SILVERCORP METALS INC.

Information Security Management Policy

Silvercorp Metals Inc. (**"Silvercorp"** or the **"Company"**) recognizes information security and data protection as critical components of its internal control system and sustainable development strategy. The Company is committed to establishing a systematic, forward-looking and risk-oriented information security management framework to safeguard the confidentiality, integrity and availability of information assets, prevent information and cybersecurity risks, ensure business continuity, maintain the reliability of financial information, and protect the legitimate rights and interests of stakeholders.

Compliance with Laws and Regulations

- We will comply with all applicable laws, regulations, and industry standards related to information security and data protection in the jurisdictions where we operate.
- We will adopt and implement recognized international practices and relevant frameworks to promote alignment with applicable international standards for information security, data privacy, and cybersecurity.

Management and Implementation

- The Audit Committee of the Board has oversight responsibility for information security and data privacy. The committee reviews and approves relevant strategies, material risks, and resource allocation to ensure alignment with the Company's overall ESG strategy and business objectives.
- Senior management is responsible for implementing the Board's decisions and shall adopt a dual reporting system of regular and ad-hoc briefings to the Audit Committee:

  Regular Briefing: Conducted on an annual basis, covering the overall status of the operation of the information security management system, risk identification and investigation, implementation of protective measures, and training delivery.

  Ad-hoc Reporting: Initiated within 24 hours in the event of major information security incidents, significant potential risks, or strategic adjustments. Response plans and risk mitigation recommendations shall be submitted simultaneously.
- The general manager of each subsidiary oversees the implementation of this Policy within their respective jurisdictions. Specialized functional departments, such as the Information Department, lead technical safeguards, while departments including Human Resources and Legal provide support in areas such as access management, compliance reviews, and personnel training.
- Employees are required to comply with this Policy and related procedures, to properly handle sensitive information, securely use Company devices and networks, avoid

unauthorized disclosure of data, and promptly report any security incidents or suspicious activities.

Information Security Management Principles

- **Privacy-First Approach:** We integrate data protection throughout the lifecycle of our operations, ensuring only necessary information of employees, customers, and stakeholders is collected, and that this information is processed, stored, and used lawfully, fairly, and minimally.
- **Rights Protection:** We respect individuals' rights to access, correct, and be informed about their data, and prohibit unauthorized data misuse or illegal trading of data.
- **Data Ethics:** We uphold data ethics, promoting fairness, transparency, and responsible use of digital technologies, and prevent data abuse or discriminatory practices.
- **Risk-oriented:** We systematically identify, assess, and manage information security and cybersecurity risks based on business characteristics and risk levels.
- **Data Classification and Tiered Protection:** We classify data based on its importance, sensitivity, and potential impact, and apply corresponding security controls and confidentiality requirements, with enhanced safeguards for critical systems, confidential business information, and sensitive personal data.
- **Role-Based Access Control:** We implement role-based access control (RBAC) to grant system access strictly according to job responsibilities, and encrypt sensitive data both at rest and in transit to prevent unauthorized access or disclosure.
- **Cross-Border Data Compliance:** We ensure that cross-border data transfers are subject to prior legal and compliance review, governed by data processing agreements with overseas partners that define data use, security responsibilities, and legal liabilities to ensure compliance with applicable laws and regulations in relevant jurisdictions.
- **Continuous Improvement:** We regularly review the effectiveness of the information security management system, identify and address areas for improvement, and promote the continuous enhancement of our security capabilities.

Employee Training

- We conduct annual information security awareness training for employees to ensure that employees understand the importance of information security, recognize potential threats, and follow established security best practices. Training covers topics such as secure handling of sensitive information, phishing awareness, and the Company's policies and procedures for reporting security incidents.

Monitoring and Auditing

We have established a regular monitoring and audit process to evaluate the effectiveness of the management system and monitor information security threats. The program includes:

- **Business Continuity Plans (BCP):** Procedures to prevent potential threats, minimize operational disruption, and ensure timely system recovery in the event of an accident.
- **Vulnerability Analysis:** Systematic identification, assessment, and prioritization of vulnerabilities in computer systems and network infrastructures.
- **Internal Audits:** Regular internal audits to evaluate the effectiveness of the management system. Results will be reported to senior management for review, and appropriate corrective actions are implemented where necessary.
- **Independent External Audit:** Annual internal control audits conducted by independent third parties, covering IT and data security, referencing internationally recognized information security standards, such as ISO 27001.
- **Data Breach Incident Response:** A comprehensive data breach response plan is established and maintained, covering incident detection, internal reporting, containment, investigation, and stakeholder notification, to ensure timely and effective handling of incidents and protect data integrity.
- **Escalation Process:** Procedures for promptly reporting any identified or suspected security incidents or vulnerabilities (including those related to systems, applications, or networks) to the IT Department or appropriate management in a timely manner.

Third Party Management

- We establish information security requirements for key partners, including compliance with this Policy or equivalent standards and access control measures. Third-party access to the Company's systems or data is subject to strict approval and monitoring, with permissions immediately revoked upon termination of cooperation to prevent third-party information security risks.

Disclosure

- We will communicate significant security incidents that may affect stakeholders in a timely and transparent manner in accordance with applicable legal and regulatory requirements. Additionally, the Company' s management practices and performance relating to cybersecurity and data privacy will be disclosed through public channels, such as the annual Sustainability Report.

Scope of Application

This Information Security Management Policy applies to Silvercorp Metals Inc., its direct business activities, subsidiaries, and contractors. Silvercorp actively encourages our

partners, including suppliers, service providers, consultants, agents, as well as potential partners for future due diligence, mergers and acquisitions, joint ventures, and other business partners, to comply with this Policy.

This Policy was reviewed and approved by the Board of Directors on March 27, 2026, and will be re-evaluated annually.