ALEXCO RESOURCE CORP.

(THE "COMPANY")

CYBER SECURITY POLICY

1. Introduction

Alexco Resource Corp. and its subsidiaries ("Alexco" or the "Company") are committed to achieving the highest level of protection from internal and external cyber security threats. The Company has implemented and will continuously review and improve its governance, policies, and practices to:

a) Ensure business continuity, including the recovery of data and operational capabilities in the event of a security breach;
b) Ensure compliance with all applicable laws, regulations, and Alexco's policies, controls, standards and guidelines;
c) Comply with requirements for confidentiality, privacy, integrity for Alexco's employees, contractors, vendors, and other users;
d) Establish controls to protect Alexco's information and information systems against theft, abuse, and other threats;
e) Instill a culture of responsibility for, ownership of, and knowledge about information and cybersecurity amongst our workforce, contractors, and administrators;
f) Ensure the protection of Alexco's data and information infrastructure;
g) Ensure the availability and reliability of the network infrastructure, systems, and services; and
h) Ensure that external service providers are made aware of, and comply with, Alexco's information security needs and requirements, and continuously assess whether they maintain acceptable cyber security protocols.

2. Purpose

The purpose of this policy is to outline the Company's requirements and provisions for preserving the security of our data and information technology and infrastructure.

The more we rely on technology to collect, store, and manage information, the more vulnerable we become to security breaches. Human error, attacks, and system malfunctions can damage and jeopardize our Company's reputation and significantly affect our operations. For this reason, we have implemented a number of security measures to help mitigate security risks, which are included in this document.

3. Scope

This policy applies to all full-time and part-time employees of Alexco, and to its directors, independent contractors, consultants, vendors, suppliers, agents, and other users of Alexco's Information Technology ("IT") resources and infrastructure (together referred to as "Users"), wherever they may be located. It is the responsibility of the Users to familiarize themselves with this policy and to abide by its provisions.

Any breach of this policy is a serious offence and will result in the consideration of sanctions up to and including termination of employment, contract or legal action.

4. Governance and Management Responsibility

Cyber security is a strategic matter for Alexco. Assessment and management of cyber security risks is routinely conducted by the CFO and VP, Finance together with external IT expert consultants retained by Alexco (the "IT Department").

The development, implementation, and communication of cyber security plans and initiatives at the Company are the responsibility of the CFO and are managed on a day-to-day basis by the VP, Finance. Cybersecurity risks and incidents are communicated in reports and updates to senior management immediately, and depending on the severity of the incident and at recommendation of the CEO, immediately communicated to the Board of Directors. At least annually, annual reports to be provided to the Board on cybersecurity systems and improvements thereto.

Cyber security must be considered by all levels of leadership where changes to business processes are made, including but not limited to, the information and technology environment. Appropriate protective measures must be undertaken at all times.

5. Authorized use of Alexco's IT infrastructure

Alexco provides access to information technology to Users, including the internal environment, information sharing tools, the internet, and social media among others, within the scope of their respective roles within the Company. Alexco prohibits use of IT resources for any purpose other than business, unless otherwise stated in this policy.

All Users must behave responsibly with respect to the intended business use of technologies and comply with software licenses, property rights, user agreements, confidentiality, and legal rights. Users must comply with Alexco's Code of Conduct, corporate policies, and all applicable laws when using Alexco's information technology resources, including without limitation, privacy and intellectual property laws.

Limited personal use is acceptable provided that it does not affect job performance and if the User adheres strictly to this policy. The Company's systems must not be used for the creation or distribution of any material considered threatening, abusive, defamatory, unlawful, sexually explicit, racist, discriminatory, or fraudulent, or that could potentially breach the corresponding software license agreement. Alexco restricts all Users from using the Internet to perform any task contrary to the law or knowingly accessing websites with content that is illegal, obscene, or hateful.

