

SILVERCORP METALS INC.
(the “Corporation”)

Code of Business Conduct and Ethics
(Effective August 6, 2026)

1. Introduction

Silvercorp Metals Inc. and its subsidiaries (collectively, the “Corporation”, “we”, “us” or “our”) require high standards of professional and ethical conduct from our employees. Our reputation with our shareholders, business partners, prospective investors and other stakeholders for honesty and integrity is key to the success of our business. No employee will be permitted to achieve results through violations of laws or regulations, or through unscrupulous dealings. We intend that the Corporation’s business practices will be compatible with the economic and social priorities of each location in which we operate. Although customs vary by country and standards of ethics may vary in different business environments, honesty and integrity must always characterize our business activity. If a law conflicts with a policy in this Code of Business Conduct and Ethics (the “**Code**”), you must comply with the law; however, if a local custom or policy conflicts with this Code, you must comply with the Code. If you have any questions about these conflicts, you should ask your supervisor how to handle the situation. This Code reflects our commitment to a culture of honesty, integrity and accountability and outlines the basic principles and policies with which all employees are expected to comply. **Please read this Code carefully and sign at the bottom to acknowledge it has been read and that you will undertake to comply with the Code at all times.**

In addition to following this Code in all aspects of your business activities, you are expected to seek guidance in any case where there is a question about compliance with both the letter and the spirit of our policies, applicable laws, rules and regulations. This Code covers a wide range of business practices and procedures. It does not cover every issue that may arise, but it sets out basic principles to guide all employees of the Corporation. This Code does not supersede the specific policies and procedures that are covered in the Corporation’s operating manuals or in separate specific policy statements. **References in this Code to the “Corporation” mean Silvercorp Metals Inc. or any of its subsidiaries. Reference to “employees” includes officers and directors.**

Those who violate the standards set forth in this Code will be subject to disciplinary action up to and including dismissal. In addition, violation of any laws, governmental regulations or this Code could result in notification to appropriate governmental authorities and public disclosure of such violation including, without limitation, the names of parties involved. ***If you are in a situation that you believe may violate or lead to a violation of this Code, follow the guidelines described in Section 22 below.***

Your cooperation is necessary to the continued success of our business and the cultivation and maintenance of our reputation as a good corporate citizen. This Code should be read together with the Corporation’s other applicable policies, including Confidentiality and Cybersecurity Policy and Anti-Corruption Policy, as amended from time to time.

2. Compliance with Laws, Rules and Regulations

Compliance with the letter and spirit of all laws, rules and regulations (including stock exchange rules) applicable to our business is critical to our reputation and continued success. All employees must respect and obey such laws, rules and regulations and avoid even the appearance of impropriety.

Not all employees are expected to know the details of these laws, rules and regulations, but it is important to know enough to determine when to seek advice from supervisors, managers or other appropriate personnel. The Corporation may hold information and training sessions to promote compliance with laws, rules and regulations, including insider trading laws.

3. Inside Information and Securities Trading

The Corporation is a public company with its shares listed for trading on the TSX and NYSE American. A central requirement for public companies is that all buyers and sellers of a company's shares have access to the same material information about the company. Material information that has not been disclosed to the public either by press release or regulatory filing is referred to as "Inside" information. Trading in a company's shares based on having Inside information is a serious breach of securities laws which can result in enforcement action being taken by regulators. This also applies to "tipping" others with the Inside information. Examples of Insider information are set out below. If there is unusual market activity immediately before a significant change to a company's share price, securities regulators will review each trade to determine whether inside trading has occurred. **INSIDER TRADING IS A SERIOUS OFFENCE, which will result in employment termination** in addition to any enforcement regulators may take.

