COLORADO RESOURCES LIMITED

(the "Corporation")

SOCIAL MEDIA & CYBERSECURITY
(the "Policy")

(Adopted by the Board of Directors on February 27, 2020)

Contents

1. INTRODUCTION

At Colorado Resources, we are passionate about what we do every day. We believe in open communication. We encourage our employees to share their passion in appropriate and respectful ways. This may be on different internet platforms such as online social networks, emails, blogs, or wikis. These platforms may change how we communicate with our colleagues, superiors, partners and customers. In order to avoid misunderstandings and problems arising, all Directors, Officers, Contractors and Employees ("Individuals") should adhere to the following policy while using any internet platform that is in association with the Corporation.

Cyber crime is becoming more commonplace. It is essential to take steps to protect the Corporation's data, technology, information and intellectual property as it represents a significant portion of our Shareholder's investment.

2. APPLICATION OF POLICY

This policy applies to all directors, officers and employees of the Corporation and its subsidiaries. The Board of Directors may delegate its responsibilities for setting the standards of this policy and for overseeing and monitoring compliance with the policy, but the Board retains ultimate responsibility and ownership of its successful implementation. Individuals are required to read and accept the contents of this policy by signing the Acknowledgement Certificate in Appendix A.

3. MONITORING OF COMPLIANCE AND WAIVERS

The CEO is responsible for monitoring compliance with this Code. A waiver of this Code will be granted only in exceptional circumstances. Any waivers from this Code that are granted for the benefit of the Corporation's directors or executive officers shall be granted by the Board of Directors only. Any waiver for employees will be granted only upon approval by the Chief Executive Officer.

4. INFORMATION AND COMPUTER RESPONSIBILITY

If you have access to Corporation computing and communication devices, you are expected to use them in a responsible manner for the benefit of the Corporation. Whether you work in an Information Technology capacity, are a member of the management team or simply use computing and communication devices to do your job, you should ensure that they are used appropriately and with care. While incidental personal use may occasionally occur and is acceptable, these resources are intended for Corporation benefit and use.

Do not disclose your computer system passwords and/or user identification to anyone except in accordance with Corporation policy. You must not use personal software on Corporation systems and must adhere to all applicable software licensing agreements when using our computer and communication systems.

5. EMAIL AND INTERNET USE

Corporation computer systems, data, programs and communication systems are the property of the Corporation.

Individuals cannot use their professional e-mails for personal use. Business e-mails are the property of the Corporation and under no circumstances can be deleted. They are not to be forwarded to anybody outside of the Corporation and are to remain confidential. We are able to monitor and record all email, internet use and files stored in private areas of our network. You should at no time expect privacy when using our computing resources – whether you are accessing them on site or from a remote location (e.g.

by employees from home). The Corporation reserves the right to monitor and review any material created, stored, sent or received on our network. As an employee, officer or director, you are encouraged to use the Corporation's proved internet resource when it is appropriate for business purposes. However, the infrastructure required to provide this access represents a sizeable commitment of our resources. You should avoid unnecessary and/or inappropriate internet use as it causes network and server congestion, additional costs and puts our computer resources at risk. For these reasons, you may not use the internet for personal, non-work related activities including viewing and/or distributing illegal, offensive or pornographic material.

6. USE OF SOCIAL MEDIA

Individuals are not to comment, discuss, or refer to any material information while posting online. Individuals are not to comment on any legal matters unless they are an official spokesperson for the Corporation, meaning there is legal approval by Colorado. The following information may be considered to be "material information" and must remain confidential:

(a) Any issuance and changes to Corporation securities affecting control of the Corporation;

(b) any capital reorganization;

(c) any significant acquisitions or dispositions;

(d) any changes in capital structure;

(e) any borrowing or lending of funds;

(f) exploration results (pending or actual);

(g) any new developments that my affect the Corporation's markets;

(h) entering into or the loss of any significant contracts;

(i) any changes in capital investment plans or corporate objectives;

(j) any significant change in management;

(k) any significant litigation;

(l) any significant labour dispute or any dispute with a contractor or supplier;

(m) any material changes in the business, operations, or assets of the Corporation;

(n) any declaration or omission of dividends;

(o) any oral or written agreement to enter into any management contract, investor relations agreement, service agreement, or related party transaction.

