Policy on Prevention of Money Laundering and Terrorist Financing Storehouse Group

GENERAL PROVISIONS

Storehouse Group and its current and future direct and indirect subsidiaries (hereinafter jointly referred to as "the Companies" and severally referred to as "the Company") is an international financial services group operating in various jurisdictions. A reputation for integrity, both in its business behavior and in its management systems, is crucial to Companies' achievement of its commercial goals and to the fulfillment of the corporate responsibilities.

Therefore, Companies is committed to the highest standards of Anti-Money Laundering and Combating Terrorism Financing (hereinafter collectively referred to as AML/CTF) compliance and requires management and employees to adhere to these standards to prevent use of the services for money laundering purposes.

The Policy on Prevention of Money Laundering and Terrorist Financing (hereinafter as the «Policy») outlines the minimum general unified standards of internal AML/CTF control which should be adhered to by the Companies in order to mitigate the legal, regulatory, reputational and as a consequence financial risks.

Detailed procedures have been produced by each Company, tailored to their own requirements and to meet local laws, regulations and standards. Non-compliance with these laws may lead to serious consequences to the financial condition and reputation of Companies.

2. THE SCOPE AND APPLICABILITY

The Policy is mandatory for all the Companies and their Employees.

The Companies should use their best endeavors to ensure that the Employees are not involved in money laundering and terrorist financing.

3. THE PURPOSE OF THE POLICY

The Policy is designed to comply with the Financial Action Task Force (FATF) standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, AML principles of the Wolfsberg Group, European Directive 2005/60/EC of October, 26, 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing as well as applicable AML/FT laws and regulations of the jurisdictions in which COMPANIES operates with subsequent amendments (the "Applicable Legislation").

The purpose of the Policy is to provide basic guidance to the Companies and their Employees, wherever located, with regard to major AML/FT requirements.

4. OBJECTIVES

Objectives pursued by this Policy are as follows:

- **To prevent criminal elements from using the Companies for money laundering activities;**
- **Promote a "Know Your Customer" policy as a cornerstone principle for the Companies business practices;**
- **Conduct self-assessments of compliance with AML policy and procedures.**

5. TERMS AND DEFINITIONS

Authorized body means national body (bodies) performing activities aimed at anti-money laundering and counter terrorism financing in accordance with the national legislation and receiving suspicious transactions reports and other reports sent by Company for compliance with national AML/CTF laws and regulations.

Beneficial owner is any individual who i. ultimately owns or controls, whether through direct or indirect ownership or control, more than 25 per cent1 of the shares or voting rights of the client; or ii. Otherwise exercises control over the management of the client.

Client/ Customer means any individual or entity who seeks to enter or has already entered into a business relationship, or conducts a one-off transaction with a Company as principal or as an agent for someone else.

Compliance officer means a person who is in charge of compliance management and/or responsible for AML in the Company.

Employee means an individual working at all levels and grades within Companies, including (but not limited to) the board of directors, the executive board, senior managers, officers, other employees (whether permanent, fixed-term or temporary).

Laundering of proceeds of crime (money) means the making of a legal appearance for the possession, use or disposal of amounts of money or other property received as the result of committing a crime.

Financing of terrorism/Terrorist financing means the providing or raising of funds or the provision of financial services in the knowledge of their being intended for financing an organization, preparing and committing any of the crimes envisaged by Applicable legislation as a terrorist act or for supporting an organized group, illegal military formation or criminal community (criminal organization) that has been formed or is being formed for the purpose of committing any of the said crimes. Politically Exposed Persons (PEP) means any individuals who are or have been entrusted (domestically or by a foreign country or by an international organization) with prominent public functions, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials.

The definition is not intended to cover middle ranking or relatively junior individuals in the foregoing categories 2.

Business relationships with family members or close associates of PEPs involve reputational risks similar to those with PEPs themselves. Shell Bank means a bank without a physical presence in any country.

1 If Applicable Legislation or international/cross-border regulations require identifying beneficial owners holding less than 25% or the Company's assessment of the money laundering or terrorist financing risk presented by the customer is high, it may be decided to verify the identities of beneficial owners holding less than 25%.