To maintain the integrity of Alexco's corporate image and reputation, to ensure effective and efficient operations, and to prevent the unauthorized or inadvertent disclosure of sensitive, confidential or personal information, Users must exercise caution and care when using any system, service or technology platform, both internal and external, including email or third party services, such as Cloud-based and social media. Personally identifiable information ("PII"), which is any data that could identify a specific individual, should not be transmitted via email or shared using any other service or technology platform without written approval by the appropriate site, corporate human resources, or finance department. For clarity, a description of PII is provided in Appendix I.

Users must also exercise caution against suspicious messages and technologies, which are often intended to bait a user into a malicious cyber event.

6. Passwords

Users are responsible for generating and utilizing effective passwords and for keeping those passwords secret and secure. Users must not appropriate, use or disclose someone else's login or password without

prior authorization by the employee's supervisor or human resources. In addition, employees must make their best efforts to ensure that the function of retaining passwords by Company computers is disabled. The IT Department will support the mechanisms that evaluate the strength of passwords and define the password change frequency for all applications, services and devices supported by the Company, along with other mechanisms to strengthen the way Users identify themselves when accessing the Company's IT resources, such as multifactor authentication. Password requirements will be adhered to as per current SOX controls, with specific conditions for length and regular changes to passwords. This will be reviewed annually by the IT Department.

7. Confidentiality

Alexco prohibits the release of confidential information to any third party, or use of confidential information, except as required in the performance of Company-related work approved by the employee's supervisor and in accordance with the terms of the applicable confidentiality agreement.

8. Privacy

Users should have no expectation of personal privacy in anything they create, store, send or receive by e-mail or when using any corporate application if they use equipment (e.g. mobile device, computers) owned or provided by Alexco. The nature of Alexco's business requires effective monitoring of activities on Alexco's network, including the conduct of Users. The Company reserves the right to review and collect all information contained in e-mails, whether or not stored solely in personal folders on the computer operated by the User, and in all equipment owned or provided by Alexco.

9. Ownership

Data and employees' work and work products belong to Alexco, including all messages, sent or received regardless of the device or application used to produce, send or receive it.

10. Security

Used unwisely, the internet can be a source of security problems that can do significant damage to the Company. Users must:

- Apply best practices to prevent any form of computer virus, Trojan, spyware or other malware from accessing the company's environment. A list of actions to prevent this from occurring, which every employee must be aware of and followed is provided in Appendix II. While this list is not exhaustive, it is illustrative of the burden of care that every employee agrees to accept in helping ensure the security of the Company and its IT environment.
- Only access websites, applications or systems for which they have authorization, either within the Company or outside it.
- Only use approved services for the uploading or sharing of Company data. A list of approved sources is provided in Appendix III.

This list is not exhaustive and is subject to revision, so prior to using any such service not on this list, employees should confirm in writing with the IT Department whether it is approved.

11. Awareness, Communication, and Training

New Employees

To mitigate the risk of unintentional disclosure of confidential information by employees, the human resources department will refer newly onboarded employees to this policy and will require formal acknowledgement that it has been read, is understood, and will be followed. In addition, acknowledgement of this policy, that it is understood and that the employee agrees to follow it will be included in the annual sign off along with the code of conduct.

Departures and/or changes in employment status

Upon a change in status, including promotion, transfer, or termination of employment, the human resources and finance departments are accountable for ensuring that the IT Department is advised so that the employee's network and physical access privileges are modified as appropriate in a timely manner.

Third Parties

Vendors, suppliers, partners, contractors, service providers, or customers with connectivity to Alexco's internal network or access to the Company's data must comply with this Policy and the policy governing system access by third parties and information sharing services attached as Appendix III.

12. Information Risk Management

The Company has developed, maintains and periodically reviews an inventory of major types of information and systems on the basis of criticality to the business. This list, on a priority basis, is used to formally assess the degree of cyber protection that the Company has, the target degree of protection, as well as the plans that are in place to achieve the target level as appropriate. The target level will reflect the nature of the information or application, as well as the acceptable risk appetite for Alexco.

