# PROHIBITED BUSINESS PRACTICES POLICY

Policy Number: 130:14
Effective Date: June 2008
Revision Date: August 2026
Applies To: All TTI Family of Companies

Created By: Compliance
Approved By: Senior Staff
Reviewed Date: August 2026

## PURPOSE

It is the policy of Berkshire, and TTI, to comply with all laws and regulations that apply to any of their activities and operations, or that may give rise to the risk of liability for Berkshire, its subsidiaries, or persons employed by any of them.

This Prohibited Business Practices Policy ("Policy") applies to all officers, directors, and employees of Berkshire and TTI. Using a risk-based approach, each subsidiary shall develop a procedure to communicate the requirements of this Policy to its Intermediaries. Each person shall comply with this Policy, abide by all applicable laws and regulations, and exercise great care not to take or authorize any actions that may create even the appearance of illegal conduct or other impropriety. Persons who violate this Policy shall be subject to appropriate disciplinary action up to, and including, termination of employment. **Berkshire and its subsidiaries will not undertake, authorize, or tolerate any business practice that does not comply with this Policy.**

If you have questions about this Policy, contact John Archer, Manisha Kadoche, Andrea Palmer or contact the Chief Financial Officer, Director of Internal Audit or Senior Manager of Ethics and Compliance at Berkshire.

## POLICY

## I. IMPLEMENTATION AND TRAINING

***Distribution.*** General managers of Berkshire subsidiaries are responsible for the enforcement of and compliance with this Policy within their area of responsibility, including the distribution of this Policy to Senior Management reporting to them, and other individuals that manage the risk areas discussed in this document, including each employee, agent, or manager who is likely to communicate, interact, or have business dealings with government officials or manage persons likely to communicate, interact, or have business dealings with government officials. Berkshire subsidiaries should make compliance policies accessible to employees electronically in their native languages. Berkshire subsidiaries must utilize appropriate technology and consider employing data analytics to monitor and understand compliance risks. Berkshire subsidiaries shall ensure that compliance personnel charged with administering the compliance program receive specialized training to enable them to effectively perform their roles.

***Training.*** This Policy, along with any related or more robust subsidiary policies, must be included in employee manuals or where employee policies are displayed. It should be provided to Senior Management and made available to all employees in English and any applicable local languages. Training must be provided to managers and employees who interact with government officials or influence trade compliance and must include a review and explanation of the areas covered by this Policy—namely anti-corruption, sanctions, export controls, anti-boycott, and customs compliance. Training should be periodic, tailored to the audience's role, expertise, and risk exposure, and conducted in the audience's native language when appropriate. Intermediaries with potential government interaction must either have adequate training programs or receive training from the subsidiary on a risk-based approach, including periodic refreshers. Training should allow for questions (if live), address past compliance incidents, and incorporate lessons learned from industry peers. Subsidiaries must regularly evaluate training effectiveness to ensure personnel have the tools and knowledge to uphold compliance standards.

***Periodic Risk Assessments.*** Each Berkshire subsidiary shall regularly assess and review its individual operations and compliance risks and document an annual risk assessment that captures the compliance risk areas discussed in this Policy that are applicable to the subsidiary. Subsidiaries should update that risk assessment as the risk profile of the subsidiary changes and adopt additional policies and procedures, as appropriate, so that it maintains an effectively designed compliance policy that is tailored to the unique compliance risks the subsidiary faces. Each subsidiary is required, based upon an examination of its risk assessment and the history of the operation of its compliance program (including compliance policy violations), to devote sufficient resources to administer its compliance program, including this policy, and is required to appoint a high-level executive to be responsible to administer its compliance program.

The risk assessment should take into consideration the management of emerging risks to ensure compliance with applicable laws. Specifically, Berkshire subsidiaries are required to have a process for identifying and managing external risks that could potentially impact the company's ability to comply with the law, including risks related to the use of new technologies such as artificial intelligence ("AI").

Berkshire subsidiaries are required to periodically assess and monitor the effectiveness of their compliance program, including examining instances where violations of compliance policies have been detected, and, where possible, implement improvements designed to prevent such violations in the future. Compliance assessments and testing should integrate data analytics capabilities wherever possible. Each subsidiary should also incorporate lessons learned from publicly known successes and failures of peers in their industry or geographic region relating to anti-corruption, sanctions, trade compliance, compliance practices, and policies into this periodic assessment. In performing this assessment, subsidiaries or their outside counsel shall consider the U.S. Department of Justice's Guidance Document on the Evaluation of Corporate Compliance Programs and evaluate the program considering the following three fundamental questions:

- Is the compliance program well designed?
- Is the compliance program adequately resourced and empowered to function effectively?
- Does the compliance program work in practice?

https://www.justice.gov/criminal-fraud/page/file/937501/download

***Disciplinary Action.*** Because Berkshire is committed to compliance with the law and this Policy, **the failure of any Berkshire subsidiary personnel to comply with this Policy will result in disciplinary action up to, and including, termination of employment.** Disciplinary action may also be taken against the manager of an employee who violates this Policy should the manager fail to properly supervise the employee or know that the employee is engaging in behavior that violates the Policy and fails to stop or prevent such behavior. Berkshire subsidiaries should establish mechanisms to reduce or claw back compensation, where permitted by law, if it determines that this Policy has been violated. Violations may include direct breaches, failure to report known violations, or withholding relevant information.

## II. REPORTING AND INVESTIGATIONS

***How to Report Concerns.*** Any Berkshire subsidiary employee who has a question about whether conduct might be illegal or involve any unethical or improper act or violate this Policy must promptly report those concerns. Each Berkshire subsidiary, or in the case of a group of Berkshire companies, the Berkshire subsidiary that is the "parent" of such group, shall designate a Compliance Officer ( John Archer) to receive and investigate such reports and to implement this Policy. Employees may also report their concerns to their supervisors or managers. If permitted by local law, anonymous reports can be made via the Berkshire Ethics and Compliance Hotline (1-800-261-8651) in the U.S. and Canada or by using Berkshire's web reporting site, which is located at www.brk-hotline.com.

Berkshire prohibits retaliation of any kind when making such a report in good faith, even if it turns out that the conduct being reported is not illegal or improper. Berkshire subsidiaries are required to have policies and training related to anti-retaliation and whistleblower protection. Berkshire subsidiaries should communicate that employees have an obligation to report misconduct.

Berkshire recognizes that the circumstances of each internal investigation are unique and may require different procedures. Therefore, Berkshire subsidiaries should consider establishing and documenting a process to manage internal investigations that originate through the hotline or any other source. This process should specify which employees are responsible and generally how the investigation should be conducted. Berkshire subsidiaries need to provide a detailed written report that describes the investigative steps and outcomes. This documented process should include analyzing misconduct and incorporating lessons learned.

***Your Cooperation is Required.*** Every employee of Berkshire or a Berkshire subsidiary is required to cooperate with any effort by Berkshire, outside legal counsel, or forensic accountants hired by Berkshire to investigate whether a violation of any compliance policy of Berkshire or any Berkshire subsidiary has occurred or whether the compliance program is operating effectively. Such cooperation includes promptly providing information that is requested and participating in interviews, investigations, and audits. Any failure to cooperate as required under this provision could result in disciplinary action up to, and including, termination of employment.