In the course of your employment, consulting activities, or as result of your role as a director, you may become aware of nonpublic information regarding the business, operations or securities of the Corporation. Unauthorized disclosure of any nonpublic information or the misuse of material nonpublic information in securities trading is strictly prohibited. It is not possible to define all situations where nonpublic information is "material", however, information should be regarded as material if there is a reasonable likelihood that it would be considered important to an investor in making an investment decision regarding the purchase or sale of the Corporation's securities. Under U.S. securities legislation, material information also includes any matters to which there is a substantial likelihood that a reasonable investor would attach importance in making investment decisions. If in doubt check with the General Counsel or Corporate Secretary of the Corporation. Nonpublic information is information that has not been previously disclosed to the general public and is otherwise not available to the general public. While it may be difficult to determine whether particular nonpublic information is material, there are various categories of information that are particularly sensitive and, as a general rule, should always be considered material. In addition, material information may be positive or negative. Examples of such information may include:

- Project exploration results, whether positive or negative
- Joint ventures with third parties, including information on the joint venture partner
- News of a pending or proposed merger or acquisition
- Financial results
- Major contract awards, cancellations or write-offs
- Exploration results or development milestones
- News of the disposition of material assets

- Impending bankruptcy or financial liquidity problems
- Gain or loss of a substantial property
- Stock splits
- New equity or debt offerings
- Significant litigation exposure due to actual or threatened litigation
- Changes in senior management
- Projections of future earnings or losses
- Dividend issuance decisions

Trading on Material Nonpublic Information: With certain limited exceptions, no officer or director of the Corporation, no employee of the Corporation or its subsidiaries and no consultant or contractor to the Corporation or any of its subsidiaries and no members of the immediate family or household of any such person, shall engage in any transaction involving a purchase or sale of the Corporation's securities, including any offer to purchase or offer to sell, during any period commencing with the date that he or she possesses material nonpublic information concerning the Corporation, and ending at the close of business on the date of public disclosure of that information (usually by Press Release), or at such time as such nonpublic information is no longer material. Where a press release is issued immediately after market, no such trading shall be undertaken until the close of the market on the following day on which the Corporation's shares trade.

Tipping: No insider shall disclose ("tip") material nonpublic information to any other person (including family members) where such information may be used by such person to his or her profit by trading in the securities of companies to which such information relates, nor shall such insider or related person make recommendations or express opinions on the basis of material nonpublic information as to trading in the Corporation's securities.

Applicability of Insider Trading Regulations to Securities of Other Companies: The insider trading guidelines described herein also apply to material nonpublic information relating to other companies related to the Corporation in any way, including the Corporation's joint venture partners or other companies the Corporation may have an investment in ("**business partners**"), when that information is obtained in the course of employment with, or other services performed on behalf of the Corporation. All employees and consultants should treat material nonpublic information about the Corporation's business partners with the same care as is required with respect to information relating directly to the Corporation.

4. Conflicts Of Interest

A conflict of interest occurs when an individual's private interest interferes, or appears to interfere, in any way with the interests of the Corporation. A conflict situation can arise when an employee takes actions or has interests that may make it difficult to perform his or her work for the Corporation objectively and effectively. Conflicts of interest also arise when an employee, or a member of his or her family, receives improper personal benefits as a result of his or her position in the Corporation. Loans to, or guarantees of obligations of, such persons may not be legally permissible and are likely to pose conflicts of interest, as are transactions of any kind between the Corporation and any other organization in which you or any member of your family have an interest. Activities that could give rise to conflicts of interest are prohibited unless specifically approved by the **Board of Directors or the Audit Committee**. It is not always easy to determine

whether a conflict of interest exists, so any potential conflicts of interests should be reported immediately to your supervisor or the Corporation's general legal counsel.

5. *Corporate Opportunities*

Employees are prohibited from taking for their personal benefit any opportunities that arise through their employment, the use of corporate property, information or position and from using corporate property, information or position for personal gain. Employees are also prohibited from competing with the Corporation directly or indirectly. Employees owe a duty to the Corporation to advance the legitimate interests of the Corporation when the opportunity to do so arises.

