CYBERSECURITY POLICY

Purpose

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

For the purposes of this Policy, 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 Corporation's Corporate Disclosure Policy, Code of Business Conduct and Ethics, Insider Trading Policy and Whistleblower Policy, each of which is available on the Corporation's website at https://www.goldroyalty.com/. In the event of any conflict between this Policy and the Corporate Disclosure Policy regarding the assessment, timing or content of public disclosure, the Corporate Disclosure Policy shall govern.

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

Management, through the CFO, will report to the Audit Committee at least quarterly, and otherwise as circumstances require, on the Corporation's strategy, risks, metrics and operations relating to cybersecurity and information security matters, including management's approaches and processes to identify, assess and manage material cybersecurity risks, significant cybersecurity and information security-related projects and initiatives and related progress, third-party and vendor cybersecurity risk, incident response and breach notification processes, the integration and alignment of such strategy with the Corporation's overall business and strategy, and trends that may affect such strategy or operations. The CEO or CFO shall notify the Chair of the Audit Committee of any Significant Incident (as defined below) as soon as practicable and in any event within twenty-four (24) hours after the CEO or CFO determines that the incident is a Significant Incident. The Chair of the Audit Committee shall determine whether to convene a special meeting of the Audit Committee and whether to inform the Chair of the Board, who may convene a special meeting of the Board.

Management Oversight/Responsibilities

Management will facilitate an environment in which the importance of managing cybersecurity risk is emphasized. The Corporation's Chief Executive Officer (the "**CEO**") 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.

The CFO shall serve as the executive responsible for day-to-day administration of this Policy (the "Cybersecurity Lead") and shall act as the primary point of contact among management, the Corporation's third party IT provider and the Audit Committee. The Cybersecurity Lead shall maintain a written incident response plan that classifies incidents by severity. For the purposes of this Policy, a "Significant Incident" means any actual or reasonably suspected cybersecurity incident that (a) may reasonably be expected to be material to the Corporation, (b) involves unauthorized access to personal information, material non-public information or financial systems, (c) involves ransomware, extortion or fraudulent funds transfer, or (d) may trigger a regulatory, contractual or privacy notification obligation.[1]

Management will ensure that personnel are provided with adequate resources and training, at least annually, to fully understand the guidelines and expectations for cybersecurity. Members of the management team may be asked by the CEO or CFO to assist with IT security investigations in the event of a breach of this Policy. If any member of

[1] The revision addresses a gap in the existing policy, which allocated cybersecurity responsibilities among several parties without identifying a single executive accountable for day-to-day administration and incident coordination. Designating the CFO provides clear ownership and ensures significant incidents are consistently assessed, managed and escalated to the appropriate management and Board bodies.

management is unaware of the best course of action in dealing with an IT-related matter, the manager shall immediately contact the Cybersecurity Lead and 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 (a) document the violation, (b) notify the CEO or CFO, (c) take reasonable steps to preserve relevant evidence and logs, and (d) request the individual surrender possession of any devices that may have suffered a security breach. Where the CEO or CFO is unavailable or is implicated in the incident, notification shall be made directly to the Chair of the Audit Committee.

Management shall establish, maintain and test, at least annually (including through tabletop exercises involving senior management and, periodically, members of the Audit Committee), appropriate cybersecurity incident-response, business-continuity and disaster-recovery arrangements, including backup and restoration procedures, escalation protocols, engagement of external legal counsel and forensic advisors (with a view to preserving privilege where appropriate), critical third-party dependencies and recovery priorities. Management shall report material test results, incidents and remediation measures to the Audit Committee.[2]

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, disclosing or distributing confidential information, personal information, copyrighted material or intellectual property without prior consent;
- opening messages, links, emails or attachments without appropriate caution and verification, or failing to report suspected phishing or social engineering;
- leaving devices or accounts unsecured or 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

[2] The revision is responsive to SEC and Canadian expectations that public companies maintain effective processes for identifying, managing, escalating and disclosing material cybersecurity risks and incidents. Although annual tabletop testing is not specifically mandated, it reflects recognized NIST and CISA practices and provides assurance to the Audit Committee that the Company's incident-response, continuity and recovery arrangements are operationally effective.

- making fraudulent offers of products, items or services from any account that represents the Corporation.

Using unapproved artificial intelligence tools for Corporation business, or submitting confidential, privileged or personal information or material, non-public information to any unapproved service.

All potential threats or loss of any Corporation device that may store confidential information must be promptly reported to the CFO. Any actual or suspected cybersecurity incident affecting the Corporation must be promptly escalated to the CEO, CFO or President. The CEO and CFO, in consultation with the Corporation's disclosure committee or other persons designated under the Corporate Disclosure Policy and with legal counsel as appropriate, shall assess without unreasonable delay whether the incident constitutes a material change or material fact requiring disclosure under applicable Canadian securities laws, or information requiring disclosure under the rules of the NYSE American or furnishing on Form 6-K under U.S. securities laws. Any such disclosure shall be made in accordance with the Corporate Disclosure Policy. Where an incident may constitute material non-public information, the CFO shall consider whether to impose a trading blackout under the Insider Trading Policy, and persons with knowledge of the incident shall keep it confidential and shall not trade in the Corporation's securities until the information has been generally disclosed or the incident is determined not to be material.[3]

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 regulations and the Corporate Disclosure Policy. The Audit Committee shall review the Corporation's cybersecurity-related disclosures in its annual securities filings. Following any disclosed incident, management shall assess whether updated or corrective disclosure is required.

Regulatory Developments

The Audit Committee shall periodically review and provide general oversight of management's implementation of this Policy and the effectiveness of the Corporation's cybersecurity risk management approaches and processes 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

The Audit Committee shall report to the Board at least quarterly concerning matters covered under this Policy and promptly advise the Board of any Significant Incident and any other developments that the Audit Committee believes should receive the Board's consideration. The Board shall receive a cybersecurity briefing from management at least annually. The Audit Committee shall also review and reassess the adequacy of this Policy at least annually and

[3] The revision establishes a documented process for promptly escalating cybersecurity incidents and determining whether Canadian, NYSE American or U.S. disclosure obligations are triggered. It also coordinates incident disclosure with the Company's disclosure and insider-trading controls, reducing the risk of delayed disclosure, selective disclosure or trading while material incident information remains undisclosed.

otherwise as it deems appropriate and recommend any proposed changes to the Board for approval.

This Policy may be amended or modified by the Board, including following the review and recommendation by the Audit Committee, to align with changes to the evolving cybersecurity threat landscape and applicable legal and regulatory requirements.

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 organization, 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.

Approved by the Board of Directors of Gold Royalty Corp.
Effective Date: December 19, 2023
Amended and Restated: November 4, 2026