## III. COMPLIANCE WITH BOTH U.S. AND FOREIGN ANTI-CORRUPTION LAW IS REQUIRED

This Policy sets forth Berkshire's position against bribery and corruption and describes the minimum procedures that must be followed to ensure compliance with this Policy and anti-bribery and anti-corruption laws. This Policy (1) identifies certain specific laws and regulations that may apply to a Berkshire subsidiary's operations, and (2) sets forth the minimum standards that must be followed to ensure compliance with those laws and regulations. The applicable laws and regulations include not only federal, state, and local laws and regulations of the U.S., but also laws and regulations of any foreign countries in which a Berkshire subsidiary does business, such as the United Kingdom's Bribery Act of 2010 and the Brazil Clean Company Act of 2014. Because the United States Foreign Corrupt Practices Act of 1977 ("FCPA") is the anti-corruption law that most broadly affects Berkshire's international business, this Policy uses that statute as a framework for setting forth Berkshire's Policy. However, the Policy uses the term "government official" in most places, where the FCPA uses the term "foreign official," to make it clear that Berkshire's Policy applies to interactions with all government officials worldwide, and that adherence to the principles and procedures set forth within this Policy will ensure compliance with all nations' anti-bribery and anti-corruption laws.

Although the current administration signaled in early 2025 a shift in FCPA enforcement priorities, including a temporary 180-day pause and later adopting a more selective approach focused on cartels, transnational criminal organizations, and conduct that undermines U.S. interests, Berkshire and its subsidiaries remain fully committed to compliance with the FCPA. We continue to maintain robust anti-corruption policies and uphold ethical business practices worldwide, regardless of changes in enforcement trends.

## IV. PROHIBITED OFFERS OR PAYMENTS

Each Berkshire subsidiary must comply with the FCPA and all other applicable anti-bribery and anti-corruption laws. The FCPA prohibits bribes, kickbacks, and favors to government officials to obtain an improper advantage or benefit, such as, among other examples, the awarding or retention of business or a government contract, obtaining a tax benefit or reduction of value-added tax or corporate income taxes, or obtaining a permit or license. Other U.S. and foreign laws prohibit bribery of non-governmental personnel (sometimes called "commercial" bribery).

***All Improper Payments Prohibited.*** Berkshire subsidiaries, subsidiary employees, and Intermediaries are prohibited from promising, authorizing, offering, or paying bribes or kickbacks to ***any person***, ***anywhere in the world*** under any circumstances for the purpose of improperly influencing their actions or gaining any improper business advantage. In addition, they must not receive such payments from any person or company in return for providing an improper advantage such as awarding business to such person or company. Berkshire subsidiary employees must exercise care when providing meals, gifts, or other business courtesies. Providing modest business courtesies in a commercial setting to create goodwill may be permissible but providing or offering lavish business courtesies with the intent or expectation of obtaining more favorable business terms or opportunities that otherwise would not be available is prohibited.

***Prohibited Purposes.*** To ensure compliance specifically with the FCPA, no Berkshire subsidiary or its Intermediaries may improperly provide, authorize, promise, or offer to provide anything of value to a government official for any of the following purposes:

- Improperly influencing the official.
- Securing any improper advantage.
- Affecting any official decision.
- Assisting the Berkshire subsidiary in obtaining or retaining business, or in directing business to another person or company.

Similarly, no Berkshire subsidiary, its employees or Intermediaries may authorize a third party to improperly offer or promise to provide something of value to a government official for any of the purposes listed above.

***"Corrupt" Payments.*** The FCPA prohibits promising, providing, offering to provide, or authorizing the provision of things of value to a government official if done "corruptly." This means that the giver has an intent or desire to improperly influence the recipient and to get something in return (*i.e.*, a *quid pro quo)*. The word "corruptly" is used in the FCPA to clarify that the offer, payment, promise, or gift must be intended to induce the official to misuse an official position to assist the giver in obtaining a business advantage.

***Government Officials.*** Under the FCPA, a government official is:

- Any officer or employee of a government or any department, agency, or instrumentality of a government.
- Any Elected officials.
- Any officer or employee of a public international organization such as the United Nations or World Bank.
- Any individual acting in an official capacity for or on behalf of a government agency, department, instrumentality, or of a public international organization.
- Any officer or employee of a company owned or controlled by a government (*e.g.,* a state-owned oil company or state-owned hospital).

- Political parties outside of the U.S. and their employees.
- Candidates for political office outside of the U.S.
- Any member of a royal family who may lack formal authority but who may otherwise be influential, including by owning or managing state-owned or controlled companies.

It is important to note that employees of state-owned or controlled entities (whether partially or completely state-owned or controlled) are considered government officials under the FCPA regardless of their rank, nationality, or classification under local law. Some individuals, who may not be considered government officials in their own country, are considered government officials under the FCPA (for example, doctors and nurses employed by a state-run healthcare system, or employees of a state oil company). In addition, a company may be under government control even if it is publicly traded, and even if some of its stock is not owned by the government. For purposes of this Policy, close family members of government officials (*i.e.,* brother, sister, mother, father, husband, wife, or child) are treated as government officials. The Policy's prohibitions also apply with regard to former government officials in cases where the former government official retains some sort of quasi-official status.

***Indirect and Direct Payments.*** The prohibition against improper payments or gifts under the FCPA applies not only to direct payments or offers of payment, but also to indirect offers or payments made through any Intermediaries. Care must be taken to ensure that Intermediaries of a Berkshire subsidiary do not authorize, promise, offer, or provide anything of value to a government official for any of the prohibited purposes described above.

***Anything of Value.*** The term "anything of value" is construed very broadly under the FCPA and includes far more than just monetary gifts. Each of the following, among other things, could constitute a thing of value:

| Cash and Financial | Hospitality Leisure | Goods and Property | Other Benefits |
|---|---|---|---|
| Money (cash, check, wire, vouchers, prepaid cards) | Meals and drinks | Art | Contractual rights |
| Excessive commissions | Entertainment (golf, sporting events) | Vehicles | Donations to charity |
| Sales below market value (discounts) | Flights on private or subsidiary aircraft | Personal gifts | Scholarships for family members |
| Purchases above market rates | Vacations | Excessive discounts on products/services | Other types of gifts |

The term also applies to intangible benefits such as contributions to an official's preferred charity, offers of employment or internships for an official's friends or family, assisting an official's family member or friend in gaining admittance to a school, visa sponsorship, or other kinds of help or assistance to officials or their friends and family. This Policy applies equally to offers of payment and things of value to relatives and family members of government officials, as to the government officials themselves.

***Nominal Gifts and Entertainment.*** There are circumstances under which providing inexpensive items to a government official may be permissible under the FCPA. For instance, providing gifts of nominal value such as pens or mugs with the Berkshire subsidiary logo, without any intent to improperly influence the official, is acceptable. Before providing even nominal gifts or entertainment to a government official, Berkshire subsidiary employees or the subsidiary must confirm that doing so is permitted by local law. Some countries prohibit providing anything of value to government officials, even gifts or entertainment of nominal value; in those countries, this Policy prohibits providing gifts or entertainment of any kind to government officials.

Any gift or entertainment provided to a government official must be modest in value, customary for the country, and made openly—not secretly—with no intent to improperly influence the official or secure a specific action. It must never be in the form of cash or cash equivalents and should promote general goodwill rather than serve as a quid pro quo. The cumulative value of all gifts or entertainment provided to the same official within a calendar year should be considered when assessing modesty. All such expenditures must be accurately recorded in the subsidiary's books and records.