6. *Confidentiality*

Employees must maintain the confidentiality of information entrusted to them by the Corporation or that otherwise comes into their possession in the course of their employment, except when disclosure is authorized or legally mandated. Employees may be required to execute a standard form confidentiality agreement upon starting employment or from time to time during the course of employment. The obligation to preserve confidential information continues even after you leave the Corporation.

Confidential information includes all non-public information that may be of use to competitors, or harmful to the Corporation or its customers, if disclosed. It also includes information that suppliers and customers have entrusted to us.

7. *Protection and Proper Use of Corporate Assets*

All employees should endeavor to protect the Corporation's assets and ensure their efficient use. Theft, carelessness and waste have a direct impact on the Corporation's profitability. Any suspected incidents of fraud or theft should be immediately reported for investigation.

Corporation assets such as monies, products, or computers may only be used for legitimate business purposes or other purposes approved by management. Corporation assets may never be used for illegal purposes.

The obligation to protect Corporation assets includes proprietary information. Proprietary information includes any information that is not generally known to the public or would be helpful to our competitors. Examples of proprietary information include intellectual property, such as new projects the Corporation is considering or in negotiations with, trade secrets, patents, trademarks and copyrights, as well as business, marketing and service plans, engineering and manufacturing ideas, designs, databases, records, salary information and any unpublished financial data or reports. Unauthorized use or distribution of this information is a violation of Corporation policy. It may also be illegal and may result in civil and criminal penalties. The obligation to preserve proprietary information continues even after you leave the Corporation.

8. *Fair Dealing*

We seek to outperform our competition fairly and honestly. We seek competitive advantages through superior performance, never through unethical or illegal business practices. Stealing proprietary information, possessing trade secret information obtained without the owner's

consent or inducing the disclosures of proprietary information or trade secrets by past or present employees of other companies is prohibited. Each employee should endeavor to deal fairly with the Corporation's customers, suppliers, competitors and employees. No employee should take unfair advantage of anyone through illegal conduct, manipulation, concealment, abuse of privileged information, misrepresentation of material facts or any other unfair-dealing practice.

9. *Discrimination and Harassment*

We value the diversity of our employees and are committed to providing equal opportunity in all aspects of employment. Abusive, harassing or offensive conduct is unacceptable, whether verbal, physical or visual. Examples include derogatory comments based on racial or ethnic characteristics or personal appearance and unwelcome sexual advances. Employees are encouraged to speak out when a co-worker's conduct makes them uncomfortable, and to report harassment when it occurs.

10. *Safety and Health*

We are all responsible for maintaining a safe and healthy workplace by following safety and health rules and practices. The Corporation is committed to keeping its workplaces free from hazards. Please report any accidents, injuries, unsafe equipment, practices or conditions immediately to a supervisor or other designated person. Threats or acts of violence or physical intimidation are prohibited.

In order to protect the safety of all employees, employees must report to work in condition to perform their duties and free from the influence of any substance that could prevent them from conducting work activities safely and effectively. The use of illegal drugs in the workplace is prohibited.

11. *Financial Statements and Recordkeeping*

Honest and accurate recording and reporting of information is critical to our financial reporting and our ability to make responsible business decisions. The Corporation's accounting records are relied upon to produce reports for the Corporation's management, Board, shareholders, creditors, governmental agencies and others. Our financial statements and the books and records on which they are based must truthfully and accurately reflect all corporate transactions and conform to all legal and accounting requirements and our system of internal controls. **A separate Code of Ethical Conduct for Financial Managers forms part of this Code as Schedule "A".**

All employees have a responsibility to ensure that the Corporation's records, including accounting records, do not contain any false or intentionally misleading entries. We do not permit intentional misclassification of transactions as to accounts, departments or accounting periods. All transactions must be supported by accurate documentation in reasonable detail and recorded in the proper account and in the proper accounting period.

