ANTI-MONEY LAUNDERING AND SANCTIONS POLICY

1. About this Policy

At Xenith IG, we are committed to conducting our business in compliance with all applicable anti-money laundering (including counter-terrorism financing) and economic sanctions laws and regulations. It is illegal under the laws of the various countries we and our stakeholders do business in to:

(a) knowingly engage in financial transactions involving proceeds of criminal activities, such as terrorism, corruption or fraud; or

(b) engage in transactions or dealings with or involving certain countries, entities and individuals sanctioned or prohibited by the U.S. Department of the Treasury Office of Foreign Assets Control (OFAC), the European Union (EU), the United Kingdom's (UK) HM Treasury and similar relevant authorities.

This Anti-Money Laundering and Sanctions Policy ("**Policy**") is designed to assist our employees with understanding our approach to identifying, mitigating and managing money laundering risk and complying with sanctions compliance standards expected of us. Failure to comply with this Policy may lead to criminal, civil or regulatory sanctions and penalties for Xenith IG as well as the individuals involved.

This Policy applies to all full-time, permanent, part-time and contract employees of Xenith IG ("**you**"). Compliance with this Policy is a condition of your continued employment or engagement with us.

2. Objectives of this Policy

(a) To ensure all persons working for us or on our behalf fully understand our responsibilities under applicable anti-money laundering and economic sanctions laws.

(b) To state our requirements and procedures for Third Party Due Diligence and onboarding of all persons doing business with us.

(c) To provide information and guidance to recognise and deal with money laundering and economic sanctions risks.

(d) To assert our commitment to maintaining adequate controls to ensure our continuous compliance with anti-money laundering and economic sanctions laws.

3. Money laundering

3.1. What is money laundering?

Money laundering is activity which involves hiding, disguising or legitimising the true origin and ownership of money used in or derived from committing crimes. In general, money laundering may involve one or more of the following activities:

(a) engaging in a financial transaction with knowledge that the transaction is facilitating criminal activity or with knowledge that the funds being used are derived from the proceeds of criminal activity;

(b) concealing the source of criminally obtained funds by subsequent transfers to disguise the origin of the funds; or

(c) facilitating a financial transaction while wilfully or recklessly disregarding the source of the assets or the nature of the transactions or business operations.

Committing money laundering is an offence punishable by law in the various countries which we and our stakeholders do business in, as is aiding and abetting in criminal activities. We, as a company, may be faced with unlimited fine and the individuals involved may face imprisonment.

It is important to note that it is not necessary that an individual be actively involved in a money laundering scheme to face liability. A person who has knowledge of the tainted source of funds but still effects a transaction involving such funds may be charged with money laundering-related offenses. Where there is no direct evidence of such knowledge, circumstantial evidence showing that an individual recklessly disregarded or was wilfully blind to such information (e.g., looked the other way when signs of illegal conduct were evident) may be sufficient to establish that such an individual was engaged in money laundering.

3.2. Managing money laundering risk

We will only provide our products and services to our customers whose identities we have been able to reasonably ascertain and for business purposes that are legitimate and not related to any criminal or corrupt activities. We will take additional steps to ascertain the identity and nature of business of our customers where there is reasonable suspicion of any potential involvement with any criminal or money laundering activities.

The following is a list of potential “red-flags” which may raise suspicion of money laundering and require further enquiry and/or escalation. This list is not intended to be exhaustive and is for illustrative purposes only:

(a) the presentation of identifying documents that appear forged, altered, or otherwise invalid;

(b) unusually large transactions with no apparent economic or business purpose;

(c) use of anonymous accounts, such as accounts for shell banks or pay-through accounts;

(d) multiple persons or accounts that share the same name, address, telephone number or other identification, but otherwise appear unrelated;

(e) one person or entity that uses multiple addresses or P.O. boxes for no apparent reason;

(f) an inability to determine the beneficial owners of a legal entity;

(g) accounts funded by one individual or entity and then transferred to an apparently unrelated individual or entity;

(h) financial activity or transactions that appears inconsistent with an employee or third party’s financial circumstances;

(i) a third party that exhibits a total lack of concern regarding performance returns or risks; and

(j) transactions with business entities incorporated in or having its main place of business in jurisdictions identified by the Financial Action Task Force as having high risk of money laundering activities.