***Willful Blindness Is Not a Defense.*** The FCPA imposes liability on companies and individuals even if they have no actual knowledge of an improper payment to a government official, in circumstances where they should have known there was a high probability that an Intermediary intended to make or was likely to make an improper payment. Accordingly, subsidiaries and subsidiary employees must not be willfully blind to facts which suggest improper payments, gifts, promises or offers of payments, gifts, or something of value to a government official. Liability for an FCPA violation cannot be avoided by attempting to ignore or "not see" the warning signs or indications of improper conduct. Employees who suspect or see indications that corrupt payments or offers of payment might be under consideration or might have been made on a Berkshire subsidiary's behalf must not "look the other way" or ignore the indications or "red flags." The lack of actual knowledge of a bribe will not be a defense under the FCPA.

***Bona Fide and Reasonable Business Expenses.*** The FCPA allows payment of legitimate travel and lodging expenses for government officials when directly related to promoting products or services, executing a contract, or supporting charitable or educational programs. Berkshire subsidiaries may only cover such expenses with advance written approval from the applicable Berkshire subsidiary's Compliance Officer, and only if permitted under local law and approved in writing by the official's government or agency. The FCPA permits paying bona fide and reasonable travel and lodging expenses for government officials.

Such expenses for government officials must be **reasonable (modest and not lavish)** and limited to travel and accommodation expenses that are incurred for a government official's direct travel to and from the location of the Berkshire subsidiary event or location. Expenses for government officials must not cover side trips, tourism, or extra days. Lodging should be reasonable, including meals incidental to business-class hotel stays during the event or travel. Payments should be made directly to service providers

whenever possible, supported by receipts, and properly recorded. Per diem allowances are prohibited, and no expenses may be paid for a government official's spouse or family members.

***Political Contributions.*** Any political contribution made must be consistent with local law and in compliance with the FCPA, and cannot be made to obtain or retain business, direct business to another person or entity, or to obtain an improper advantage. No political contribution should be made outside of the U.S. without:

- The receipt of written legal advice by local counsel concerning the legality of the contribution under local law.
- The receipt of written legal advice from U.S. counsel concerning the legality of the contribution under the FCPA.
- Prior written approval of the applicable Berkshire subsidiary's Compliance Officer or other appointed representative such as the subsidiary's Legal Department.

***Charitable and Educational Contributions.*** Any charitable or educational contribution, including expenses for travel, lodging, or meals, must be consistent with local law and in compliance with the FCPA, and cannot be made to obtain or retain business, direct business to another person or entity, or to obtain an improper advantage. Berkshire and its subsidiaries should perform and document appropriate risk-based due diligence prior to making a charitable or educational contribution outside of the U.S. to determine if "red flags" exist which might increase the anti-corruption compliance risk associated with making the contribution.

***The FCPA's Accounting and Internal Control Provisions.*** The FCPA imposes strict accounting and recordkeeping requirements on Berkshire (as a public company) and each of its consolidated subsidiaries. These accounting provisions have two primary components: the books and records provision and the internal controls provision.

*Books and Records*

The accounting provisions require Berkshire and its consolidated subsidiaries to maintain books and records which accurately and in reasonable detail reflect transactions and the disposition of assets. This requirement extends not only to the general ledgers but also to all documents that describe business transactions and dispositions of assets such as invoices, receipts, expense reports, purchase orders, and shipping documents. False, misleading, or incomplete entries in Berkshire subsidiary books and records are prohibited. This Policy also prohibits the maintenance of undisclosed or unrecorded funds or accounts. Because the books and records provision does not include a materiality requirement, any false record, no matter what the amount, can give rise to an FCPA violation. Therefore, all personnel must take responsibility for compliance with the books and records requirements of the FCPA. No employee should assume that accurate books and records are the responsibility of just those in finance and accounting.

*Internal Controls*

The internal controls provision of the FCPA requires Berkshire and its controlled subsidiaries to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that:

- Transactions are executed in accordance with management's general or specific authorization.
- Transactions are recorded as necessary to permit preparation of financial statements in conformity with generally accepted accounting principles or any other criteria applicable to such statements and maintain accountability of assets.
- Access to assets is permitted only in accordance with management's general or specific authorization.
- The recorded accountability for assets is compared with the existing assets at reasonable intervals and appropriate action is taken with respect to any differences.

For subsidiaries that are minority-owned by Berkshire, Berkshire's obligation is to make a good faith attempt to use its corporate governance practices/guidelines to cause the subsidiary to comply with the FCPA's internal controls requirement above. This applies equally to Berkshire subsidiaries that have non-controlling interests in joint ventures.

It is therefore the policy of each Berkshire subsidiary that all transactions be recorded in a timely, consistent, and accurate manner in terms of amount, accounting period, purpose, and accounting classification. Furthermore, each Berkshire subsidiary must abide by the following rules:

- Each transaction or disposition of assets by a Berkshire subsidiary must have proper authorization. Receipts must be obtained and kept for any travel, gifts, or entertainment provided to a government official. A request for reimbursement for such expenses must be accompanied by supporting documentation including: (a) a description of the expenditure, (b) its purpose, (c) identification of the recipient of the funds, (d) the amount of money spent, and (e) the manner of payment. These records should be periodically monitored for compliance with this Policy.
- An invoice or statement on agency letterhead indicating the services provided and the amount due must support any payment to a government agency or official.
- No secret or unrecorded fund or asset of a Berkshire subsidiary shall be created or maintained, and no accounting balances shall be created or maintained that do not have supporting documentation, are fictitious in whole or in part or have no reasonable basis in fact.
- No checks of a Berkshire subsidiary may be written to "cash," to "bearer," or to third-party designees of a party entitled to payment. Other than documented petty cash transactions, no cash transactions may be made,

unless such transaction is evidenced by a receipt bearing the signature of the recipient and the recipient is a party with whom the relevant Berkshire subsidiary has a written contract.

- All petty cash accounts must be maintained with strict controls to ensure that no cash is dispensed without the proper approvals. Approval must be subject to the recipient's demonstration that the funds are to be expended only for a proper purpose. The use of cash should be limited to the extent possible, and all uses of petty cash must be appropriately documented with third-party receipts, where practicable. Documentation supporting petty cash transaction should include: (a) the business purpose for the use of the cash, (b) the date, (c) the amount paid, (d) the name of the person dispensing the cash, (e) the name of the person receiving such cash from the Berkshire subsidiary account, and (f) the name of the ultimate recipient of the cash, if different.
- Payments to Intermediaries should be made only in the country where the Intermediary provides the services or in the country, if different, in which the Intermediary has its headquarters. The practice of transferring funds to accounts in countries other than the location of the services or the Intermediary's headquarters is not permissible unless the Intermediary provides a valid business purpose, proper supporting documentation, and the transactions are authorized by the designated Berkshire subsidiary's Compliance Officer.
- Access to systems of accounting or financial records shall not be given to individuals without proper authorization. Destruction or removal of a Berkshire subsidiary's records may be undertaken only in compliance with such Berkshire subsidiary's internal policy and the policy of Berkshire.

