Cybersecurity Policy
(Effective December 19, 2023)

Purpose

The Board of Directors of the Corporation has adopted this Cybersecurity Policy (or the "**Policy**" as the context provides for) with a purpose of serving as a standard for setting, reviewing and implementing the Corporation's cybersecurity goals, objectives and targets.

The "Corporation" includes Gold Royalty Corp. and all of its subsidiaries. All vendors, suppliers and partners working with the Corporation are expected to comply with the principles found in this Policy as they relate to the Corporation and its businesses, and are encouraged to adopt similar policies within their own businesses.

This Policy should be read in conjunction with the other Corporation policies set forth below which are available on the Corporation's website at https://www.goldroyalty.com/.

The information that exists within the information technology ("**IT**") network and infrastructure (the "**Cyberspace**") is a valuable asset of the Corporation and, therefore, benefits from protection and preservation thereof. Effective information security management is necessary for the secured sharing and protection of information within the Corporation's Cyberspace.

This Policy serves as a framework within which risks to the confidentiality, integrity or availability of the Corporation's assets within the Cyberspace are managed in accordance with the agreed upon cybersecurity approach. In guiding the Corporation's ongoing operation, maintenance and effective management of its cybersecurity initiatives, this Policy will detail the roles and responsibilities of key personnel, provide guidance on the initiatives necessary to meet the objectives of this Policy.

Applicability

This Policy applies to all directors, officers, employees, consultants and contractors of the Corporation and any parent, holding companies and subsidiaries regardless of the terms of their contract (collectively, "**you**"), who use computing devices and network resources connected to the Corporation's Cyberspace. References in this Policy to "**we**", "**us**" or "**our**" shall be interpreted as referring to the Corporation unless the context suggests otherwise.

Policy Statement

The Corporation recognizes the importance of effective information security management and strives to maintain the confidentiality, integrity and availability of information in the Cyberspace. In aspiring to prevent, detect and respond to unauthorized and malicious attacks in the Cyberspace, the Corporation will identify, prioritize and manage dedicated efforts towards both protection of information and the minimization of risks of unauthorized and malicious access to information in the Cyberspace.

The Board of Directors of the Corporation (the "**Board of Directors**") aims to lead the Corporation in a direction that minimizes the risk of unauthorized and malicious use, disclosure, potential theft, alteration or damaging effects of the Corporation's operations while concurrently enabling the sharing of information in the Cyberspace. The Board of Directors is committed to ensuring that risks to the confidentiality, integrity or availability of Corporation-owned information assets are managed appropriately by implementing an information security risk management approach. In addition, the Corporation strives to ensure continued protection and maintenance of a secure environment for users of its Cyberspace information by aligning its information security approach. This includes reserving a right to monitor and audit network and system usage at any time for compliance reasons pursuant to this Policy. The Corporation views all reports of breaches hereunder seriously and will abide by rigorous investigation processes in the event of a breach.

Members of the Board of Directors and management overseeing the information security risk management approach of the Corporation will be provided with opportunities for continuing education in cybersecurity and evolving cybersecurity risks in order to better understand and evaluate the Corporation's preparedness.

Roles and Responsibilities

Board and Committee Oversight

The Board of Directors will oversee this Policy primarily through the Audit Committee of the Corporation (the "**Audit Committee**"). The Audit Committee will be responsible for the implementation of the Corporation's oversight, programs, procedures, and policies related to cybersecurity, cybersecurity risks, information security, and data privacy.

Management shall report to the Audit Committee on the Corporation's and its subsidiaries' strategy, risks, metrics and operations relating to cybersecurity and information security matters, including significant cybersecurity and information security-related projects and initiatives and related progress, the integration and alignment of such strategy with the Corporation's overall business and strategy, and trends that may affect such strategy or operations.

Management Oversight/Responsibilities

The Corporation's management team shall facilitate an environment in which the importance of managing cybersecurity risk is emphasized. The Corporation's Chief Executive Officer and Chief Financial Officer (the "**CFO**") will oversee the details of the information security risk management approach of the Corporation, and may appoint team leads from various departments of the Corporation from time to time to assist with certain aspects of the Corporation's cybersecurity risk mitigation strategy. While these leaders will oversee the strategy pursuant to this Policy, cybersecurity is the responsibility of all business stakeholders and requires the cooperation and compliance of all personnel.