2 FATF Guidance on Politically Exposed Persons (Recommendations 12 and 22) from June 2013.

6. RISK-BASED APPROACH (RBA)

6.1. Risk management

A risk-based approach takes a number or all of the following steps in assessing the most cost effective and proportionate way to manage and mitigate the money laundering and terrorist financing risks faced by the Companies:

- identify and assess the money laundering and terrorist financing risks that are relevant to the

Company;

- design and implement controls to manage and mitigate the assessed risks;

- monitor and improve the effective operation of these controls.

Risk management generally shall be regarded as a continuous process, carried out on a dynamic basis. Companies therefore ensure that their risk management processes for managing money laundering and terrorist financing risks are kept under regular review. It is recommended that the Companies revisit their assessments at least annually.

The general principle of a RBA is that, where there are higher risks, Companies should take enhanced measures to manage and mitigate those risks; and that, correspondingly, where the risks are lower, simplified measures may be permitted (pursuant to Applicable Legislation). In particular, they should increase the degree and nature of monitoring of the business relationship, in order to determine whether those transactions or activities appear unusual or suspicious.

6.2. Country Risk

Country risk, in conjunction with other risk factors, provides useful information as to potential money laundering and terrorist financing risks. Country risk is not solely related to the country of origin of a customer.

It should also take into account that a customer may have business interests in or relevant links to a country that may signify that the customer should be placed in a higher risk category.
Factors that may result in a determination that customers from, in or connected with a particular country pose a higher risk includes, for example:

- Countries subject to sanctions, embargoes or similar measures issued by, for example, the United Nations ("UN") or European Union;

- Countries identified by credible sources (e.g. FATF, FATF-style national authorities or other recognized evaluation bodies and EU Commission) as lacking adequate money laundering laws and regulations;

- Countries identified by credible sources as providing funding or support for terrorist activities; or

- Countries identified by credible sources as having significant levels of corruption, or other criminal activity.

6.3. Customer Risk

Determining the potential money laundering and terrorist financing risks posed by a customer, or category of customers, is critical to the development of an overall risk framework. Based on its own criteria, a Company determines whether particular customers poses a higher risk of money laundering and terrorist financing and whether, in some cases, mitigating factors are sufficient to conclude safely that customers engaged in such activities do not, in reality, pose a higher risk of money laundering or terrorist financing. Application of risk variables may increase or decrease the perceived risk in each case.

6.4. Product Risk

Certain products and services offered by Companies may pose a higher risk of money laundering or terrorist financing depending on the nature of the specific product or service offered. Such products and services may facilitate a higher degree of anonymity, or involve the handling of high volumes of currency or currency equivalents.

7. CUSTOMER DUE DILIGENCE (CDD) AND KNOW YOUR CUSTOMER (KYC)

7.1. General provisions of Customer Identification

In identifying a customer, the Company obtains a range of information from the customer and verifies this information (or some of it) through the use of reliable, independent source documents, data or information.

As a mandatory part of the CDD process, Companies perform screening of the parties involved against internal and external restricted and black lists.

Companies take reasonable measures to establish, whether the customer is acting for another person or entity and to identify persons to whose advantage the customer acts, except in situations specifically exempted by Applicable Legislation.

It is strongly recommended the Companies take steps to ensure that they hold appropriate up-to-date information on their customers. The Companies review and update existing customer records based on Company's risk based approach and internal documents but not less frequently than once every three years.

7.2. Simplified Customer Due Diligence (SCDD)

For such categories of customer or business as Listed Companies 3 and Public Authority, a set of SCDD measures reflect the accepted low risk of money laundering or terrorist financing that could arise from such business. Prior to applying SCDD, Companies have to conduct and document appropriate testing to satisfy themselves that the customer or business qualifies for the simplified treatment under this Policy and Applicable Legislation.