Any individual who has reason to believe that a violation of the foregoing rules may have occurred at any Berkshire subsidiary, including that a payment to a government official was mischaracterized in a Berkshire subsidiary's books and records, must promptly report that concern to a supervisor or Compliance Officer or through the Berkshire Ethics & Compliance Hotline. Any inquiry from the internal or independent auditors of a Berkshire subsidiary must be responded to fully, accurately, and promptly.

***Penalties.*** A violation of the FCPA can result in serious consequences for Berkshire, a Berkshire subsidiary, and for the individuals involved. These include significant monetary and criminal penalties up to imprisonment for individuals. Monetary penalties for companies have exceeded $1 billion in egregious cases.

## V. PROHIBITED TRANSACTIONS WITH CERTAIN COUNTRIES/ REGIONS AND PERSONS

Each Berkshire subsidiary and its employees must comply with all applicable economic and trade sanctions and embargo programs under U.S. law, United Nations resolutions, and the laws and regulations of other countries to which they are subject. Compliance requires careful monitoring of, and sometimes prohibition of, transactions involving sanctioned countries and regimes and sanctioned individuals, entities, vessels, aircraft,

and cryptocurrency wallets (*e.g.,* terrorists, proliferators of weapons of mass destruction, and narcotics traffickers). In most cases, violations can result in criminal penalties of up to 20 years in jail, a $1 million fine, or both, and civil penalties per violation in an amount up to the greater of $377,700 or twice the value of the transaction involved. However, depending on the type of violation and the statutory regime implicated, the applicable penalties vary. In 2024, the statutes of limitations and recordkeeping requirements for U.S. economic sanctions and embargo programs were extended from five years to ten years. This ten-year limitation period applies retroactively to any violation that occurred after April 24, 2019. Berkshire subsidiaries are expected to update their internal policies and procedures to reflect this change.

Most of the trade restrictions described in Section V of this Policy apply to "U.S. persons," which include all (i) companies organized in the U.S. and their foreign branches, (ii) companies and persons located in the U.S. or located outside of the U.S. who are otherwise subject to U.S. jurisdiction (*e.g.*, through utilization of the U.S. banking system, including **all** U.S. Dollar-denominated transactions occurring anywhere in the world), and (iii) U.S. citizens and permanent resident aliens wherever located (including U.S. persons acting on behalf of foreign persons). For purposes of the U.S. embargo of Cuba and the sanctions applicable to Iran, as described below, foreign entities owned or controlled by U.S. persons are also subject to these sanctions programs.

The policies set forth in this Section V must be adopted by all Berkshire subsidiaries that are organized in the U.S. or that have U.S. operations. Any Berkshire subsidiary that is organized outside of the U.S. and does not have U.S. operations or U.S. employees should carefully evaluate its legal obligations with respect to these trade restrictions, taking into account such factors as its ownership by Berkshire or other U.S. persons, the citizenship of its employees, the nature and location of its operations and third-party relationships (in particular banking relationships and use of U.S. Dollars), and whether it utilizes or sells goods, services, or technology subject to U.S. export controls, and shall adopt all portions of this Policy that are applicable to its operations, or are otherwise prudent, to the extent consistent with local law. Any potential conflict between local law and the trade restrictions described below should be addressed by the Compliance Officer of the affected Berkshire subsidiary in consultation with legal counsel and the Chief Financial Officer of Berkshire, Director of Internal Audit of Berkshire, or the Senior Manager of Ethics and Compliance of Berkshire.

***Below is more specific information regarding certain country or activity-specific sanction programs:***

***Transactions with Cuba, Iran, North Korea, and certain occupied or annexed regions of Ukraine.*** The U.S. has instituted comprehensive embargoes against the following countries/geographical regions:

- Cuba
- Iran

- North Korea
- The “Donetsk People’s Republic,” “Luhansk People’s Republic,” Crimea Region, and certain portions of the Zaporizhzhia and Kherson regions (Russian-occupied portions of Ukraine)

These sanctions programs include an embargo or prohibition (with certain exceptions) barring U.S. persons from engaging in trade, commercial, or financial transactions involving the individuals and entities located in the above countries/regions. Some non-exhaustive examples of dealings that may be restricted include:

- Imports into the U.S., and, in some cases, into other countries, of goods, technology, software, or services from, or originating in, the embargoed country/region.
- Exports from the U.S. or, in some cases, from foreign countries, of goods, technology, software, or services, either directly or through Intermediaries, to the embargoed country/region.
- Investments in the embargoed country/region.
- Brokering the sale of goods, technology, or services to or from the embargoed country/region, even if the transaction is done entirely outside of the U.S.
- Providing insurance or reinsurance to businesses or property of the embargoed country/region or its nationals, or for imports from, or exports to, the embargoed country/region or its nationals.
- Other transactions in which a financial institution or other person acting on behalf of the embargoed country/region has any interest.

The embargo programs are subject to frequent changes. Detailed information regarding these embargoes, including “FAQs” and other guidance, can be obtained from the Office of Foreign Assets Control (“OFAC”) website at https://home.treasury.gov/policy-issues/financial-sanctions/sanctions-programs-and-country-information. Employees responsible for compliance at Berkshire subsidiaries are encouraged to consult the OFAC website regularly and to sign up to receive email announcements from OFAC when changes occur or new information or guidance becomes available.

In addition, no Berkshire or Berkshire subsidiary employee or representative may travel for business to the embargoed countries listed above without the prior written approval of the Compliance Officer of the Berkshire subsidiary. If such travel is approved, it may be undertaken only in accordance with any conditions of approval. Furthermore, regardless of whether the travel is for business or for personal reasons, no Berkshire or Berkshire subsidiary employee may carry Berkshire or Berkshire subsidiary issued devices into those countries (e.g., laptops, mobile phones, tablets or other mobile devices, etc.), and no employee’s personal mobile device carried on such travel may include any application(s) that allow access to any Berkshire or Berkshire subsidiary’s email system or network.

In light of the complexity of the laws and sanction programs described in this section, **no Berkshire subsidiary to which this Section V applies may engage in any transactions or conduct of the type described above and below that is known to, directly or indirectly, involve, Cuba, Iran, North Korea, Russia, Syria, Venezuela or the above-referenced occupied regions in Ukraine**, without prior consultation with the Compliance Officer of the affected Berkshire subsidiary in consultation with legal counsel and the Chief Financial Officer of Berkshire, Director of Internal Audit of Berkshire or Senior Manager of Ethics and Compliance of Berkshire.