All Corporation books, records, accounts and financial statements must be maintained in reasonable detail, must appropriately reflect Corporation transactions and must conform to both applicable legal requirements and the system of internal controls of the Corporation. Unrecorded or "off the books" funds or assets should not be maintained.

Business records and communications may become public through legal or regulatory investigations or the media. We should avoid exaggeration, derogatory remarks, legal conclusions or inappropriate characterizations of people and companies. This applies to communications of all kinds, including email and informal notes or interoffice memos. Records should be retained and destroyed in accordance with the Corporation's records storage and retention policy.

The Corporation will make full, fair, accurate, timely and understandable disclosure in periodic reports and documents required to be filed by the Corporation under applicable securities laws and in other public communications made by the Corporation, in accordance with the Corporation's Corporate Disclosure Policy.

12. *Use of E-Mail and Internet Services*

E-Mail systems and Internet services are provided to help us do work. Incidental and occasional personal use is permitted, but never for personal gain or any improper purpose. You may not access, send or download any information that could be insulting or offensive to another person, such as sexually explicit material or jokes, unwelcome propositions, ethnic or racial slurs, or any other message that could be viewed as harassment. Also remember that "flooding" our systems with junk mail and trivia hampers the ability of our systems to handle legitimate Corporation business and is prohibited.

Employees should not download copyrighted materials, should not copy material that is not licensed to the Corporation and should follow the terms of a license when using material that is licensed to the Corporation. No changes should be made to licensed materials without the prior consent of the Corporation. In addition, employees are discouraged from downloading games and screensavers, as these are common sources of viruses.

Your messages (including voice mail) and computer information are considered the Corporation's property and you should not have any expectation of privacy. Unless prohibited by law, the Corporation reserves the right to access and disclose this information as necessary for business purposes. Use good judgment, and do not access, send messages or store any information that you would not want to be seen or heard by other individuals.

13. *Information Governance and Data Security*

Silvercorp's information is a key corporate asset, essential to the success of our business. It therefore needs to be managed and protected in accordance with its commercial value and level of sensitivity. There are also a number of laws which impose requirements on how we manage our information, particularly personal data. Employees, contractors, business partners and other stakeholders should be able to trust that we handle their personal data in accordance with applicable data protection laws. It is important that we have appropriate procedures and systems in place to ensure information is properly managed. Failure to manage and protect information as required by law may undermine our reputation and lead to investigations, fines and/or other penalties for the company and/or individuals.

We differentiate between various types of information to enable data identification and define ownership, sensitivity, management and appropriate protection during its life cycle. We implement procedures and systems to ensure that we manage and protect company information

properly. We act responsibly and follow applicable policies and procedures when using our systems or dealing with company information, whether in hard copy or electronic format. We do not share confidential company information, unless we are entitled to do so and it is required for our business activities, or to comply with legal or regulatory obligations. We only retain company information for as long as it has value to the business and where it is required for legal or regulatory purposes.

We collect, use and keep personal data only for lawful purposes and as required to meet business requirements. We follow applicable procedures when dealing with personal data and we promptly report any personal data breaches to the local data protection contact person or to Human Resources, Legal, Compliance, or Information Technology.

We are committed to complying with applicable data retention and destruction obligations which require us to retain company information for as long as required for legal, compliance or business purposes and to destroy information - in particular personal data - after expiry of the applicable retention period.

We safeguard company information and are careful who can access it. We are committed to using legitimate software. We recognize the value of company information and work in a secure way to protect and ensure its integrity. We recognize the cyber risks we face and use tools, systems and processes with clear ownership and accountability to adequately protect our information, based on its commercial value and sensitivity. We are committed to protecting Silvercorp's information as well as the information relating to our workforce, former employees, business partners and other stakeholders and to complying with all legal requirements regarding its identification, protection, use, retention and destruction

14. *Political Activities and Contributions*

We respect and support the right of our employees to participate in political activities. However, these activities should not be conducted on Corporation time or involve the use of any Corporation resources such as telephones, computers or supplies. The Corporation's name must not be used in any political activity unless previously authorized by management. Employees will not be reimbursed for personal political contributions.