Business Continuity

The IT Department is responsible for the development and communication of standards and guidelines for acceptable IT related business continuity and disaster recovery plans. Business continuity and disaster recovery plans have been developed and the IT Department is responsible for developing and updating a continuity plan for the overall IT environment, including data backup and recovery.

To prevent the deployment of software and IT equipment that could compromise the security of the entire information technology infrastructure, the IT Department will establish standards for the development, acquisition, or installation and approval of all new software and major equipment purchases. No software should be installed on Company-owned devices unless approved by the employee's direct supervisor and the IT department. Alexco installs only properly authorized and licensed software and prohibits any installation or use of unauthorized, unlicensed or illegally copied software.

To protect from changes that could compromise Alexco's operations, the IT Department will enforce standards for the approval and deployment of changes to the information technology infrastructure and environment as well as the implementation of any new applications of any type. These standards, require, amongst other provisions, that all changes be appropriately governed and managed – and must be tested, documented, with risks to cyber security, business, technical, and

legal considered, and have user acceptance documented before being installed in the production environment. The approved deployment plan must include rollback and contingency procedures.

Viruses and Malware

To defend the Company from computer viruses and malware, all computers and devices connecting to Alexco's infrastructure must be approved devices and have the standard, authorized anti virus and malware protection software installed. It is responsibility of the IT Department to keep this software updated and of users to report to the IT Department any sign of infection. To further enhance security, personal email is not to be accessed, either through the web browser or applications, on Company laptops or computers. It is acceptable to sync tablets and mobile phones to personal email accounts as these devices do not access the Company network.

Remote Access

Users must secure their remote access credentials. 'Save Password' options should not be used. Users must assume remote networks, such as home based, public wireless hot spots, etc., are unsecure and therefore Users should adhere to the best practices and procedures laid out by the IT Department, including, but not limited to the Bring Your Own Device (BYOD) described in this policy to prevent interceptions, eavesdropping, unauthorized access, or direct attacks that could risk the integrity of the overall network.

Lost Devices

To prevent the disclosure of confidential information in lost or stolen devices, the IT Department implements encryption and other security mechanisms to dynamically protect Alexco's data. The User is responsible for taking appropriate precautions to prevent damage to, loss or theft of any device issued to them or approved for use by them. Each User must report immediately to their supervisor and to the IT Department any lost or stolen devices and any suspected or confirmed breaches of those devices. The IT Department will take the required measures to wipe remotely, where possible, any Alexco data still hosted on the lost device. If the User's device is lost, stolen or upon termination, the IT Department will wipe the device, which may include user's private information. It is not the responsibility of Alexco to recover any personal data or media from a lost or stolen device.

Disposal of Company Electronic Devices

The last stage in the life cycle of electronic devices involve the appropriate, secure, and sustainable disposal of all devices being retired. The IT Department is responsible for collecting and documenting the disposal of outdated or damaged devices including desktops, laptops, tablets, monitors, mobile phones, telephones, and other electronics and accessories to be disposed of.

The IT Department will select and coordinate the use of a certified service or supplier to have all devices inventoried and comprehensively wiped with a unified endpoint management solution before being recycled to minimize both the risk of unintended disclosure of confidential information and possible environmental impacts.

Bring-Your-Own-Device (BYOD)

Users must obtain the written approval of the IT Department before using any personally owned device to connect to or access Alexco's systems or network.

Equipment

Users are responsible for the hardware assigned to them. Relocations and transfers of equipment must be approved in writing by the IT Department.

VPN

In order to protect corporate data while using public networks, the IT Department, where required, will provide and support secured remote access, including Virtual Private Networks (VPN). Only Company or approved BYOD issued devices will be configured with VPN (or equivalent) access. Users with VPN credentials are responsible for maintaining their confidentiality according to the password provisions of this policy.