***Transactions with Syria***. Until 2025, Syria was the target of comprehensive U.S. sanctions, similar to those country programs targeting Cuba, Iran, North Korea, and the occupied regions in Ukraine discussed above. In July 2025, in the wake of a new government taking control of Syria, OFAC removed its comprehensive sanctions program. In September 2025, the U.S. Department of Commerce followed suit and issued new licenses permitting export to Syria of a significant number of U.S.-origin products. That said, meaningful list-based sanctions restrictions remain in effect in Syria, and export of U.S.-origin products is subject to significant end use restrictions and limitations. Despite providing sanctions and export control relief, the U.S. continues to designate Syria as a State Sponsor of Terrorism. Commercially, Syria is a very challenging jurisdiction in which to do business. Given the tenuous situation on the ground, and because of the risk that sanctions may be reimposed if the new Syrian government engages in harmful activity, **any transaction involving Syria must be approved by the Senior Manager of Ethics and Compliance of Berkshire.**

***Transactions with Venezuela***. Due to ongoing and increasing concerns of the U.S. Government regarding political and social developments in Venezuela, OFAC and other federal agencies have developed and implemented sanction programs relative to a variety of specific industries, government agencies, individuals, and entities. The various sanction programs, when considered together considering their breadth and complexity, make this a *de facto* embargo on dealings with Venezuela. Therefore, Berkshire has a policy of not doing business with or in Venezuela, or with individuals or entities that constitute the government of Venezuela. **Any contemplated transaction with Venezuela must be approved by the Senior Manager of Ethics and Compliance of Berkshire.**

***Russian Sanctions and Export Restrictions.*** **Berkshire has a policy of not doing business in or with Russia.** Prior to doing any business involving Russia, Berkshire subsidiaries must adopt detailed written operating policies and procedures regarding how business will be conducted in compliance with these sanctions and annually submit such policies and procedures for the prior approval of the Chief Financial Officer of Berkshire, Director of Internal Audit of Berkshire, and the Senior Manager of Ethics and Compliance of Berkshire. This applies to revenue derived from Russia as well as supply chain and service provider relationships (*e.g.*, software development and coding). These Russian sanctions have been expanded and updated frequently and likely will continue to evolve until the Ukraine conflict ends. Under the U.S. sanctions, for example, hundreds of Russian companies, most banks, dozens of high-net worth

Russians, and the companies they own, or control are the subject of complete prohibitions on business with the U.S. Also notable is a complete prohibition on "new investment" in Russia by U.S. persons.[1] As a consequence of this prohibition, U.S. persons may not buy equity securities or debt from, or otherwise lend to, **any Russian-domiciled entity**. They similarly may not engage in such business with non-Russian entities that have more than half of their revenue or assets in Russia, or where the purpose of the investment is to support activities in Russia. U.S. persons are also prohibited from making new capital expenditures to build new facilities or factories or to engage in new business operations in Russia. Russian subsidiaries of U.S. companies may continue to maintain (but not grow) pre-existing operations, subject to a number of other sanctions restrictions about who they sell to, bank with, and interact with in the government.

The U.S. also prohibits U.S. persons from providing a number of services to the Russian economy, regardless of whether the recipient is the target of list-based sanctions. The services bans include: accounting, trust, and corporate formation services; management consulting services; architecture and engineering services; quantum computing services; and information technology ("IT") and software services. Similar sanctions target involvement in the production and transport of Russian oil and gas, including a prohibition on providing nearly any services (including insurance) with respect to the maritime transport of Russian oil unless within certain price caps. Russian companies that operate in the above sectors or in finance, metals/mining, and aviation are at increased risk for being targeted by list-based sanctions.

Changes to U.S. export controls prompted by the Ukraine conflict have the effect of presumptively denying export of nearly any U.S.-controlled items to Russia. This includes, with limited exceptions, relatively ubiquitous encryption features found in computer software, among most "dual-use" hardware and technical information.
It is worth noting separately that legacy restrictions on certain debt or equity transactions with respect to Russia exist.[2] These prohibitions date back to 2014 and have largely been subsumed by the "new investment" ban discussed above, but they remain in force and should be evaluated separately.

***Transactions with China***. China is currently subject to extensive U.S. economic sanctions and export control measures that restrict dealings with Chinese companies or individuals and prohibit or place license requirements on certain U.S. exports and re-exports to China. Multiple U.S. Government agencies have updated their various lists to include Chinese Government entities and officials, as well as numerous private entities and individuals. Under the U.S. Export Administration Regulations ("EAR"), the U.S. Commerce Department's Bureau of Industry and Security ("BIS") Entity List identifies numerous well-known Chinese companies and their worldwide affiliates (such as

[1] See Executive Order 14071 and implementing "FAQs" promulgated by OFAC.

[2] For example, see Executive Order 13662 and implementing Directives 1 – 4 maintained by OFAC regarding prohibitions on new debt and equity and providing goods and services in support of deep water, Arctic offshore, and shale drilling in Russia.

Huawei) to whom exports and re-exports of items that are "subject to the EAR" are prohibited without a BIS license. In addition, the EAR applies end-use controls and an export and re-export license requirement (with a policy of denial) for certain commercial items when shipped to companies in China that also manufacture and support defense articles for use by the Chinese military or companies in China who support military intelligence[3]. The U.S. has also revised its treatment of Hong Kong, eliminating separate export licensing rules and requiring goods to reflect Chinese origin. Subsidiaries must comply with U.S. laws banning imports tied to forced labor, especially from Xinjiang. These restrictions are evolving rapidly, and Berkshire subsidiaries doing business with or in China must regularly review developments and ensure their policies and procedures remain compliant with current sanctions, export, and import requirements.

***Transactions with Certain Blocked Individuals, Entities, and Groups.*** The U.S. has also instituted economic and trade sanctions programs prohibiting U.S. persons, including companies located outside the U.S. who are owned by a U.S. parent, from engaging in unlicensed transactions of almost any nature with designated individuals, entities, vessels, aircraft, and cryptocurrency wallets. The U.S. Government identifies such individuals, entities, vessels, aircraft, and cryptocurrency wallets by putting their names on the list of Specially Designated Nationals and Blocked Persons (the "SDN List") maintained by OFAC. Other lists of parties with which various transactions are restricted or prohibited include the Foreign Sanctions Evaders List, the Sectoral Sanctions Identification List (the "SSI List"), and the Non-SDN Chinese Military-Industrial Complex Companies List, each as maintained by OFAC the Entity List, the Denied Persons List and the Unverified List, each as maintained by BIS; and the Debarred Parties List, as maintained by the U.S. Department of State's Directorate of Defense Trade Controls ("DDTC").

The SDN List includes individuals, entities, etc. that have engaged in conduct that is inimical to U.S. national security and foreign policy interests, such as "Transnational Criminal Organizations," "Narcotics Traffickers," "Terrorist Organizations," "Proliferators of Weapons of Mass Destruction" and other conduct such as cyber-related crime, election interference, corruption and human rights violations. Others on the list include persons and entities from the embargoed countries and regions described above (*e.g.*, Cuba, Iran, North Korea, and the Crimea, Luhansk and Donetsk Regions of Ukraine).

The SDN List is updated frequently (sometimes, as often as several times a week) and is available on the Internet at https://home.treasury.gov/policy-issues/financial-sanctions/specially-designated-nationals-and-blocked-persons-list-sdn-human-readable-lists.[4]

[3] To assist exporters in applying these controls, BIS introduced the Military End-Users List (found in Supplement 7 to Part 744 of the EAR) (and the Military-Intelligence End-Users List (found in Section 744.22 of the EAR).

[4] The OFAC website also offers a search engine for the SDN List and other lists maintained by OFAC at https://sanctionssearch.ofac.treas.gov/.

Persons subject to OFAC sanctions include not only persons named on the SDN List but also entities that are directly or indirectly 50% or more owned in the aggregate by one or more entity on the SDN List. Such entities must be treated as blocked or designated parties. Thus, it is important to know the ownership structure of companies with which transactions are conducted to determine whether the company, though perhaps itself not an SDN, is an SDN by application of OFAC's 50 Percent Rule. This analysis often includes an understanding of the companies' owners' owners. In addition to all persons and entities explicitly named on the SDN List or that are SDNs by application of OFAC's 50 Percent Rule, blocking requirements apply to the Governments of Cuba, Iran, North Korea, and all Iranian financial institutions.

