Cybersecurity Disclosure

Purpose

We maintain a Cybersecurity Policy and Incident Response Plan designed to establish acceptable uses of electronic devices, communications systems and network resources, and the framework for reporting and managing cybersecurity incidents. Due to the sensitive nature of cybersecurity, our Cybersecurity Policy and Incident Response Plan are confidential. The purpose of this document is to provide general commentary regarding our approach to cybersecurity management. Our Cybersecurity Policy, our Incident Response Plan, and this document apply to Royal Gold, Inc. and its subsidiaries ("Royal Gold," "we," or "our").

Overview of Risks

Like many businesses and organizations, Royal Gold faces constant and evolving cyber threats. Our systems, and those of our third-party service providers, could be vulnerable to damage or disruption caused by catastrophic events, power outages, natural disasters, computer system or network failures, viruses or malware, physical or electronic break-ins, unauthorized access, or other cyber-attacks.

Any security breach could compromise our networks or those of our service providers, and the information stored on them could be improperly accessed, disclosed, lost, or stolen. Any unauthorized activities could disrupt our operations, damage our reputation, or result in legal claims or proceedings, any of which could adversely affect our business, reputation, or operating results.

Responsibility

Our Board of Directors and senior management oversee matters relating to cybersecurity. Under its Charter, the Audit and Finance Committee of our Board of Directors is responsible for reviewing the security of our information technology systems and operations, including programs and defenses against cyber threats. All members of the Audit and Finance Committee are independent under Nasdaq and SEC rules. The full Board of Directors is briefed on cybersecurity at least annually and receives more frequent updates as warranted by the business operating environment. Our Chief Financial Officer and Treasurer is responsible for cybersecurity matters at the management level.

Training and Safeguards

Employees engage in an online cybersecurity training program semi-annually or more frequently as warranted by changes to the business operating environment.

Royal Gold has a number of physical and technical safeguards in place to address cybersecurity risks and conducts risk assessments as prudent, including external and internal penetration tests and social engineering campaigns.

Before allowing any external party, including service providers, to access to our networks we implement appropriate cybersecurity access procedures.

Response to Cybersecurity Breaches

Under our Incident Response Plan an incident response team is designated to respond in case of any cybersecurity breaches.