CYBER SECURITY POLICY

Introduction

1.1 Cyber security has been identified as a major risk for the Company and every employee and contractor needs to contribute for us to remain secure.

1.2 The Company has invested in technical cyber security measures, but we also need our employees and contractors to be vigilant and act to protect the Company IT systems.

1.3 This Policy provides information about your role in keeping the company secure.

1.4 Please contact the CEO/Managing Director if you have any questions about cyber security.

1.5 If you are an employee, this Policy forms part of your employment contract. Any breach of this Policy shall constitute a breach of contract.

1.6 If you are a contractor, this Policy forms a part of your contract of engagement. Any breach of this Policy shall constitute a breach of contract.

Cyber security requirements

2.1 You must:

(a) choose strong passwords (the company's IT team advises that a strong password contains a combination of characters, symbols and numerals);

(b) keep passwords secret;

(c) never reuse a password; and

(d) never allow any other person to access the company's systems using your login details, without express written authorization to do so.

2.2 You must not turn off or attempt to circumvent any security measures (antivirus software, firewalls, web filtering, encryption, automatic updates etc.) that the IT team have installed on your computer, phone or network or the company IT systems.

2.3 You must report any security breach, suspicious activity, or mistake you make that may cause a cyber security breach, to the CEO/Managing Director immediately.

2.4 You must only access work systems using computers or phones that the company owns.

2.5 You must not install software onto your company computer or phone (if required by the Company). All software requests should be made to the CEO/Managing Director.

2.6 You should avoid clicking on links to unknown websites, downloading large files, or accessing inappropriate content using company equipment or networks.

Consequences of system misuse

3.1 The Company considers the following actions to be a misuse of its IT systems or resources:

(a) any malicious or illegal action carried out against the company or using the company's systems;

(b) accessing inappropriate, adult or illegal content within company premises or using company equipment;

(c) excessive personal use of company IT systems during core working hours;

(d) removing data or equipment from company premises or systems without permission, or in circumstances prohibited by this Policy;

(e) using company equipment in a way prohibited by this Policy;

(f) circumventing technical cyber security measures implemented by the company's IT team; and

(g) failing to report a mistake or cyber security breach immediately.

3.2 If you are an employee, misuse of the IT system will be referred to the human resources team and may be considered misconduct; if you are a contractor and are found to be misusing the company IT systems, your contract may be terminated (subject to Company evaluation).

Glossary

CEO means the person appointed as the Chief Executive Officer of the Company from time to time.

Company means Koonenberry Gold Limited and its subsidiaries.

Managing Director means the person appointed as a Managing Director of the Company from time to time.

Policy means this document or any amending or replacement document.

Approved by the Board 18/06/2021