7.3. Enhanced Customer Due Diligence (ECDD)

The Companies may apply enhanced due diligence measures based on the risk assessment, thereby requiring intensive 'due diligence' for higher risk customers, especially when the monies are to be paid out into an account other than one in the name of the original applicant and particularly when the proceeds are to be paid to a third party. The examples of

3 Company listed on a Regulated Market (e.g. the London Stock Exchange Official List) and securities of listed company are admitted to trading on a regulated market. Customers requiring higher due diligence may include Politically Exposed Persons (PEPs), Correspondent banking institutions, etc.

8. CUSTOMER ACTIVITY MONITORING

8.1. General provisions

The monitoring procedures include types of customer's transactions, the profile of the customer, comparison of the customer's activity and profile with that of a similar, peer group of customers.

8.2. Prohibited Activities

The Companies would not do business with

- Anonymous customers;
- Shell-banks;
- Client is engaged in activity which is deemed to be black listed (e.g. by a regulators). The Persons which are currently under any sanctions (international, national, other foreign applicable sanctions).

8.3. Transaction Monitoring

Any information pointing to money laundering or terrorist financing must be reported to the relevant authorities in accordance with the requirements of Applicable Legislation. The details of transactions prone to AML risks shall be adequately described and a framework for monitoring of transactions and reporting suspicious transactions as well as adequate guidance to staff to recognize suspicious customer behavior shall be outlined in internal documents.

9. REPORTING PROCEDURES

The following core obligations are part of reporting procedures of Companies:

- all employees participates in raising information about transactions, which are subject to reporting procedures,
- the Company's Compliance Officer considers all internal reports on transactions subject to reporting procedures and makes an external report to the Authorized body subject to Applicable legislation,
- the details of transactions which are subject to reporting procedures and all correspondence exchanged with the authorities in relation to these transactions are documented,
- the external reports to the Authorized body should contain as much information about the customer, transaction or activity as is determined by national laws and regulations.

10. RECORD KEEPING

All records are kept for at least 5 years and contain records obtained through CDD measures; account files and business correspondence; the results of any analysis undertaken; documents relating to business relations and executed transactions; correspondence with the clients and other persons with whom Companies keeps a business relation.

The five year period is calculated following the carrying out of the transactions or the end of the business relationship.

11. CONFIDENTIALITY AND PERSONAL DATA PROTECTION

The information about customers and their transactions obtained in the course of fulfilling AML/CTF internal control is considered as confidential.

The employees of the Companies should avoid disclosure to other persons the AML/CTF ways and means implemented by the Company. The "tipping off" is strictly prohibited.

12. TRAINING

One of the most important controls over the prevention and detection of money laundering or terrorist financing is to have employees that are alert to the risks of money laundering/terrorist financing and well trained in the identification of mandatory control transactions and unusual activities or transactions which may prove to be suspicious.
It is recommended that Companies' relevant employees and in particular employees engaged in customer on-boarding, customer servicing, or in settlements receive training at least once a year. Following national laws and regulations, the circle of employees being trained may be broadened.

Extra trainings are given, if AML/CTF laws and regulations or the Company's policies and procedures, as well as new business products and services have materially changed.

13. INTERNAL CONTROL AND AUDIT

Compliance with this Policy monitored through a combination of internal audit, external audit and regulatory reviews in accordance with Applicable AML Legislation and/or regulations.

The self-assessment of the AML/CTF internal control in the Companies should regularly take place.

Policy on Prevention of Money Laundering and Terrorist Financing

The Policy on Prevention of Money Laundering and Terrorist Financing (hereinafter — «the Policy») outlines the minimum general unified standards of anti-money laundering and combating terrorism financing which should be adhered to by the whole Storehouse Group.

In any country where the applicable anti-money laundering laws and regulations require the Storehouse Group` s companies to establish higher standards, they must meet those standards.

Adherence to this Policy is absolutely essential for ensuring that all Storehouse Group companies, regardless of geographic location, fully comply with applicable anti-money laundering laws and regulations.

Storehouse Group is committed to examining its anti-money laundering strategies, goals and objectives on an ongoing basis and to maintaining an effective Policy for the Group's business.