We may occasionally express our views on local and national issues that affect our operations. In such cases, Corporation funds and resources may be used, but only when permitted by law and by our strict guidelines. The Corporation may also make limited contributions to political parties or candidates in jurisdictions where it is legal and customary to do so. No employee may make or commit to political contributions on behalf of the Corporation without the approval of senior management.

15. *Gifts and Entertainment*

Business gifts and entertainment are customary courtesies designed to build goodwill among business partners. These courtesies include such things as meals and beverages, tickets to sporting or cultural events, discounts not available to the general public, travel, accommodation and other merchandise or services. In some cultures they play an important role in business relationships. However, a problem may arise when such courtesies compromise – or appear to compromise – our ability to make objective and fair business decisions.

Offering or receiving anything of value with the intention or appearance of improperly influencing a government official or private person, in order to obtain or convey any improper advantage, or for any other corrupt purpose, is strictly prohibited. It is important to recognize that even when there is no intent to convey a bribe such intent may be inferred from the surrounding circumstances. For the purposes of this Code, the phrase “**anything of value**” includes without limitation cash, travel, meals, gifts, entertainment, favors, services, loans and loan guarantees, investment or business opportunities, the use of property or equipment, job offers, transportation, the payment or reimbursement of debt, and other tangible and intangible payments.

These guidelines apply at all times, and do not change during traditional gift-giving seasons. No gift, entertainment nor anything else of value should ever be offered, given, provided or accepted, whether directly or indirectly, by any director, employee or Agent (as defined below in section 19) of the Corporation, or by any family member of a director, employee or Agent, unless it (1) is not a cash gift, cash equivalent (which includes, without limitation, gift cards, phone cards, meal vouchers or cards) in the form of stock or other similar consideration, (2) is consistent with customary business practices, (3) is not excessive in value, (4) is not intended and cannot be construed as a bribe or payoff (5) is permitted by the rules of the recipient’s employer, and (6) does not violate any applicable laws or regulations, including without limitation, the **Corruption of Foreign Public Officials Act** (Canada), the Prevention of Bribery Ordinance (Hong Kong), and the **Foreign Corrupt Practices Act** (USA), no matter where the gift occurs. Further, it must not be given with such frequency that it appears that an effort is being made to avoid restrictions under local law or this Code.

Expenses related to a gift or anything of value from a director, employee or agent of the Corporation must be supported by receipts and accurately recorded on the Corporation’s books and records.

Further, all gifts, meal, travel and entertainment *of any value* provided by any director, employee or agent of the Corporation, or by any family member of any director, employee or agent of the Corporation, to any government official must (i) receive the prior approval (in writing) of the **Chair of the Audit Committee**, and (ii) be transparently and accurately recorded in the Corporation’s books and records.

Please discuss with your supervisor any gifts or proposed gifts if you are uncertain whether they are appropriate.

16. Anti-Money Laundering

Money laundering is the process of concealing the criminal origin of money or other assets (such as raw materials), so they appear to come from a legitimate source. It is illegal, unethical and facilitates criminal conduct. Failure to address the risk of money laundering could undermine our reputation and lead to investigations, fines and/or other penalties for the company and/or individuals.

We are aware of the risk of third parties exploiting us by engaging in money laundering, terrorist financing, and sanctions evasion. We do not assist, support, participate in or permit money laundering or terrorist financing. We do not accept money or other assets if we know or suspect

that they derive from any kind of criminal activity. We do not knowingly deal with criminals, suspected criminals or the proceeds of crime.

Suspicious activity is identified by transaction behaviors where the amount, frequency, source, flow, or intended use are clearly inconsistent with the counterparty's identity, financial status, and business operations. Specifically, employees must be alert to the following characteristics:

- The goods or services provided are clearly inconsistent with the counterparty's scale of operations or industry trading practices;
- The contract amount seriously exceeds the counterparty's production scale or actual asset position;
- Fund movement patterns are seriously inconsistent with the counterparty's production and operating cycles;
- Corporate accounts of subsidiary business units frequently transfer large sums to personal accounts for rapid consumption.

