Information on the Applied Anti-Money Laundering and Counter-Terrorist Financing Principles

1. General Information

The Anti-Money Laundering and Counter-Terrorist Financing Policy (hereinafter referred to as the "Policy") is intended to prevent and mitigate potential risks that Pilot Innovation (hereinafter referred to as the "Company") may become involved in any illegal activities.

In order to comply with international and local regulations, the Company implements effective internal procedures and mechanisms aimed at preventing money laundering, terrorist financing, drug and human trafficking, the proliferation of weapons of mass destruction, corruption and bribery, as well as responding to any forms of suspicious activity conducted by its Users.

"Money Laundering (legalization of proceeds derived from criminal activity)" shall be understood as the act defined in Article 299 of the Act of 6 June 1997 – the Criminal Code.

"Terrorist Financing" shall be understood as the act defined in Article 165a of the Act of 6 June 1997 – the Criminal Code.

This Policy shall under no circumstances be interpreted as a complete set of all policies, procedures, and control measures applied by the Company to prevent money laundering, terrorist financing, and other forms of illegal activity.

2. Company Obligations

2.1 Obliged Entity in Poland

TAILCOR SP. Z O.O. is subject to regulation under the Act of the Republic of Poland of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (Journal of Laws 2018, item 723), as well as other applicable legal acts.

Supervisory Authorities

The Company is supervised by the General Inspector of Financial Information (GIIF), which is the competent authority in Poland responsible for monitoring and preventing financial crimes.

Company Obligations

Customer Identification and Financial Security Measures (KYC/CDD):

- Implementation of "Know Your Customer" (KYC) procedures;
- Customer risk assessment in accordance with the Risk-Based Approach (RBA);
- Enhanced Due Diligence (EDD) for high-risk customers.

Reporting Obligations to GIIF:

- Reporting transactions with a value of EUR 15,000 or more;
- Mandatory reporting of suspicious transactions that may be related to money laundering or terrorist financing;

- Maintaining appropriate documentation for a minimum period of 5 years.

Compliance with International AML/CTF Standards:

- Directive (EU) 2015/849 (4th AML Directive);
- Regulation (EU) 2023/1113 of the European Parliament and of the Council on information accompanying transfers of funds and certain crypto-assets and amending Directive (EU) 2015/849 (Transfer of Funds Regulation);
- FATF (Financial Action Task Force) Recommendations on combating financial crime.

3. The Client Should Exercise Due Diligence

Comprehensive customer identity verification (Customer Due Diligence, CDD) is a mandatory measure under the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (Journal of Laws 2023, item 1124). The Company is required to collect, verify, and keep customer information up to date at all stages of the business relationship.

Depending on the risk level assigned to a customer, different levels of CDD are applied:

- **Standard Due Diligence (SDD)** – applied to low-risk customers;
- **Enhanced Due Diligence (EDD)** – applied where an increased risk is identified and requires additional data.

3.1. Standard Due Diligence Measures

Individual customers should provide:

- A passport or national identity card;
- Proof of residential address (e.g., a bank statement, a utility bill);
- Biometric verification (liveness check) in the case of remote verification.

Corporate customers should provide:

- Constitutional/founding documents;
- Identification documents of the beneficial owner(s) and members of the management board;
- Proof of the company's registered address;
- Extract/information from the National Court Register (KRS);
- Confirmation of source of funds;
- A list of the top 5 business partners and the agreements concluded with them;
- Information about the website and confirmation of domain ownership.

3.2. Enhanced Due Diligence (EDD)

The Company applies Enhanced Due Diligence measures where:

- Customer data raises doubts as to its reliability;
- The customer is a financial institution from a third country;
- The customer is a Politically Exposed Person (PEP) or a close associate/family member of a PEP;

- The customer resides in or conducts business activities in a high-risk jurisdiction.

In the case of EDD, the Company may:

- Request additional documents confirming the customer's identity;
- Verify the customer's source of funds and source of wealth;
- Increase the frequency of transaction monitoring;
- Conduct an in-depth analysis of the customer's business activities.

3.3. Source of Funds Verification

The Company is obliged to ensure that the funds used by the customer originate from lawful sources. For this purpose, the following may be required:

- Bank statements;
- Documents confirming income and investments;
- Evidence of sale of assets or other lawful transactions.

4. Politically Exposed Persons (PEPs)

The Company determines whether a customer or their beneficial owner is a Politically Exposed Person (PEP), a family member, or a close associate of a PEP. If a customer is identified as a PEP, Enhanced Due Diligence (EDD) measures are automatically applied.

5. Ongoing Monitoring and Data Updates

The Company implements transaction monitoring systems in accordance with the Act of 1 March 2018 on Counteracting Money Laundering and Terrorist Financing (Journal of Laws 2018, item 723).

The purpose of monitoring is to detect and prevent suspicious financial transactions that may be related to money laundering (AML) or terrorist financing (CTF).

5.1. Monitoring Procedures

Transaction monitoring is conducted on an ongoing basis and includes:

- Analysis of customer transaction activity patterns;
- Automated transaction screening using data analysis systems;
- Manual review of transactions that meet suspicious criteria;
- Screening of transactions against sanctions lists and high-risk jurisdiction lists;
- Assessment of the customer's risk level and transactional activity.

