external sources onto any Company computer, telephone, tablet or other device without authorization from the Employee's manager. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. Incoming files and data should always be virus-checked in accordance with the Company's guidelines before they are downloaded.

Employees must not attach any device or equipment to the Company's systems without authorization from the Employee's manager. This includes any flash drive, MP3 player, tablet, mobile telephone or other similar device, whether connected via a USB port or in any other way.

Employees must inform their manager immediately if they suspect a device connected to the Company's systems is infected with a virus.

Employees must not attempt to gain access to restricted areas of the Company's network, or to any password-protected information, unless authorized to do so in performance of the Employee's duties.

Telephone and Voicemail

The Company provides landline telephones, and may provide mobile telephones, to Employees for use in performing their job duties. Telephone calls are an important method of communication with co-workers and may be the first or only point of contact third parties have with the Company. Employees must be courteous and informative in all telephone calls made or received on the Company's behalf.

Employees using a landline or mobile telephone to discuss the Company's confidential information should ensure that their conversation cannot be overheard.

Employees with dedicated landline or mobile telephones are required to maintain a password protected voicemail account and must check any messages left on this account periodically.

In using landline or mobile telephones provided by the Company, Employees must avoid incurring charges that are not approved by their manager (including long distance charges, roaming

charges, data charges and texting charges). The Company may require an Employee to repay charges incurred by the Employee in using the Company's telephone for personal purposes.

Mobile telephones provided to Employees for work purposes remain the property of the Company, and Employees are responsible for their security and condition. Loss of a Company mobile telephone must be reported immediately.

Email

The Company provides Employees with access to email. Unless otherwise provided an exemption by the Chief Executive Officer ("CEO"), Employees must not use personal email, text messaging or instant messaging systems for work purposes. Employees should always consider whether email, text messaging or instant messaging is the appropriate method for a particular communication, as opposed to communication in person, by telephone, or by another form of electronic messaging.

Passwords. This policy's rules regarding passwords apply to use of the Company's email systems.

Email. Employees must use secure encrypted email provided by the Company to protect the Company's confidential information sent via email. Employees should access their work emails at least once every working day, stay in touch by remote access when traveling in connection with work, and use an out of office response when away from the office for more than a day.

Message Content. Employees must not send abusive, obscene, discriminatory, harassing, derogatory, defamatory, or otherwise inappropriate messages via email, text message or instant message. Anyone who feels that they have been harassed, bullied, or threatened, or who is offended by material received from a colleague in this manner should inform their manager.

Employees should take care with the content of emails, text messages or instant messages. Incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Employees have no control over where a message may be forwarded by the recipient and should avoid saying anything that would cause offence or embarrassment if it were forwarded to colleagues or third parties, or if it were made public.

Deletion. Emails may be disclosed in legal proceedings in the same way as paper documents. Deletion from an Employee's inbox or archives does not mean that a message cannot be recovered for the purposes of disclosure. All messages should be treated as potentially retrievable, either from the Company's main server or using specialist software.

General Rules. Employees should:

- Inform the sender of a message when the Employee receives a message intended for someone else.
- Respect the privacy of others by using the "Bcc" address line in email when appropriate.
- Review the content and recipients of a message before sending it.
- Label messages appropriately to indicate their sensitivity (e.g., "For Internal Use Only").

Employees should not:

- Send or forward personal messages through the Company's systems which the Employee would not want the Company, a co-worker, or a third party to read.
- Send or forward spam, chain mail, junk mail, cartoons, jokes or gossip.
- Contribute to system congestion by sending trivial messages, copying or forwarding emails to those who do not have a real need to receive them, or using "reply all" unnecessarily on an email with a large distribution list.
- Sell or advertise using the Company's communication systems or broadcast messages about lost property, sponsorship or charitable appeals.
- Agree to terms, enter into contractual commitments or make representations by email, text message or instant message unless appropriate authority has been obtained from the Company. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter.
- Send messages from another person's email account, mobile telephone or instant messaging account (unless authorized) or under an assumed name.

Internet Use

Internet access is provided through the Company's IT and communications systems primarily for business purposes. Occasional personal use may be permitted as described in this policy.

Employees should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive or in bad taste. Even web content which is legal in Canada may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Employees must not use the Company's systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even on the Employee's non-working time, unless authorized to do so in performance of the Employee's duties.