We do not facilitate the acquisition, ownership or control of criminal proceeds or other assets deriving from criminal activity nor do we assist others in concealing criminal proceeds or assets. We do not tolerate tax evasion of any kind. We maintain strict risk-based screening procedures to identify whether counterparties, their beneficial owners, or other relevant parties we deal with are subject to sanctions, anti-money laundering, terrorist financing concerns.

To manage our money laundering risk exposure and ensure compliance, we implement a number of controls and processes. These include: due diligence procedures to determine the background, ownership, business purpose and identity of our counterparties; risk-based screening against applicable watchlists required by the People's Bank of China (PBOC), FinCEN (U.S.), and FINTRAC (Canada); and controls in respect of payments we make and receive using a risk-based approach to ensure that they are consistent with the requirements of this policy. As a general rule, we make all payments under our contracts to, and receive payments from, our contractual counterparties to avoid the risk of facilitating money laundering, sanctions evasion or tax evasion.

We require employees to immediately report any discovered suspicious transactions to the front-line AML Task Force. The Task Force shall conduct a preliminary review and, where suspicious activity is confirmed, submit a Suspicious Transaction Report (STR) to Compliance. Compliance will verify the report against original vouchers and escalate it to the management. Upon receipt, management shall organize internal control and legal personnel to conduct an in-depth investigation and issue an opinion. If confirmed, the Compliance Department is mandated to report the findings to the relevant regulatory authorities (e.g., FinCEN, FINTRAC, or the PBOC).

17. Address the Risk of Fraud

Fraudulent activity is unethical and can be illegal. Failure to address the risk of fraud may undermine our reputation and lead to investigations, fines and/or other penalties for the company and/or individuals. We do not engage in fraudulent behavior, and we do not knowingly assist or facilitate any third party to commit fraud.

Fraud is the act of engaging in deceptive or intentionally misleading activity in order to obtain an unfair or illegal financial or personal gain. To prohibit and prevent fraud, we require employees to be alert to any unusual or suspicious arrangements which could expose us to the risk of fraud, and

to report any such arrangements to Compliance.

18. *Comply with All Sanctions*

The global nature of our business, and because sanctions apply across borders, means the transactions or activities we engage in may be subject to sanctions or other restrictive measures imposed by multiple government authorities. Government authorities impose restrictive measures for a variety of national security and foreign policy reasons, either unilaterally, based on United Nations Security Council resolutions, or other multilateral policy initiatives.

Failure to address the risk of violations of these measures may undermine our reputation and lead to investigations, fines and/or other penalties for the company and/or individuals.

We are committed to complying with all sanctions, export controls and trade embargoes applicable to our business activities. We do not participate in transactions or engage in conduct designed or intended to evade or facilitate a breach of applicable sanctions or other restrictive measures. We do not conduct business in, or involving any, embargoed territory, or sanctions targets, directly or indirectly. This includes a prohibition on all direct or indirect investment, payment, or provision of resources to sanctioned entities. We do not engage in any sanctionable activity that could result in the designation of Silvercorp as a sanctions target.

We only allow deviations from these general requirements in exceptional circumstances with prior approval from Compliance and, under all circumstances, these transactions must be compliant with applicable laws. To manage our sanctions risk exposure and ensure compliance, we implement controls and processes including screening and due diligence on our counterparties, beneficial owners, and other relevant parties we deal with. This involves regular screening of customers and suppliers against relevant sanctions lists, including those imposed by Canada, OFAC, the European Union, and other local jurisdictions of operation. We use a risk-based approach to determine whether they are a sanctions target, sectoral sanctions identification entity, or otherwise attract sanctions risk. To mitigate identified risks, we utilize restrictive clauses in our commercial contracts and maintain alternative supplier plans to ensure business continuity. We also implement controls in respect of our payments, using a risk-based approach to ensure that they are consistent with the requirements of this policy. We require employees to be alert to sanctions risk and to report any sanctions issues identified to Compliance. We are transparent with Silvercorp's banks and counterparties in relation to our business.

