CYBER SECURITY POLICY

Purpose

Endura Mining (**Company**) is committed to protecting its business information and systems in order to preserve its reputation and reduce the risk of negative events and incidents. This policy provides the basis for the Company's cyber security management and applies to all Personnel, information systems and information assets used by, or on behalf of the Company, including those managed or hosted by third parties

Definitions

"**Personnel**" shall mean:

- all directors, senior executives, employees and officers of the Company;
- contractors (including sub-contractors) occupying permanent or part time fixed term contracts;
- consultants or suppliers of goods or services and their staff; and
- third parties including intermediaries and associates.

"**Administrator**" shall mean the individual responsible for coordination of the Company's IT information systems.

Policy framework

Cyber Security Principles

All Personnel are required to:

- keep all electronic devices' passwords secure and protected;
- only log into accounts through safe networks and approved applications and software;
- install security updates and upgrade antivirus software as required by the Administrator;
- never leave devices unprotected and exposed, and lock all electronic devices when they are unattended;
- follow and apply the same cybersecurity policies and procedures when working remotely as would apply when working in the office;
- not attempt to turn off or circumvent any security measures; and
- report any security breaches, suspicious activities or issues that may cause a cyber security breach to the Administrator.

Device Security and Using Personal Devices

- All devices owned or provided by the Company must have an approved antivirus and fire wall software installed. This subscription is managed by the Administrator.
- Logging in to any work accounts on personal devices, such as mobile phones, tablets or laptops, can put Company data at risk. Use of personal devices must be approved by the Administrator.

Password Requirements

To avoid employee work account passwords being compromised, Personnel must:

- use a passphrase containing at least 8 characters (which must contain a mixture of capital and lower-case letters, numbers and symbols);
- not write down their password or leave it unprotected;
- not exchange credentials unless specifically requested or approved by a supervisor; and
- change passwords regularly or as directed by the Administrator.

Email Security

Emails can contain malicious content and malware. To reduce risk, Personnel should:

- not open attachments or click any links where content is not well explained;
- verify the email addresses and names of senders;
- search for inconsistencies;
- block junk, spam and scam emails;
- avoid emails that contain common scam subject lines such as prizes, products and money transfers; and
- contact the Administrator if they are not sure whether an email or type of data is safe.

Transferring Data

Data transfer is a common cause of cybercrime. When transferring data, Personnel should:

- avoid transferring personal information, such as customer data or employee information; and
- only share data over authorised and secure networks.

Acceptable Use

- User accounts on work systems are to be used for business purposes only and not for personal activities.
- Personnel are responsible for protecting all confidential information used and/or stored on their accounts. This includes their user logins and passwords. Personnel are prohibited from making unauthorised copies of such confidential information and/or distributing it to unauthorised persons outside of the Company.
- Personnel must not purposely engage in any activity with the intent to degrade the performance of the system, divert system resources to their own use, or gain access to Company systems for which they do not have authorisation.

Oversight and enforcement

The implementation of this policy will be monitored by the Head of People and Culture, and the Board will be provided with regular reports on progress and performance. The security and status of Company systems will be regularly checked and tested by a third-party IT consultant.

This policy will be subject to regular periodic review which as a minimum will be conducted annually.