In addition to being prohibited from engaging in transactions with SDNs, U.S. persons who come into possession or control of any property in which an SDN has any interest, must "block" or "freeze" such property (*e.g.,* by placing blocked funds in a blocked account) and report the blocking to OFAC within 10 business days. This is most often relevant in a banking context but may be a reason a seller (located anywhere in the world) is unable to be paid for services previously rendered or goods already delivered.

Before entering into any transaction and shipping goods, each Berkshire subsidiary should conduct applicable screening of parties (including vendors and customers) and, when applicable, their owners against the SDN and other restricted/denied party lists, including the SSI List, to identify any applicable restrictions that may prohibit or restrict the transaction. The U.S. Government has aggregated U.S. lists into the Consolidated Screening List which is available at https://legacy.export.gov/csl-search. In lieu of manual screening, there are a variety of third-party software vendors that can provide automated screening tools. Berkshire subsidiaries are required, as part of their risk assessments, to consider whether acquiring such a screening tool would be appropriate given the volume and nature of its transactions. Each Berkshire subsidiary that adopts a screening tool should ensure that it covers all applicable U.S. lists and all applicable lists of other countries in or with which the subsidiary does business.

Each subsidiary should develop a risk-based procedure to screen transactions and ensure compliance with any applicable prohibitions, sanctions, and embargoes. Subsidiaries should monitor compliance with Section V of this Policy.

No Berkshire subsidiary or employee to which this Section V applies may engage in any transactions, or conduct any activities with, any person, entity, vessel, aircraft, or cryptocurrency wallet on the SDN List (or any person who is otherwise blocked), whether directly, or indirectly, and any prospective dealings with persons on, or suspected to be on, the SDN List must be immediately reported to the applicable Berkshire subsidiary's Compliance Officer.

***Ransomware Payments.*** OFAC issued an advisory regarding the payment of ransom (or other extortion type payments) in connection with malware attacks. Persons associated with several types of malware have been added to the SDN List, including persons associated with Triton, Cryptolocker, SamSam, WannaCry 2.0 and Dridex, as

well as companies that facilitate financial transactions for ransomware actors, including SUEX. In addition, OFAC recently issued guidance designed to assist the virtual currency industry in complying with OFAC sanctions:

Sanctions Compliance for the Virtual Currency Industry

OFAC has stated that applications for licenses allowing ransomware payments to SDNs are subject to a presumption of denial. Berkshire subsidiaries who face ransomware demands from malicious cyber actors, or who provide insurance or reinsurance covering cyber ransomware demands or payments, should undertake due diligence to ensure that the party demanding a ransom payment is not an SDN or otherwise subject to trade sanctions. Requests for ransomware payments, where a Berkshire subsidiary is the victim, should be communicated to Berkshire and recorded in the Berkshire cyber-breach reporting portal. Ransomware or other extortion payment requests must only be made by the subsidiary when approved by Berkshire Senior Management and subsidiary Senior Leadership. In cases where the Berkshire subsidiary provided insurance or reinsurance covering cyber ransomware demands, such reinsurance claims should only be paid after compliance with the applicable written cyber ransomware due diligence procedures that have been approved by that subsidiary's Compliance Officer. OFAC also strongly recommends prompt reporting of such demands to law enforcement. OFAC's latest guidance on potential sanctions risks of facilitating ransomware payments contains important information regarding OFAC's expectations regarding reducing the risk of extortion by a sanctioned actor through adopting or improving cybersecurity practices, as well as cooperation with OFAC and law enforcement may be found at:

Updated Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments

The U.S. Cybersecurity and Infrastructure Security Agency has also urged organizations of all sizes to take measures to reduce their risk of ransomware attacks and improve their cybersecurity resilience, and has created the website www.stopransomware.gov, which brings together tools and resources from multiple federal government agencies that organizations can use to learn more about how ransomware works, how to protect themselves, how to report incidents and how to request technical assistance.

***Facilitation.*** No Berkshire subsidiary or employee, wherever located, may facilitate any transaction with any embargoed country, entity, or individual, etc. that is the subject of sanctions, including any SDN, without appropriate license or other authorization having been issued. "Facilitation" is "any unlicensed action by a U.S. person that assists or supports trading activity with [a sanctions target] by any person," with certain narrow exceptions (*e.g.,* activities of a "purely clerical" nature, or of a "reporting nature that does not further trade or financial transactions").

For example, prohibited "facilitation" occurs if a U.S. Berkshire subsidiary or any U.S. person anywhere in the world:

- Alters policies or procedures to permit a foreign affiliate to accept a transaction involving a prohibited party.
- Refers an inquiry or request to quote or bid from a party restricted or embargoed under U.S. law to a foreign subsidiary or affiliate
- Responds to a request for proposal involving a prohibited party or country.
- Formally or informally votes on a transaction (*e.g.*, as a board member), approves, directs, or executes transaction documents, where the transaction would be prohibited if performed by a U.S. person or within the U.S.
- Allows a foreign Berkshire subsidiary to utilize the resources of a U.S. Berkshire entity (*e.g.*, computer systems, licensed software, banking relationships, operational oversight, management, or legal services, *etc.*) to support its transactions, where the transaction would be prohibited if performed by a U.S. person or within the U.S.

If you receive a communication from a Berkshire foreign subsidiary that may be related to any transaction(s) that would be prohibited if performed by a U.S. person or within the U.S., please consult with your subsidiary's Compliance Officer before responding to that communication or engaging in discussion regarding the transaction.

Prohibited facilitation of the form described above may include knowing facilitation of fraudulent remote workers from embargoed countries. See Section X below for further discussion of fraudulent remote workers from North Korea.

***Secondary Sanctions.*** The U.S. Government also maintains "secondary sanctions" programs, in many cases mandated by legislation, under which sanctions can or must be imposed on foreign persons who engage in dealings with SDNs or other activities contrary to U.S. national security or foreign policy. Secondary sanctions seek to regulate the business of foreign companies that have no nexus to the U.S. by imposing consequences for engaging in such activities. Secondary sanctions are particularly prevalent in the context of the Iran and Russia sanctions programs, but many other sanctions programs also have secondary sanctions elements. Under secondary sanctions, foreign companies that do business with SDNs and embargoed countries can be subject to certain consequences that may affect their ability to do business with the U.S., including denial of access to the U.S. financial system or designation of the foreign person as an SDN. Berkshire's non-U.S. subsidiaries should inform themselves of secondary sanctions and consider possible secondary sanctions risks of dealing with SDNs or engaging in other dealings that could result in secondary sanctions exposure.

***Disclosure of Iran-Related Activities.*** Section 13 of the U.S. Securities Exchange Act of 1934 requires that certain issuers registered with the Securities and Exchange Commission ("SEC"), including Berkshire, disclose in their public filings and in separate reports to the SEC if the issuer or any of its affiliates has knowingly engaged in certain specified activities related to Iran and transactions or dealing with certain "blocked persons." For these issuers, quarterly and annual reports must include disclosure on all the reportable activities that occurred during the period covered by the report (*e.g.*, for

an annual report, during the fiscal year). Disclosure is required regarding the activities of each of Berkshire's subsidiaries, which are considered affiliates under the law.

