

## **I. Introduction**

### ***Company Policy***

It is the policy of Twist Bioscience Corporation and its direct and indirect subsidiaries (the “Company”) to prohibit and actively mitigate the risk of money laundering and any activity that facilitates money laundering or the funding of terrorist or other criminal activities. The purpose of this Policy is to ensure, to the extent possible, that the Company is not a conduit for money laundering or an unwitting facilitator of criminal activity and to further ensure that all Company directors, officers, and employees are aware of that commitment. This Policy shall be overseen and managed by the Company’s Chief Financial Officer.

### ***Applicability***

This Policy applies to all Company directors, officers, and employees worldwide. This Policy is meant to cover both the activities of customers as well as Company counterparties and other business relationships.

### ***General Background***

Money laundering is the process by which people try to conceal illicit funds or otherwise enter into transactions to make these funds appear legitimate.

- Most countries, including the United States, have laws prohibiting money laundering.
- Money-laundering liability can arise through knowledge of, or willfully blindness to, transactions involving the proceeds of a wide-range of criminal activity. In addition, the U.S. money-laundering laws make it a serious offense to transmit money into or out of the United States with the intent of promoting criminal activity, including criminal activity that violates the laws of a foreign country. Indeed, U.S. foreign corruption charges are often accompanied by money laundering allegations as well.
- Violation of U.S. or foreign money laundering laws can result in serious criminal penalties for entities and individuals; forfeiture of funds or assets, including funds received or assets acquired for actual services rendered. Even an allegation of money laundering would associate the Company or an individual associated with the Company with serious criminal activity and cause significant harm to the Company’s reputation and damage to the Company’s business.

Terrorist financing is the process of providing money or resources, for any purpose, to designated terrorist organizations or providing money or resources to help any person commit terrorist activities.

- Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes, including terrorist finance.
- Terrorist financing is a serious criminal offense and the reputational issues associated with any involvement with terrorist organizations or activities can be devastating.

## II. Policy Details

### *General*

In order to avoid money laundering and terrorist financing risks, all Company personnel must at all times be sensitive to anything that suggests that any of the Company's customers or counterparties: (1) may not be legitimate businesses or otherwise not engaged in legitimate business activity; (2) may be paying the Company, or others, with funds from illegitimate sources; or (3) are evidencing irregular or unusual activities that might suggest illegal conduct is taking place.

The level of scrutiny for any particular customer or counterparty will turn on a number of factors, including the size and complexity of the transaction and the jurisdictions in which it will take place. Where required, counterparty screening required by the Company's International Trade Controls Compliance Manual must also be conducted.

We understand that we often have limited visibility into any given transaction. We also understand that in many cases, the legitimacy of the customer or counterparty will be clear. Nevertheless, Company personnel are expected to always be alert for warning signs, including the red flags described below under "Suspicious Transactions."

If any of these red flags—or anything else that calls into question the legitimacy of the customer or counterparty—are present, raise the matter with the Company's Chief Financial Officer, Controller, or Chief Ethics and Compliance Officer.

Red flags must be evaluated with common sense and in the context in which they arise. What may be unusual in one part of the Company's business in a particular region or with a particular asset, may be perfectly normal in a different part of the business or region. The key is to notice signs of irregular activity that lack commercial justification or rationale. We must also be particularly sensitive to transactions in which funds originate from or are destined for high-risk regions or countries, particular those known for drug-trafficking, public corruption, and other unlawful activity.

Regardless of any assumed innocent explanation, the potential concern must be addressed before the Company enters into or facilitates the relationship with the customer or counterparty. In many cases, further diligence can address the concerns and the relationship can proceed.

### ***Acceptable Forms of Payment***

Cash transactions should be strictly avoided (including transactions involving petty cash). In the event that any transaction is conducted in cash, it must be documented with receipts.

### ***International Transportation of Currency or Monetary Instruments***

Do not engage in the physical transportation (e.g., mailing or shipping) of currency or negotiable monetary instruments (e.g., personal or bank checks, promissory notes and money orders which are specifically in bearer form, etc.) into or out of the United States.

### ***Reporting of International Bank and Financial Accounts***

The Company may have a responsibility to report to the U.S. Treasury Department certain financial interests in non-U.S. bank accounts or other non-U.S. financial institution accounts for itself, any subsidiaries and any shareholder, officer, or director thereof who has a financial interest in, or signature authority over, any non-U.S. bank account, including a securities or other financial account in a non-U.S. country, but only if such account had a value exceeding \$10,000 at any time during the calendar year.

### ***Restricted Person/Country Requirements***

Company transactions must not involve countries, governments or persons sanctioned by U.S. authorities. The Company may not engage in any direct and indirect dealings with:

- persons in U.S.-embargoed countries, including Iran, North Korea, Sudan and Syria; or
- Individuals and entities who are “blocked persons” on the OFAC List of Specially Designated Persons, <http://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx>, and entities that are 50%-or-more owned by blocked persons.

### ***Counterparty Identification***

For transactions in excess of \$25,000 USD, the Company must know the identity of and elicit basic information from all persons involved in such transactions (“transaction parties”). For these purposes, a transaction party shall include the buyers, sellers, and third-party intermediaries in transactions engaged in by the Company.

The Company will assure that each transaction party that is a customer of the Company provides standard identifying information in accordance with the Company’s Customer Set-Up and Credit Check Policy and Order Acceptance Policy.

### ***Suspicious Transactions***

Be watchful for “red flags” that suggest an unusual risk of AML violations. These red flags include, for example:

- Proposed unusual payment methods (such as cash).
- Proposed large upfront payments not attached to a firm purchase commitment for Company products or services pursuant to a contract or purchase order.
- Unwillingness by a customer or supplier to provide complete or accurate contact information, financial references, or business affiliations.
- Requests to maintain an unusual degree of secrecy with respect to a transaction.
- Purchases or sales that are unusual for the particular customer or supplier.
- Purchases or sales that are not in conformity with customary practice.
- Payments made through third parties that have not provided the Company with customer information.

### ***Compliance Program***

It is the Company’s policy that all appropriate action be taken to ensure that the Company and its officers and employees comply with the provisions of AML and this Policy. In furtherance of this Policy, the Company will:

- Distribute this Policy to all employees.
- Provide training to employees involved with overseas operations (both new and existing) on the requirements of AML, and the existence of this Policy and require key persons to obtain certifications in AML compliance, as appropriate.
- Develop methods for and conduct periodic internal audits of the implementation of the policy by the Company’s employees, as appropriate.
- Review each material transaction of the Company, including any mergers or acquisitions, to obtain reasonable assurance that the Company’s counterparties in such transactions are not in violation of the AML.
- Keep records as to potential and actual AML violations and report all such matters in compliance with applicable law.

### **III. Conclusion**

It is your responsibility to avoid any activity that could harm the Company's ability to compete legally and ethically in the international marketplace. Although the preceding guidelines should inform you about activities to avoid in international business dealings, you should seek help whenever you are not certain that your actions comply with the above. Feel free to contact our Chief Financial Officer, Controller or Chief Ethics and Compliance Officer.