19. *Use of Agents, Consultants, and Other Third Parties*

The Corporation, and possibly executives and employees of the Corporation, may be held criminally liable for bribes paid by an agent, consultant, joint venture partner, business partner or other third party who can act on behalf of the Company (referred to here collectively as "**Agents**"). Actual knowledge of the bribery is not required to incur liability. In light of this fact, thorough due diligence must be conducted before entering into agreements with Agents, all agreements with Agents must contain strong provisions designed to ensure that the Agents do not violate this Code or applicable anti-corruption laws, and all employees of the Corporation must be aware of "red flags" or warning signs that could indicate a problem with an Agent.

a. *Due Diligence*

When a director or employee of the Company initiates any business relationship with an Agent, it

is important to make a full risk assessment. **It is the responsibility of General Counsel to ensure that this is done and to ensure that the results of the assessment are appropriately recorded.** This must include a background check, tailored to the risk level and significance of the proposed relationship, to ensure that the Agent possesses both the requisite qualifications and a solid reputation for business integrity. The risk level and significance associated with the Agent should be assessed based on factors such as the nature of the relationship, the size of the contract, the location where the services will be performed, and whether the services will involve interaction with government officials. At a minimum, the due diligence process should include: gathering information from available sources concerning the ownership, management, capabilities and reputation of the Agent; reviewing the proposed structure and terms of the proposed relationship, including compensation provisions; and requiring and checking multiple references.

b. Agreements

Every agreement with an Agent must be in writing and describe the services to be performed, the fee basis, the amounts to be paid, and other material terms and conditions of the representation. The agreement also should contain written provisions (i) requiring that the Agents comply fully with this Section 19 of this Code and all applicable laws, rules and regulations, including anti-corruption laws, (ii) affording the Corporation appropriate monitoring and audit rights, including rights to access to books and records of the Agent, and (iii) allowing the Corporation to terminate the relationship in the event of non-compliance with any anti-corruption-related undertaking. Finally, an Agreement should require that, at the time it is executed, and whenever otherwise requested by the Corporation, the Agent will sign a certification confirming its compliance with Section 19 of this Code and the applicable anti-corruption laws.

Payments to Agents should never be made in cash, and should be made to the Agent's bank account in the country where the services are performed or where the Agent's offices are located.

c. "Red Flags" or Other Warning Signs

If, for any reason, any employee of the Corporation has reason to suspect that an Agent is engaging in potentially improper conduct, no further payments should be made until an investigation can be conducted. While not exclusive, the following warnings or "red flags," which may be present before entering into or during the term of an Agreement, are signs that an Agent might be engaged in inappropriate or illegal activity:

- The Agent has a history or reputation for bribes or other unlawful conduct;
- There is a history or reputation of corruption in the country where the Agent being hired;
- Unusual or excessive payment requests, such as requests for over-invoicing, up-front payments, ill-defined or last-minute payments, success fees, unusual commissions, or mid-stream compensation payments;
- Requests for payment to a third party, to a numbered account, or in cash or other untraceable funds;
- Use of holding companies or other methods or parties to obscure ownership or participation of the Agent, without adequate business justification;
- Any refusal by the Agent to provide records and documents.

d. Facilitating payments

Although some anti-bribery laws permit payments to government officials in limited circumstances for the purpose of facilitating or expediting the administrative performance of routine

governmental actions, it is the Corporation's policy that no such payments may be made.

e. Exceptions

Any exception to Section 19 of this Code, including with respect to payments arrangements, must be approved in advance **by the Board of Directors**.