A broad range of activities are reportable, including those relating to Iran's energy sector, military capabilities, suppression of human rights or involving certain financial transactions; or Iranian SDNs. Reportable activities include, among others:

- Certain activities relating to Iran's petroleum industry, such as providing insurance or reinsurance contributing to Iran's ability to import refined petroleum products.
- Certain activities contributing materially to Iran's ability to acquire or develop destabilizing numbers and types of advanced conventional weapons or weapons of mass destruction.
- Certain activities related to business with the Government of Iran.
- Certain activities supporting Iran's acquisition or use of goods or technologies that are likely to be used to commit human rights abuses against the people of Iran.

If employees of a Berkshire subsidiary have reason to believe that any potentially reportable activity has occurred, they must promptly report the matter to the Chief Financial Officer of Berkshire, Director of Internal Audit of Berkshire and Senior Manager of Ethics and Compliance of Berkshire, so that a determination may be made as to whether the activity is of the type required to be disclosed under U.S. law. Because there is no materiality threshold for transactions subject to the disclosure requirement, it is important that Berkshire be made aware of all such activities, even those that may seem minor or incidental.

***Ongoing Compliance.*** As anti-terrorism and foreign policy programs evolve and related rules change, the nature and extent of permitted and prohibited activities could change; for instance, additional countries or persons could become subject to embargoes or sanctions programs, or existing embargoes could be lifted, or sanctions programs relaxed. Also, additional, or different requirements may be applicable to Berkshire companies that are not U.S. persons or that are doing business outside of the U.S. Each Berkshire subsidiary should monitor applicable sanctions programs and other trade restrictions to ensure that its policies remain current. Berkshire subsidiary employees should consult with their Compliance Officer to confirm compliance with applicable requirements before entering any contractual or business relationship with persons or involving countries implicating potential embargoes or sanctions programs. Berkshire subsidiaries should retain all OFAC related records (including screening records, license information, etc.) for a minimum of ten years.

Guidance regarding OFAC's expectations regarding risk assessments and compliance is available at A Framework for OFAC Compliance Commitments.

## V. OTHER RESTRICTED TRANSACTIONS

***Export and Import Compliance.*** Through various statutes and regulations including, but not limited to, the International Traffic in Arms Regulations ("ITAR"), the EAR, the Importation of Arms, Ammunition and Implements of War regulations and U.S. Customs laws and regulations (collectively "U.S. Import and Export Control Laws"), the U.S. Government controls the import (permanent and temporary) into and the export (temporary and permanent) directly from the U.S., or indirectly from or through a foreign country, of products, software and technology/technical data; and the provision of related defense services to foreign persons/nationals. In addition, the ITAR includes registration requirements for U.S. manufacturers (including processors) and brokers of defense articles subject to the ITAR, even if those companies do not export from the U.S. These regulations also prohibit any unlicensed release of controlled technical information to certain foreign nationals within the U.S., which are "deemed" to be exports.

The agencies responsible for administering the EAR and the ITAR have also published lists of parties with which various export or re-export transactions are restricted or off-limits (referenced above in the *Transactions with Certain Blocked Individuals, Entities and Groups* section page 12)***.***

It is the policy of each Berkshire subsidiary to comply fully with U.S. Import and Export Control Laws, as well as applicable local export and import laws. Each Berkshire subsidiary should evaluate its operations to determine whether it is subject to these regulations and, if so, develop appropriate procedures to address its individual compliance risks, particularly with respect to sensitive items at risk of being diverted to sanctioned countries, entities, or persons.

***U.S. Anti-Boycott Laws.*** It is the policy of each Berkshire subsidiary to comply fully with all applicable U.S. anti-boycott laws. No Berkshire subsidiary or its employees may take any action that, directly or indirectly, supports the boycott of Israel or any other foreign boycott not sanctioned by the U.S. Any employee with concerns as to whether a transaction implicates U.S. anti-boycott rules, or the boycott or anti-boycott laws of any other country, should consult with the subsidiary's Compliance Officer and not proceed with the transaction until advised. Moreover, if employees receive a boycott-related request, they must promptly notify the subsidiary's Compliance Officer.

U.S. anti-boycott laws prohibit U.S. companies and their "controlled in fact" foreign affiliates, to the extent U.S. commerce is involved, from participating in foreign boycotts that the U.S. does not sanction. Moreover, if a boycott-related request is received, it must be reported to the Commerce Department within 30 days of the end of the calendar quarter in which it was received. Participating in an unsanctioned foreign boycott can also have negative tax consequences. Although the anti-boycott laws apply to all non-U.S. sanctioned boycotts imposed by foreign countries, the Arab League's boycott of Israel is the principal foreign economic boycott covered. While the Treasury Department has identified Iraq, Kuwait, Lebanon, Libya, Qatar, Saudi Arabia, Syria, and

Yemen as boycotting countries, other countries may be sources of boycott requests, as well.

## VI. RETENTION OF INTERMEDIARY SERVICES

Prior to engaging Intermediaries (as defined above on page 2), each Berkshire subsidiary shall conduct appropriate and thorough due diligence documented in writing concerning Intermediaries. Each Berkshire subsidiary employing the services of such Intermediaries shall develop and maintain documented due diligence procedures appropriate to the risks presented that allow the subsidiary's compliance personnel to evaluate and consider the business rationale for needing the Intermediary's assistance as well as the compliance risks posed by the Intermediary partners, including the Intermediary's and partners' reputations and relationships, if any, with foreign officials or the family members of foreign officials and any compliance risk "red flags." Each Berkshire subsidiary should engage in monitoring, assessing, and managing the compliance risks associated with the use of Intermediaries throughout the lifetime of the relationship, and not just during the onboarding process, by periodically updating the due diligence on Intermediaries. Subsidiaries should update the due diligence of Intermediaries that face a higher assessed risk of FCPA compliance at least every two years and determine an appropriate risk-based timeline for lower risk Intermediaries. Centralized IT tools should be used to manage due diligence, documentation, and certifications efficiently.

Due diligence performed on Intermediaries shall include, at a minimum, a documented evaluation of the Intermediary's owners and management to determine if any are affected by a listing on any U.S. prohibited parties lists, such as the SDN List, as well as whether any qualify as foreign officials under the FCPA, and an evaluation of the Intermediary's character, qualifications, experience, reputation for integrity and proven ability to provide the service for which it is being retained. Factors against retention of an Intermediary include, but are not limited to, any unusual requests for compensation and any unusual payment, shipment or destination terms as well as the discovery of any facts, circumstances or "red flags" that might suggest that use of the Intermediary might create an increased FCPA, sanctions, or trade compliance risk. The following are examples of some common red flags that are associated with an increased compliance risk:

- The transaction involves a country known for an increased risk of corruption based on the Corruption Perception Index ("CPI") ranking of the country.
- A reference check reveals flaws in the Intermediary's background.
- Due diligence reveals that the Intermediary is a shell company or that there is something else unorthodox about the Intermediary's structure.
- The Intermediary requests payment to an offshore account or other non-standard payment terms.
- The Intermediary is not clearly qualified or lacks the necessary experience to perform the functions for which it has been engaged.
- The Intermediary is recommended by a government official.

