Atlas Consolidated Mining and Development Corporation

CYBER SECURITY POLICY

1. Purpose

The purpose of this Policy is to preserve the security and confidentiality of the Corporation's Data and Information; implement process in times of disruption; avoid security breaches; set up protocols during disaster recovery and identify risks to mitigate or avoid a great financial damage to the Company and its reputation that may be caused by human errors, hacker attacks and system malfunctions.

2. Scope

The Policy applies to all Directors, Officers, Employees, Contractors, Seconded Employees, Volunteers, and Anyone who has permanent or temporary access to the Company Network Systems.

3. Security Protocols

The Corporation's Confidential Data and Information are valuable. Covered Persons are obliged to protect these data and information. Hence, to avoid security breaches, Security Protocols shall be implemented which include but are not limited to the following:

a. Lock down of port security through mac address filtering by static entry of mac address.

b. Lock down of USB access with exceptions as may be determined by reason of government mandated transactions and indispensable Company operation.

c. Lock down of read and write access to removable media devices.

d. Non elevation of user access or system administration rights to all users and devices under the Company domain except the Information Technology (IT) Department.

e. Prohibition and prevention of noncompany owned computer devices to connect to the Company's local network range.

f. Blocking of websites not necessary for Company operations including social media sites.

g. Installation of updated anti-virus and firewall software.

h. Prohibition on logging into Company accounts and systems through unsecure and private networks.

i. Prohibition on accessing internal systems and accounts from other people's device or lending their own device to others.

j. Orientation and briefing for new hires in protecting their devices as well as constant updates on new scam emails or viruses and ways to combat them.

k. Prohibition on accessing, opening or clicking of suspicious attachments, links and websites specially if offering clickbait titles like prizes or advice as well as total ban of downloading suspicious, unauthorized, illegal, unlicensed software, movies, songs, games using Company equipment and device.

l. Checking of email and names of people to ensure legitimacy and reliability. Ensure that recipients of the data or information are authorized people or organizations and have adequate security policies. In the event of inconsistencies, giveaways or suspicious and unsafe email or messages, Covered Persons are required to seek the IT Department's assistance.

m. Changing of passwords regularly, password secrecy and implementation of password with at least eight characters including capital, lower-case letters, numbers and symbols. Writing of password is discouraged. Reporting and changing of account passwords at once when device is stolen or damaged.

n. Prohibition on transferring sensitive data and information to other devices or accounts unless necessary. Sharing of such must only be done over Company network or system and not over public Wi-Fi or private connection.

o. Turning off of screens and locking of devices when leaving desks specially when working outside Company premises and prohibition of posting of pictures in social media sites and other platforms that may reveal or leak Company sensitive data and information.

p. Reporting of scams, privacy breaches and hacking attempts to the IT Department, which in turn will endorse the same to Risk Management.

q. Arranging for Cyber Security Training for all Covered Persons and engaging of Cyber Security Consultant.

r. Remote accessing is strictly and exclusively for IT Department only unless permission is given to Covered Employee. Strict Implementation of data encryption, protection standards and settings and securing of private network must be observed.

4. Breach Protocols

The following shall be enforced in accordance with applicable laws and policies, and in the best interests of the Company with the objective of identifying, containing and combating any security breach:

a. Activation of a taskforce comprised of the IT Department, Risk Management, End Users and Technical Experts and the pre-determined response protocol in place such as lockdowns as soon as the breached or threat has been verified to protect the data or information that have not been affected, suppress the immediate threat, restore operations and recover from such disaster.

b. Reporting to the Board and call for emergency meeting if the situation warrants. Issuing of official statement may also be done if necessary.

c. Assessment of context (intentional or inadvertent), extent and severity of breach to identify who and what have been affected and how can such affect the company or its victim.

d. Carrying out a thorough post-breach audit to improve security practice, determine and punish who may be responsible and avoid future breaches.

e. Implementation of new and improved security and breach protocols.

5. Disciplinary Actions

All Covered Persons who cause security breaches shall face disciplinary action. Intentional, repeated or large scale breaches which cause severe financial or other damage shall have severe disciplinary action up to and including termination. Covered Persons who disregard the Company Security instructions will face progressive discipline, even if such has not resulted in a security breach.

.

6. Miscellaneous

This Policy has been adopted by the Board Directors (Board) of AT and any material amendment to the terms of this Policy must be approved by the Board. This Policy shall take effect upon approval by the latter and shall apply prospectively. The same shall be reviewed by the Board annually.