INFORMATION TECHNOLOGY AND CYBERSECURITY POLICY

This Information Technology and CyberSecurity Policy (the "Policy") is meant to protect Altius Minerals Corporation data and infrastructure, outline guidelines that govern cybersecurity measures and define IT infrastructure usage.

The Policy applies to Altius, its subsidiaries and affiliates, and all employees and consultants of Altius.

Policy Scope

The policy applies to all stakeholders.

- Altius user access to IT infrastructure usage is provided to employees to facilitate productivity and assist them to effectively perform their duties and responsibilities within the company. Altius assigns laptops, cellular phones or desktops and associated hardware and software to its employees, and requires that the hardware and software be used for conducting company business. If an employee leaves voluntarily or involuntarily, the devices and any licensed software are expected to be returned to Altius IT unless specified in a written agreement that is signed by the departing employee and an authorized Altius employee. All users must respect the intended business use of technologies, and comply with software licenses, property rights, user agreements, confidentiality, and legal rights.
- Altius expects users to strictly comply with the company's Code of Conduct, policies, and all applicable law when using the IT resources. This also includes respecting privacy and intellectual property laws.
- Altius expects users to be responsible for creating unique passwords that are safeguarded against any inadvertent access. The minimum password length should be 8 characters with a minimum of three of the following mix of character types: uppercase, lowercase, numbers, and symbols. The password should not be identical to account name or email address. Passwords

are to be changed every 6 months but due to challenges related to COVID-19 quarantining and working from home, this part of the policy was suspended until resumption of normal office operations.

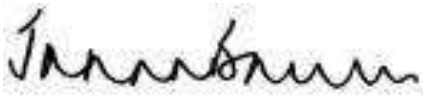
- Any data creation using Altius resources belongs to the company and cannot be used by or sent to any unauthorized parties.
- Altius IT infrastructure users are allowed to use removable media on computers. However, sensitive information should be stored on removable media only when required in the performance of assigned duties or when responding to legitimate requests for information
- Email usage by users should be treated in the same manner as any other form of communication. Users must exercise caution when sending email. Sensitive information must not be forwarded unless that email is critical to business. The content of e-mail should be in accordance to the conduct outlined in the code of business conduct by Altius.
- Users are encouraged to scrutinize all emails before clicking links or making responses. The IT manager from time to time sends out updates as to new phishing techniques and reminders to be vigilant. All users will defer to the IT manager if they receive an email they are suspicious of before they take any further action.
- The use of remote access Virtual Private Network (VPN) connections to facilitate data transfer between employees should be done under the guidelines of the existing IT processes. All accounting, investor relations, compliance, disclosure and due diligence information is expected to be stored on the company file servers to allow for company access. Third party consultants using Altius's VPN will have access to specific folders which is authorized by their direct supervisor and are expected to observe the same guidelines for file storage.
- Security breaches must be reported immediately to IT personnel. The issues must be documented including any follow-up after the incident.

- Altius uses an Endpoint Detection and Response software which is industry leading with respect to ransomware protection. All laptops, desktops, servers having access to the network have this software installed. It is constantly updated to the most current version using smart updates.
- Periodic review and audit of the IT infrastructure will be completed every 24 months by an independent external cybersecurity consultant. The frequency of audits will be evaluated and modified if necessary.
- Board members will be offered continuing education in cybersecurity in order to better understand and evaluate Altius's preparedness.
- Altius management leading IT infrastructure will be provided with opportunities for continuing education including annual conference attendance in order to educate management on on evolving cybersecurity risks.

REVIEW OF THIS POLICY

The Board recognizes that the policy is an evolving area in Canada and globally and will review this policy on a regular basis to ensure that it is effective in achieving its objectives and that the Corporation's practices continue to be representative of sound corporate governance practices.

Adopted by the Board of Directors on August 9, 2021.

Signed 

Executive Chair of the Board of Directors