- The Intermediary is partially owned or controlled by a government official.
- The Intermediary has a close personal family or business relationship with a government official or relative of a government official or makes large or frequent political contributions to government officials.
- The Intermediary charges above market amounts for its services.
- The Intermediary suggests that a particular amount of money may be necessary to obtain or retain business or to close a certain deal.
- The Intermediary requests reimbursement of extraordinary, poorly documented, or last-minute expenses.
- The Intermediary objects to FCPA representations, warranties and covenants, and related anti-corruption language in agreements with the Berkshire subsidiary.
- The Intermediary objects to signing FCPA compliance certifications.
- The Intermediary refuses to disclose its ownership, including any beneficial or other indirect owners, principals, or employees, or requests that the identity of its owners, principals or employees not be disclosed.
- The Intermediary requests a large contingency or success fee.

For any Intermediary regarding whom there is an appreciable risk that the Intermediary may interact with government officials or present an FCPA, sanctions, or trade compliance risk, Berkshire subsidiaries are required to have a written agreement with anti-corruption/sanctions/trade compliance contract terms appropriate to the risks presented, including audit rights, and must require the Intermediary to execute an appropriate annual certification of compliance with trade and anti-corruption laws, including the FCPA. Such certifications of compliance shall be annually updated and maintained by the subsidiary.

## VII. MERGERS AND ACQUISITION DUE DILIGENCE

Where a merger or acquisition is consummated, efforts shall be taken to ensure that this Policy and any additional policies of the acquiring Berkshire subsidiary are implemented as quickly as is practicable to the newly acquired business; and compliance training is conducted in accordance with this Policy for the directors, officers, and relevant employees of the newly acquired business. In addition, following the acquisition, the acquiring Berkshire subsidiary shall ensure that a thorough and documented assessment of the acquired company's individual operations and compliance risks is performed that captures the compliance risk areas discussed in this document and that are applicable to the acquired company as a result of the unique nature of its business operations and its geographic location. Based upon this documented risk assessment, the acquiring Berkshire subsidiary shall require the acquiree to implement and adopt additional policies and procedures, as appropriate, so that it maintains an effectively designed compliance policy that is tailored to the unique compliance risks the subsidiary faces.

## VIII. ANTI-MONEY LAUNDERING COMPLIANCE

It is Berkshire's policy to conduct business only with persons or entities who share our commitment to legal compliance and whose funds have a legal source. In the U.S. and all other countries in which Berkshire subsidiaries conduct business, Berkshire subsidiary employees must take reasonable risk-based measures to prevent and detect money laundering and avoid potential criminal liability for and reputational risk associated with such activity. Under money laundering criminal provisions, it is generally a crime to engage in transactions with knowledge that the proceeds are from illegal activity. Similarly, Berkshire subsidiary employees must conduct reasonable due diligence on persons or entities to ensure they are engaged in legitimate business activity.

Certain Berkshire subsidiaries will have affirmative anti-money laundering obligations if they operate in regulated sectors, which may include banking, asset management (i.e., SEC-registered investment advisers), money services or money transmission, gambling/gaming, insurance, and real estate. U.S. federal regulations and analogous foreign laws can mandate anti-money laundering procedures and training programs, audits, and proactive monitoring and reporting of suspicious activity. Berkshire companies that operate in or adjacent to regulated sectors should seek legal advice to determine if they are required to adopt such policies and procedures. Of particular relevance, the U.S. Treasury, Financial Crimes Enforcement Network (FinCEN) amended certain federal regulations in 2024 that—for the first time—include SEC-registered investment advisers in scope of "financial institutions" that are required by law to have certain anti-money laundering programs. Berkshire subsidiaries with affiliated advisers or broker dealers should consult with counsel to ensure these regulated entities have suitable compliance programs.

## IX. RISKS ASSOCIATED WITH NEW AND EMERGING TECHNOLOGY

Berkshire subsidiaries must understand how emerging technologies are deployed and used within their operations and assess the resulting unique risk profile. Berkshire subsidiaries must adopt policies and procedures, controls, governance, and training programs to address these risks. Berkshire subsidiaries must continually monitor and update the framework to manage emerging technological risks, including hiring controls.

Over the past decade, many U.S. companies, including Berkshire subsidiaries, have faced increasingly sophisticated cyber threats from foreign intelligence services, criminal groups, hacktivists, and insiders. These attacks, which include ransomware, identity theft, and deepfake-enabled fraud, pose serious risks to infrastructure, reputation, and legal compliance. A growing concern involves North Korean IT workers[5] infiltrating companies by posing as legitimate remote employees or freelancers, using stolen identities, virtual private networks ("VPNs"), and deepfakes to bypass hiring processes. These schemes have generated hundreds of millions of dollars for the North

[5] Guidance on the North Korea Information Technology Workers is available at https://ofac.treasury.gov/media/923126/download?inline or https://www.microsoft.com/en-us/security/blog/2025/06/30/jasper-sleet-north-korean-remote-it-workers-evolving-tactics-to-infiltrate-organizations/

Korean government and have affected hundreds of companies, including Fortune 500 firms and cybersecurity providers. In some cases, company-issued equipment is mailed to U.S.-based facilitators who install remote access tools to enable the fraud, leading to DOJ prosecutions and highlighting the urgent need for robust identity and IT controls.

Given the heightened threat environment, Berkshire subsidiaries must diligently protect critical data through increased cyber resilience and risk reduction while developing a strong and collaborative IT workforce. Berkshire subsidiaries that hire remote IT workers should seek legal advice to ensure that red flag indicators have been implemented for hiring freelance developers and payment platforms to identify fraudulent IT workers. Berkshire subsidiaries must also maintain mitigation measures to better protect against these risks. In addition, Berkshire subsidiaries must adopt the following controls as applicable using a risk-based approach for all employees regardless of whether they are remote, IT-related, or otherwise.

- Require in-person identity verification during onboarding.
- Conduct thorough reference checks for all candidates.
- Include contract clauses requiring live identity verification for third-party consultants and contractors.
- Use enhanced identity verification methods beyond government identification (e.g., social media checks).
- Cross-reference names and emails against databases of known fraudulent IT workers.
- Require video cameras to be on during interviews and flag unusual behavior.
- Detect and block access to/from anonymous or suspicious VPNs.
- Implement risk-based conditional access and Multifactor Authentication (“MFA”).
- Restrict unregistered or unknown devices from connecting to company systems.
- Review and manage access privileges for remote and contract IT workers.
- Enable IP restrictions to block access from sanctioned countries.
- Block and alert on use of remote access tools and nonapproved USB devices.

## X. RESOURCES

This Policy discusses a variety of statutes, regulations, and U.S. Government agencies. Each agency offers helpful guidelines and resources on its webpage. The following are some U.S. Government websites that you may find helpful as you review and apply the compliance areas discussed in this Policy:

- ***U.S. DOJ’s Guidance Document on the Evaluation of Corporate Compliance Programs***
- ***U.S. DOJ’s FCPA Resource Guide***
- ***OFAC Sanctions Program Guides by Country***
- ***U.S. BIS’ Resources for Establishing an Export Compliance Program***
- ***U.S. Directorate of Defense Trade Control’s Resources for Establishing an Effective ITAR Compliance Program***

It is also possible to sign up for regular email updates from OFAC, BIS and DDTC through the links above. Berkshire subsidiaries should review these and other resources to make sure they are familiar with the controls that apply to their business and keep them current with changes in law and regulations.