INFORMATION TECHNOLOGY POLICY

1 PURPOSE

Evrim Resources Corp. (the “Company”) has adopted this Information Technology Policy (the “Policy”) to provide guidelines for employees, directors, officers and others to govern use of information technology resources within the Company.

2 SCOPE

The corporate information systems, data, and computing assets, which include but are not limited to computers, computer networks, printers, and other related pieces of equipment and/or systems, are the property of the Company and are valuable corporate assets. Individuals using and having access to these corporate assets must take reasonable and prudent steps to preserve the integrity of the systems and their data and to protect the assets. These assets are to be used for appropriate business-related functions only.

All communications emanating from the Company or made and transmitted in the Company’s name shall be professional in nature as they represent the corporation, its employees, board of directors, and those individuals it serves.

3 AUTHORITY AND RESPONSIBILITY

All Information Technology (“IT”) requests must be reported to the IT Coordinator, as designated by the CEO, for resolution by the information services contractor (IS Group).

4 GUIDELINES

a) Assets and modifications to information assets:

Corporate information assets include but are not limited to the hardware, software, and data that make up the client workstations, laptops, tablets, local area networks, wide area networks, smartphones, telephones and other communication systems. All information services (IS) acquisitions will be managed by the IS Group. Accordingly all changes, modifications, and alterations to computing assets must be made by, or in consultation with, the IS Group.

b) Physical security and loss prevention:

Reasonable and prudent steps should be taken to protect corporate data and corporate information systems. At no time should these steps be breached, evaded, bypassed, or circumvented.

All removable devices should be carried with due care and attention to the possibility of unauthorized access or physical loss of the asset. Lost or stolen assets should be immediately reported to the IT Coordinator.
c) Access and password controls:
Corporate data and corporate information systems should only be used as authorized by executive management and/or the IT Coordinator. Access to corporate data and corporate information systems should conform with an individual's job function and/or description.

- Data security and confidentiality procedures are an indispensable and integral part of the information system policies and procedures. These procedures may include but are not limited to the granting and prudent administering of passwords.
- Corporate data must be protected from negligent and intentional damage. Recovery from this damage is imperative if the Company is to operate without business interruption.

Any action which breaches, evades, or circumvents these reasonable and prudent steps should be immediately reported to the IT Coordinator. Failure to report these actions is a violation of policy and subject to disciplinary action.

d) Backup and anti-virus protocol:
The IS Group shall develop, implement, and be responsible for redundant backup systems that ensure the safe and effective storage of critical corporate data. The IS Group shall also develop and implement an anti-virus protocol meant to protect data and data systems from software that can damage or otherwise corrupt the Company's data and data systems.

Protocols will be reviewed on an annual basis or more often as required by hardware or software modifications.

e) Data ownership:
The corporate information systems, data, and computing assets are the property of the Company and are valuable corporate assets and must not be considered private.

f) Data storage:
Each employee is responsible for ensuring that data, which they generate, is properly stored on the servers. Any data stored on laptops, desktops or portable media shall be transferred to the appropriate permanent storage location as soon as possible.

g) Internet and internet services:
The Internet may only be used for purposes that benefit the Company and that are directly applicable to an individual's role within the Company and authority. The Internet may also be used to conduct personal business that is reasonable and usual during the course of a business day.
The Internet or Internet connections shall not be used to transfer information that is in violation of or contradicts the intent or spirit of these policies or procedures.

The Internet must not be used for commercial purposes outside those directly related to or benefiting the Company.

Recognizing that use of the Internet, and in particular the content that can be printed and copied from it, can reflect negatively on the Company, use will be made of the Internet with the sole purpose of benefiting the Company.

The Internet may not be used to access other systems for which the user has no authorization.

h) Electronic mail:

E-mail is a corporate resource and may be used solely for purposes that directly benefit the Company or that relate to an individual’s role in the Company and authority.

E-mail may not be used:
- to provide corporate information or corporate performance information without prior written consent of Corporate Disclosure Officers, or
- to distribute material that contradicts or is in violation of these policies, or
- to conduct personal business beyond what is reasonable and usual during the course of a business day.

5  RIGHT TO MONITOR

The Company reserves the right to monitor use of IS assets, audit, screen, and preserve data as it deems necessary in to maintain compliance with corporate policy. The company reserves the right to review the content of files (corporate or otherwise) maintained and/or accessed through the network. In addition, network backup devices and client drives, or client backup devices are also subject to this audit/screening.

The Company reserves the right to monitor e-mail use and review the content of all messages and files on the e-mail system. In addition to the Company’s access and use, e-mail information is also subject to review by law enforcement or government agencies; as this information may be used and accessed during investigative review.

6  CONSEQUENCES

Violation of the Policy or misuse of corporate assets is subject to disciplinary actions including but not limited to the loss of applicable corporate privileges or more severe disciplinary actions including employment termination.

Should an individual become aware of a violation of this policy, he or she should consult with management or the Company’s external legal counsel. In addition, violations may be reported to the other contacts listed in the Company’s Whistleblower policy.