You must carry out additional enquiries if you become aware of any potential red-flags before proceeding with the transaction or engagement. You must always be mindful of Xenith IG being used for money laundering or aiding or abetting in criminal activities, and you must report any red-flags that cannot be resolved and any suspicious activity or transaction to the Legal and Compliance Department.

4. Sanctions

4.1. Sanction laws and regulations

Various authorities internationally and in the jurisdictions within which we and our stakeholders and affiliates operate, including the governments of the United States of America, the European Union and the United Nations Security Council, prohibit or restrict trade or commerce with certain sanctioned countries, governments, entities, individuals, and activities.

In some cases, these authorities impose comprehensive sanctions on entire countries/territories; in other cases, more limited sanctions are imposed that target particular activities or certain government officials, individuals or entities associated with activity in particular countries or regions. These activities may include, among other areas, corruption, human rights abuses, terrorism, international narcotics trafficking, transnational crime, or weapons of mass destruction proliferation.

The types of activities prohibited or restricted by sanctions may vary. Blocking sanctions may require us to block the property and interests in property of Sanctions Targets or control and prohibit unlicensed transactions involving Sanctions Targets. They may also generally prohibit persons from approving, facilitating, participating in, or guaranteeing a transaction involving Sanctions Targets, such as transactions involving certain sector of the Russian and North Korean economy.

For our purposes, the "**Sanctions**" we observe are the economic sanctions laws, regulations or trade embargoes administered, enacted or enforced by the United Nations Security Council and the government of:

(a) the United States of America;
(b) the European Union;
(c) Australia;
(d) Indonesia;
(e) Hong Kong;
(f) Singapore;
(g) Malaysia; and
(h) all other countries which Xenith operates in,

including the Office of Foreign Assets Control of the United States Department of Treasury ("**OFAC**"), the United States Department of State, United States Department of Commerce's Bureau of Industry and Security, the United Nations Security Council, and the Monetary Authority of Singapore ("**Sanctions Authorities**"), and the individuals or entities or the subject of any Sanction are the “**Sanction Targets**” and the countries the subject of any Sanction are the “**Sanctioned Countries**”).

4.2. Prohibited dealings

Failure to comply with Sanctions may lead to severe civil and criminal penalties to Xenith IG and to you personally, and affect our ability to do business with our customers, suppliers and business partners. You must immediately raise to the Legal and Compliance Department any actual or potential Sanctions nexus or concern, including:

(a) any third parties that are engaged by or that engage us are Sanctions Targets or are located in a Sanctioned Country;

(b) any transaction with or relating to a Sanctions Target or involving a Sanctioned Country; or

(c) you become aware of an existing or potential obligation to block or freeze any property or payment involved in a transaction with or relating to a Sanctions Target or a Sanctioned Country.

5. Compliance

5.1. Finance Department

The Group Financial Controller and the Finance Department are responsible for:

(a) establishing, operating and supervisory procedures regarding transactions involving cash, currency and other financial instruments that comply with this Policy;

(b) promptly notifying the Chief Executive Officer and the General Counsel of any questionable transactions for guidance or corrective action; and

(c) implementing appropriate monitoring policies and procedures to comply with anti-money laundering and sanctions regulation regimes and for the United States, the OFAC monitoring procedures.

5.2. Legal and Compliance Department

The General Counsel and the Legal and Compliance Department are responsible for:

(a) managing the process for onboarding our customers, suppliers and business partners, and conducting due diligence on them in accordance with our Third Party Due Diligence Guidelines;

(b) establishing and implementing an anti-money laundering and sanctions policy and program that meets applicable legal and regulatory requirements, and overseeing the anti-money laundering and sanctions program in accordance with local laws and regulations; and

(c) conducting regular and periodic training to all our employees on anti-money laundering and sanctions laws and regulations, and our responsibilities under them.

The Legal and Compliance Department will maintain and retain adequate customer records, records of Third Party Due Diligence reviews, investigations and post-investigation activities in compliance with relevant legal and regulatory requirements, policies, and standards, including applicable record management and retention policies and procedures. Records must be retained for a minimum of five (5) years from the date of the relevant transaction or business relationship, or such longer period as required by applicable law.

6. Additional guidance

If you have any questions in relation to this Policy, please contact the Legal and Compliance Department at legal@xenithig.com.