Personal Use of IT and Communications Systems

Personal use of the Company's IT and communications systems (including work email, internet access, and telephones) is permitted subject to the following rules:

- Use must take place substantially outside normal working hours.
- Use must not involve unprofessional or inappropriate content.
- Use must not interfere with an Employee's work responsibilities or productivity.
- Use must not incur costs for the employer.

Personal use of the Company's IT and communications systems may be monitored as described in this policy. Employees should have no expectation of privacy in the use of the Company's IT and communications systems for personal purposes.

The Company may, at its discretion, prevent access to certain telephone numbers, internet sites or other electronic communications if personal use is considered excessive, unprofessional, harassing or abusive.

Monitoring

The Company monitors the access and use of its IT and communications systems, including its computer networks/telephones/email/text messaging/instant messaging/voicemail/internet use as reasonably required to protect its business interests and to meet its legal obligations. These purposes include, but are not limited to:

- Protecting the integrity of the Company's IT and communications systems. This includes protection against computer viruses, damage to software or hardware, loss of the Company's documents or information, and protecting against excessive telephone or computer usage.
- Protecting against unauthorized access or disclosure of the Company's confidential information, proprietary information, or Employee or third party personal information in the Company's control.
- Protecting Employees against discriminatory, harassing or violent behavior from co-workers or third parties.
- Monitoring the use of email and telephone systems to ensure that use is in accordance with this policy.
- Finding lost messages or data, or to retrieve messages lost due to computer failure.
- Assisting in investigations of alleged wrongdoing or violations of employer policies.
- Complying with any other legal obligation.

To achieve these purposes, the Company may access, intercept or review any information created on, transmitted to, received or printed from, or stored or recorded on the Company's IT and communication systems. Monitoring may include, without limitation, the interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of IT and communications systems, including installation, removal or alteration of software or hardware.

The Company may store copies of such data and communications acquired through monitoring for a period of time after they are created and may delete such copies from time to time without notice.

Employees should have no expectation of privacy in any content created, transmitted, received, accessed or stored on the Company's IT and communications systems. Employees should not use the Company's IT and communications systems for any matter that the Employee wants to be kept private or confidential from the Company.

While Employees should have no expectation of privacy in the use of the Company's IT and communications systems, any Employee personal information collected in the process of monitoring will be used or disclosed only as required to protect the Company's business interests and to meet its legal obligations.

Prohibited Use

Employees are prohibited from using the Company's IT and communications systems for any inappropriate or illegal purpose. This includes but is not limited to:

- Any purpose that violates the Company's policies.
- Excessive use that interferes with the Employee's job duties.
- Disclosing the Company's confidential or proprietary information, or that of a third party, including third party personal information in violation of law or the Company's policies.
- Any use that violates the intellectual property rights of third parties.
- Carrying out illegal activities.
- Representing your personal views as those of the Company.
- Online gambling.
- Forwarding spam.
- Creating, viewing, accessing, transmitting or downloading any inappropriate material, including:
 - pornography;
 - offensive, obscene, or criminal material;
 - material which is likely to cause embarrassment to the Company or to our clients;
 - false and defamatory statements about any person or organization;
 - material which is discriminatory, derogatory, or which promotes hatred or violence;
 - any information in breach of copyright;
 - confidential information about the Company, its Employees, or its clients (except as authorized in the proper performance of an Employee's work);
 - any other information which is likely to create criminal or civil liability for the Company or the Employee.

Where evidence of misuse is found, the Company may undertake a more detailed investigation, involving the examination and disclosure of monitoring records to those appointed to undertake the investigation and to any witnesses or managers involved in Employee discipline. If necessary, such information may be provided to the police in connection with a criminal investigation.

Consequences for Failure to Comply

Any violation of this policy may be grounds for disciplinary action, up to and including termination of employment.

Administration of This Policy

The Company expressly reserves the right to change, modify or delete the provisions of this Information Technology Policy without notice.

If the Company does not have a CEO, then "CEO" shall be replaced by "President" in this document.

Acknowledgment of Receipt and Review

I, _____ (Employee name), acknowledge that on _____ (date), I received a copy of the Company's Information Technology Policy, and that I read it, understood it and agree to comply with it.

Date: _____

By: _____
(signature)

Name: _____
(please print)

Job Title: _____