(p) Any and all photos taken on Colorado properties, even if on personal devices (i.e. cell phones), are the property of the Corporation. They are not to be posted to any social media platforms unless by a social media manager.

7. ONLINE CONDUCT

Individuals must familiarize themselves this policy along with the Corporation's other policies including the Code of Business Conduct & Ethics and the Employees & Contractors policy; and also their signed

Confidentiality Agreement.

Just as in the Employees & Contractors policy, any disrespectful conduct while online such personal insults, comments of discrimination based on appearance, race, gender, age, religion, sexual orientation, disability, or any other legally protected categories is strictly prohibited and will result in immediate and severe consequences.

Individuals should use professional judgment while online and must not represent the Corporation in an untrue or misleading way. Individuals are personally responsible for the content that they post online. It should be made clear that any ideas and opinions of the individual are that of the individual and not of the Corporation. Under no circumstances are any individuals to post on behalf of the Corporation unless they are a designated social media manager or have consent from such person.

Individuals should make sure that any personal online profile that may be associated with the Corporation (Facebook, Linked-In, Instagram, etc) should appear how they would like their clients, colleagues and superiors to perceive them.

Individuals are to be aware of any copyrights or ideas that are not their own. Words of another individual are to be properly referenced and used only under the permission of the author.

Individuals should remember that while using property of the Corporation, such as Corporation computers and the Colorado internet network, activity may be monitored and recorded.

8. CYBERSECURITY: DEVICE SECURITY

Logging in to any of Corporation's accounts using personal devices such as mobile phones, tablets or laptops, can put the Corporation's data at risk. Therefore we do not recommend accessing any of the Corporation's data from personal devices. If Individuals chose to use personal devices to access the Corporation’s confidential data and information, employees are obligated to keep their devices in a safe place, not exposed to anyone else.

The following recommendations are considered best practice:

(a) Keep all electronic devices' password secured and protected

(b) Logging into company's accounts should be done only through safe networks

(c) Install security updates on a regular basis

(d) Upgrade antivirus software on a regular basis

(e) Don't ever leave your devices unprotected and exposed

(f) Lock your computers when leaving the desk

9. CYBERSECURITY: EMAIL SECURITY

Emails can carry scams or malevolent software (for example worms, bugs etc.). In order to avoid virus infection or data theft, our policy is always to inform employees to:

(a) Abstain from opening attachments or clicking any links in the situations when its content is not well explained

(b) Make sure to always check email addresses and names of senders.

(c) Search for inconsistencies

(d) Be careful with clickbait titles (for example offering prizes, advice, etc.)

In the case that an Individual is not sure if the email received, or any type of data, is safe, they should contact our management.

10. CYBERSECURITY: MANAGING PASSWORDS

To avoid passwords getting hacked, use these best practices for setting up passwords:

(a) At least 8 characters (must contain capital and lower-case letters, numbers and symbols)

(b) Do not write down password and leave it unprotected

(c) Do not exchange credentials when not requested or approved by supervisor

(d) Change passwords every [x] month

11. CYBERSECURITY: TRANSFERRING DATA

Individuals must only share data over the Corporation's network. Where confidential information must be shared by other means, it must be encrypted and shared only be a secured mechanism that is compliant with all applicable data sharing rules and regulations including data protection laws. Individuals should contact management for guidance before sharing any data or information in an unsecured form.

12. CYBERSECURITY: WORKING REMOTELY

Individuals may work remotely with written permission of the Corporation's management and provided it is conducted in compliance with the Corporation's policies.

13. DISCIPLINARY ACTION

When best practices and the Corporation's policies are not followed, disciplinary action may result. In cases of intentional or repeated breaches, this may result in serious consequences including termination and the Corporation may seek damages.

APPENDIX A – ACKNOWLEDGEMENT CERTIFICATE

I, the undersigned, declare that I have read and understood the Corporation's Social Media & Cybersecurity policy and its related policies. I acknowledge and agree to comply with the Social Media & Cybersecurity policy and amendments thereto, provided such amendments have been brought to my attention.

Name _____

Employee Number _____

Signature_____ Date _____