The Company applies a Risk-Based Approach (RBA), under which customers are classified according to risk levels (low, medium, high, and unacceptable), and their transactions are analyzed with an appropriate level of scrutiny.

5.2. Identification of Suspicious Transactions

The Company is obliged to maintain a register of suspicious transactions and report them to the General Inspector of Financial Information (GIIF).

5.3. Risk Assessment

The Company conducts an internal risk assessment on an annual basis, taking into account:

- **Geographical factors** (countries with high levels of corruption or weak financial supervision);
- **Type of customers** (Politically Exposed Persons, financial institutions);
- **Payment instruments used** (cash, anonymous payment methods);
- **Nature of the customer's business activity** (companies operating in sectors with elevated AML/CTF risk).

As part of the assessment, corrective actions are developed to minimize risks and improve monitoring processes.

5.4. Use of Technology in Monitoring

The Company uses advanced technologies for the analysis of transactional data, including:

- Automated monitoring systems with machine learning algorithms;
- Blockchain analytics to trace cryptocurrency transactions;
- Databases of sanctions lists, Politically Exposed Persons (PEPs), and adverse media;
- Behavioral data analysis tools.

These technologies enhance the accuracy of detecting suspicious transactions and reduce the number of false positives.

6. Responsible Officer

The Responsible Officer (RO) within the Company oversees compliance with the AML/CTF Policy and ensures adherence to the legal requirements of the Republic of Poland and international standards.

Main Responsibilities:

- Supervising compliance with anti-money laundering and counter-terrorist financing procedures, including transaction monitoring;
- Cooperating with the General Inspector of Financial Information (GIIF) and submitting reports on suspicious transactions;
- Developing and updating internal AML/CTF procedures;
- Training employees and conducting internal audits;
- Performing risk assessments and implementing corrective actions.

The Responsible Officer serves as the key point of contact with regulators and ensures the effectiveness of the Company's internal control framework.

7. Refusal to Provide Services

Unacceptable Customers

The Company does not establish business relationships with customers who:

- Refuse to provide the requested information and documentation for verification purposes;
- Are so-called shell banks (banks without a physical presence in a regulated jurisdiction);
- Reside in or conduct business activities in countries subject to international sanctions or prohibited under the Company's internal policies;
- Raise reasonable suspicions of potential involvement in money laundering, terrorist financing, or other illegal activities.

Restricted Countries and Territories

The Company does not accept customers from the following countries and territories:

Afghanistan, Albania, Algeria, Andorra, Angola, Anguilla, Antigua and Barbuda, Argentina, Bahamas, Bahrain, Bangladesh, Barbados, Benin, Bermuda, Bolivia, Botswana, Brazil, Brunei, Bulgaria, Burkina Faso, Burundi, Cambodia, Cameroon, Cape Verde, Cayman Islands, Central African Republic (CAR), Ceuta, Chad, Chile, China, Colombia, Comoros, Congo, Cook Islands, Costa Rica, Cuba, Croatia, North Korea, Democratic Republic of the Congo, Djibouti, Dominican Republic, Ecuador, Egypt, El Salvador, Equatorial Guinea, Eritrea, Eswatini, Ethiopia, French Guiana, Gabon, Gambia, Ghana, Grenada, Guadeloupe, Guatemala, Guinea, Guinea-Bissau, Haiti, Honduras, Iceland, India, Iran, Iraq, Côte d'Ivoire, Jamaica, Japan, Jordan, Kenya, Korea, Kuwait, Laos, Lebanon, Lesotho, Liberia, Libya, Macau, Madagascar, Maldives, Mali, Melilla, Marshall Islands, Martinique, Mauritania, Mexico, Monaco, Mongolia, Morocco, Mozambique, Myanmar, Namibia, Nepal, Nicaragua, Niger, Nigeria, Pakistan, Palestine, Panama, Paraguay, Peru, Philippines, Puerto Rico, Qatar, Republic of the Congo, Kosovo, Réunion, Russia, Rwanda, Sahrawi Arab Democratic Republic, Samoa, São Tomé and Príncipe, Sark, Saudi Arabia, Senegal, Serbia, Sierra Leone, Somalia, South Africa, South Sudan, Sri Lanka, Saint Barthélemy, Saint Maarten, State of Palestine, Sudan, Switzerland, Syria, Taiwan, Tanzania, temporarily occupied territories of Ukraine (Crimean Peninsula, Donetsk Oblast, Kharkiv Oblast, Kherson Oblast, Luhansk Oblast, Zaporizhzhia Oblast), Togo, Transnistrian Moldovan Republic, Trinidad and Tobago, Tunisia, Turkey, Turkmenistan, Uganda, United Arab Emirates (UAE), United States of America (USA), Uruguay, Vanuatu, Venezuela, Vietnam, Western Sahara, Yemen, Zambia, Zimbabwe.

8. Cooperation and Information Sharing

The Company actively cooperates with regulatory authorities and law enforcement agencies in order to prevent money laundering and terrorist financing. Paypilot provides the necessary information based on official requests, in accordance with applicable laws and international obligations.

For matters related to cooperation and information exchange, the Company may be contacted at: **info@tailcor.com**