Incident management

To promptly respond to threats, Users are expected to communicate security incidents to the IT Department immediately. Security incidents include any violation of this Cyber Security policy that compromises corporate data. The IT Department is responsible for the channels and procedures that guarantee that security incidents are identified, contained, investigated, and remedied.

Legal and Compliance

Alexco will regularly assess developments within the Company and the environment, and ensure the promulgation of corporate-wide policies for:

- Cyber security management;
- Management of third party's access to the Company network; and
- Other policies as required to ensure minimum standards of care are taken by the organization to protect against cyber threat.

Cyber risk will be monitored and be included in the report to the Board of Directors annually. All contracts for the provision of cyber related services to the Company should be reviewed by a member of Senior Management to ensure that Management has the understanding of residual risks for purposes of making relevant business decisions.

Issue Date: April 26, 2021

Appendix I

Personally Identifiable Information ("**PII**") is any information that can be used to identify, contact, or locate an individual, either alone or combined with other easily accessible sources. It includes information that is linked or linkable to an individual, such as medical, educational, financial and employment information. Examples of data elements that can identify an individual include name, fingerprints or other biometric (including genetic) data, email address, telephone number or social security number. Safeguarding company-held PII (and other sensitive information) is the responsibility of each and every member of the workforce.

Regardless of your role, you should know what PII is, and what your responsibility is in ensuring its protection. Although society has always relied on personal identifiers, defining and protecting PII has recently become much more important as a component of personal privacy, now that advances in computing and communications technology, including the internet, has made it easier to collect and process vast amounts of information. The protection of PII and the overall privacy of information are concerns both for individuals whose personal information is at stake and for organizations that may be liable or have their reputations damaged should such PII be inappropriately accessed, used, or disclosed.

PII can also be exploited by criminals to steal a person's identity or commit other crimes. According to FBI statistics, identity theft continues to be one of the fastest growing crimes and can cause both financial and emotional damage to its victims. Due to this threat, many governments have enacted legislation to limit the distribution of personal information. The following list contains examples of information that may be considered PII:

- Name, such as full name, maiden name, mother's maiden name, or alias;
- Personal identification number, such as social insurance number (SIN), passport number, driver's license number, taxpayer identification number, patient identification number, and financial account or credit card number;
- Address information, such as street address or email address;
- Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well defined group of people;
- Telephone numbers, including mobile, business, and personal numbers;
- Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry);
- Information identifying personally owned property, such as vehicle registration number or title number and related information; andInformation about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information).

Sometimes, one or two pieces of information can be combined with other information to compromise someone's identity, even if the individual pieces of information seem harmless.

Appendix II

Best Practices to Prevent Cyber Security Threats

The following are best practices to be adopted by Alexco Users to prevent any form of computer virus, Trojan, spyware or other malware infection.

- Do not open emails from unknown senders;
- Don't click on any links within emails that seem suspicious or from unknown senders;
- Don't install any software on company issued computers without prior approval from IT department;
- Only open websites that you know. Never randomly click a link as it may direct you to a malicious website or trick you to download an infected file or program;
- When using USB flash drives, thumb drives or any other removable drives, make sure you scan them using your security software. Best practice is to ask the IT Department to scan if you're not sure;
- Limit the amount of information that is published on the internet about yourself or about Alexco. Public information can be used for social engineering;
- Report any suspicious computer activity to the IT Department immediately;
- Educate yourself on the protection systems that are installed on your computer and check if they are current on any alerts/updates;
- Never leave your computer unattended while outside the company offices or your home where anyone could plug in a USB device. As a best practice always log off or lock your computer session before leaving your computer unattended.

Appendix III

Approved Services for Secure Transfer or Sharing of Alexco Information

The following services have been approved for the transfer of Alexco information within and outside the Company:

- Alexco's Microsoft Sharepoint and Teams;
- Alexco's Dropbox for Business;
- Alexco's server's and email system;
- Alexco's data room
- Financial management accounting systems