Anti-Money Laundering and Anti-Terrorism Financing Policy

1. GENERAL PROVISIONS

1.1. Asia Technology and Production Limited (hereinafter – the Company) is an international business company registered and existing under the laws of Hong Kong. The Company is a provider of money transfer and payment processing services.

1.2. The company shall comply with the requirements contained in the Hong Kong Anti-Money Laundering and Terrorist Financing Regulations inforce, as well as the requirements of other laws and regulations to the extent in which they relate to the Company's operations.

1.3. The company shall strictly adhere to the policies and procedures outlined in this document (hereinafter – the Policy).

1.4. The company develops this Policy, introduces amendments and additions to it at its own discretion, and oversees compliance with its provisions and requirements.

1.5. The current version of the Policy is always available on the website at: https://garrypay.com.

1.6. The Customer shall read the Policy prior to accepting the Company's Terms of Conditions. The Customer's acceptance of the Terms and Conditions, as well as the Customer's making transactions in the Company's System after accepting the Terms and Conditions, shall signify the Customer's acceptance of all provisions of the current version of this Policy.

2. COMPLIANCE OFFICER

2.1. To oversee and implement the procedures reflected in the Policy, the Company appoints the Compliance Officer.

2.2. The Compliance Officer is responsible for the collection, analysis, and investigation of information on any suspicious activities and the training of the company's employees pertaining to the relevant procedures; the Compliance Officer shall determine the procedures and rules for carrying out Customers identification, reviewing and monitoring unusual or suspicious transactions and technical features of the Company's implementation of this Policy.

3. CUSTOMER IDENTIFICATION POLICY

3.1. The Company uses the complex of procedures for identification and verification of Customers that may vary depending on transaction amounts.

3.2. The Customers whose transaction amounts do not exceed EURO 999.00 or its equivalent in any consecutive period of 30 (thirty) days, are required to confirm the name and address.

3.3. For the purposes of Customers' identification, the Company requests the following documents:
3.3.1. To verify a personal account:
● proof of identity (passport, driver's license, national identity card);
● proof of address (bank statement, utility bill);
● phone number verification by receiving a code via Telegram Messenger.

3.3.2. To verify a business account:
● all the documents specified in paragraph 3.3.1 in respect of the senior management and shareholders;
● incorporation documents for a company, including:
− state registration certificate (certificate of incorporation);
− company's charter;
− articles of incorporation (if available);
− document, confirming the powers and authority of the person authorized to act on the company's behalf without a power of attorney, etc.

3.3.3. The Company reserves the right to request additional documents with or without reason.

4. 'KNOW YOUR CUSTOMER' VERIFICATION PROCEDURES

4.1. The Company conducts the Know Your Customer (KYC) verification procedures to avoid the risk of being held liable and to protect itself from a Customer attempting to use the Company for carrying out illegal activities.

4.2. As part of the KYC procedures, the Company evaluates Customers' transactions, as well as collects and stores information on the essential facts pertaining to Customers, potential Customers, and their transactions.

4.3. After carrying out the identification procedures pertaining to a Customer, the Company stores the information obtained in this Customer's file. The Company is under obligation to carry out the identification procedures pertaining to a Customer once.

4.4. The Company is committed to protecting Customers' rights and the confidentiality of their personal data. The Company collects personal information from Customers only to the extent necessary to ensure the Company's properly providing services to Customers. Such personal information about Customers and former Customers may be disclosed to third parties only in a limited number of circumstances, in accordance with the applicable laws and agreements between the Company and the Customer.

4.5. The company shall carefully maintain Customers' files, including statements, transaction reports, receipts, notes, internal correspondence, and any other documents related to the Customer both in the electronic and paper format for a period of at least 5 (five) years from the date of the relevant transaction.

5. IDENTIFICATION AND DETECTION OF SUSPICIOUS ACTIVITIES

5.1. Any financial transaction that may be related to money laundering activities shall be considered to be suspicious activities.

5.2. Grounds for determining that a specific transaction is suspicious may be personal observations and experience of the Company's employees, as well as information received or identified.

5.3. The Compliance Officer shall continuously monitor and update the systems used by the Company to detect suspicious activities.

5.4. In accordance with the applicable laws of Hong Kong, and the requirements of international organizations, the Company may, where appropriate and without the obligation of obtaining the Customer's approval or notifying the Customer, notify regulating and/or law enforcement agencies of any suspicious transactions.

5.5. Different requirements for reporting suspicious transactions may depend on the nature and amount of a transaction.

5.6. The Company shall periodically refer to and consult the lists which may from time to time be published by the authorities of the Hong Kong, and international organizations that contain lists of known terrorists or persons suspected of terrorist activities, terrorist organizations, high-risk countries, a list of countries subject to sanctions, jurisdictions that do not provide sufficient level of anti-money laundering procedures, as well as countries subject to sanctions to determine whether the Company's Customer or potential Customer, and/or such Customer's country of jurisdiction is included in the above lists.

5.7. The Company shall continuously conduct due diligence procedures pertaining to its Customers and scrutinize transactions carried out by them to ensure these transactions' compatibility with the Company's knowledge of its Customers, their business and, when necessary, their source of funds.

6. THIRD PARTIES

6.1. To perform some of its business functions, the Company uses third-party service providers. The Company shall make an effort to determine, during the initial and ongoing due diligence process, to the extent possible whether there are any initiated investigations and filed lawsuits against any such third-party service providers. The Company shall also determine whether a third-party provider has obtained all the necessary licenses, permits, and approvals before establishing a business relationship with such third-party service provider.

6.2. With respect to its own staff, the Company shall carefully review all candidates for employment and determine whether the activities of a new employee fall in the category that is susceptible to money laundering activities. In addition, the Company has prepared and implements a number of personnel training programs on customer identification procedures and prevention of money laundering activities.

7. CIVIL AND CRIMINAL PENALTIES

7.1. Government authorities of different countries and, in some cases, international organizations, may impose severe civil and criminal penalties against any person that violates the laws and regulations referred to in paragraph 1.2 of the Policy. Such civil and criminal legal penalties may include fines in the amount of up to hundreds of thousands or even millions of dollars, and the term of criminal punishment may be up to 10 (ten) years in prison. In addition, government authorities may confiscate any property involved in criminal violation of these laws and regulations, including companies, bank accounts, or any other assets that may be associated with criminal violations.

7.2. Under certain circumstances, companies may be deemed criminally responsible for the actions of their employees. In this regard, it is important for the employees of our Corporate Customers to have adequate knowledge in this sphere; it is also important that such Corporate Customers should ensure the compliance of their employees' actions with the said laws and regulations.

8. COMPLIANCE STATEMENT

8.1. The Corporate Customer (the Corporate Customer's authorized employee) certifies that they have read and understood this Policy, and that they (or their company) shall operate in full compliance with the requirements and standards outlined in the Policy and comply with all applicable laws and other regulations and requirements governing its activities as a Corporate Customer.

8.2. The Corporate Customer (the Corporate Customer's authorized employee) acknowledges that they are responsible for their actions in accordance with the effective laws in the field discussed in this Policy and shall bear responsibility pertaining to failure to comply with such laws