20. Waivers of This Code of Business Conduct and Ethics

Any waiver of this Code with respect to a director or officer of the Corporation may be made only by the **Board of Directors or the Audit Committee**. Any such waiver will be promptly disclosed to the extent required by applicable laws or stock exchange regulations.

21. Reporting of any Illegal or Unethical Behavior

We have a strong commitment to conduct our business in a lawful and ethical manner. Employees are encouraged to talk to supervisors, managers or other appropriate personnel when in doubt about the best course of action in a particular situation and are required to promptly report violations of laws, rules, regulations or this Code to your manager, the Corporation's General Counsel or the Chair of the Audit Committee. **Potential violations of the anti-bribery provisions should be reported directly to the Chair of the Audit Committee or through the Whistleblower Program.** In addition, complaints and concerns regarding questionable accounting, internal control or auditing matters should be submitted to a Chair of the Audit Committee or to the Whistleblower Program. Such submissions may be made confidentially and anonymously if desired.

We prohibit retaliatory action against any employee who, in good faith, reports a possible violation. It is unacceptable to file a report knowing it to be false.

22. Compliance Procedures

This Code cannot, and is not intended to, address all of the situations you may encounter. There will be occasions where you are confronted by circumstances not covered by policy or procedure and where you must make a judgment as to the appropriate course of action. Since we cannot anticipate every situation that may arise, it is important for the Corporation to set forth a general way to approach a new question or problem. These are the steps to keep in mind:

- Make sure you have all of the facts. In order to reach the right solutions, you must be as fully informed as possible.
- Ask yourself what you are specifically being asked to do. This analysis will enable you to focus on the specific issues that are raised and the available alternatives. Use your judgment and common sense. If something seems unethical or improper, it probably is.
- Clarify your responsibility and role. In most situations, there is shared responsibility. Are your colleagues informed? It may help to get others involved and to discuss the problem.
- Discuss the problem with your supervisor. This approach is best in most if not all situations. Your supervisor may be more knowledgeable about the issue and will appreciate being brought into the process. It is a supervisor's responsibility to help you to solve problems.

• Seek help from Corporation resources. In the rare instance in which it may not be appropriate to discuss an issue with your supervisor, or in which you feel uncomfortable approaching your supervisor you have the option to:

- report the issue using Corporation's anonymous Whistleblower system
- discuss the problem with the Corporation's general legal counsel; or
- If you prefer to write, address your concerns to the Corporation's general legal counsel or the Chief Executive Officer.

• You may report ethical violations in confidence and without fear of retaliation on the Whistleblower phone lines. If your situation requires that your identity be kept secret, the Corporation will protect your anonymity. The Corporation does not permit retaliation of any kind against employees for good faith reports of ethical violations. An officer or employee who retaliates against someone who has reported an ethical violation in good faith is subject to discipline up to and including termination of employment. These procedures are intended to encourage and enable employees and others to raise serious concerns within the Corporation rather than seeking resolution outside the Corporation.

• Ask first. If you are unsure of the proper course of action, seek guidance before you act. If you do not feel comfortable discussing the matter with your supervisor, please call the Corporation's general legal counsel. If you require an interpreter, every reasonable effort will be made to provide you with one. We strive to ensure that all questions or concerns are handled fairly, discreetly and thoroughly.

23. Whistleblower Laws

The obligations of confidentiality set forth in this Code and the Code of Ethical Conduct for Financial Managers are subject to applicable whistleblower laws, which protect your right to provide information to governmental and regulatory authorities. You are not required to seek the Corporation's permission or notify the Corporation of any communications made in compliance with applicable whistleblower laws, and the Corporation will not consider such communications to violate this or any other Corporation policy or any agreement between you and the Corporation.

I, _____, **acknowledge**
having read and understood this Code of Conduct
and agree to comply with it at all times.

Signature

Date

EFFECTIVE DATE

This policy was reviewed by the Corporate Governance and Nominating Committee and last approved by the board of directors on August 6, 2026.