Management will ensure that personnel are provided with adequate resources and trainings to fully understand the guidelines and expectations for cybersecurity. Members of the management team may be asked by the CFO to assist with IT security investigations in the event of a breach of this Policy. If any member of management is unaware of the best course of action in dealing with an IT-related matter, the manager shall immediately contact the Corporation's third party IT representative. Upon becoming aware of a potential violation of this Policy or a breach of cybersecurity, the member of management must immediately document the violation and request the individual surrender possession of any devices that may have suffered a security breach.

Employee, Consultant and Contractor Responsibility

All employees, consultants and contractors shall exercise professional judgement in using computing devices and network resources connected to the Cyberspace. All information, physical and intellectual properties stored on electronic and computing devices or existing within the Cyberspace remain the sole property of the Corporation. Therefore, employees, consultants and contractors must neither access nor share confidential and proprietary information prior to receiving consent from management or the Corporation's directors and officers.

Employees, consultants and contractors are strictly prohibited from performing any act that would be contrary to this Policy, including but not limited to:

- accessing data, a server or an account for any purpose other than conducting the Corporation's business in the ordinary course;
- copying or distributing copyrighted material or intellectual property without prior consent;
- opening messages, emails or attachments from unknown sources;
- leaving accounts unattended where another person may gain access;
- installing any copyrighted software without obtaining approval from the Corporation's third party IT group;
- disabling Corporation-enabled security features and requirements, including firewalls, user logins, passwords, multi-factor authentication applications and anti-virus programs;
- sharing passwords with other individuals or allowing others access to your accounts;
- exporting software, technical information, encryption software or technologies prior to obtaining consent from either management or the Corporation's third party IT group; and
- making fraudulent offers of products, items or services from any account that represents the Corporation.

All potential threats or loss of any Corporation device that may store confidential information must be promptly reported to the CFO.

Disclosure

Disclosure of cybersecurity and information security related matters, including material cybersecurity incidents, risk factors, risk management, governance, strategy, and other disclosures shall be provided in accordance with applicable laws and regulation. The Audit Committee shall also review the Corporation's cybersecurity-related disclosures in its annual securities filings.

Regulatory Developments

The Audit Committee shall monitor, on an ongoing basis, the implementation and effectiveness of this Policy and shall, annually or otherwise when applicable, assess:

- key legislative and regulatory developments that could materially impact the Corporation's cybersecurity and digital technology strategy, operations or risk exposure;
- engagement with government agencies, industry peers, and other critical infrastructure sectors on cybersecurity and related resiliency;
- industry trends, benchmarking and best practices relating to cybersecurity and digital technology; and
- any relevant cybersecurity and digital technology metrics.

Reports to the Board of Directors

The Audit Committee shall report regularly to the Board of Directors concerning its matters covered under this Policy and advising the Board of Directors of any developments that the Audit Committee believes should have Board of Directors' consideration. The Audit Committee shall also annually review and assess the adequacy of this Policy and recommend any proposed changes to the Board of Directors for approval.

This Policy will be updated as determined by the Audit Committee and Board of Directors to align with changes to the evolving cybersecurity threat landscape.

Restrictions and Limitations

Individuals who are subject to this Policy are not limited to the restricted use of specific devices. This Policy is all encompassing and incorporates all future and personal devices that may be used to store IT and confidential information of the Corporation, including intellectual property.

Enforcement

Failure to comply with this Policy or support this Policy and the mandates herein may compromise the Corporation's information assets and cause irreparable harm to the organisation, its people, clients and digital and physical assets. For further clarity, violations of this Policy may include, but are not limited to, the conscious release of data or confidential information to unauthorized parties, conscious downloads of software or hardware that jeopardizes the security of the Corporation, and openly sharing passwords with any individual. Violations or breaches of this Policy or the associated schedules, standards or guidelines may result in suspension and/or discipline up to and including termination, in addition to administrative sanctions or legal actions.