Prime Business LLC AML and KYC Policy

1. Purpose

The purpose of this policy is to establish a robust framework for compliance with Anti-Money Laundering (AML) and Know Your Customer (KYC) regulations, specifically tailored to our operations as a financial IT solutions provider. This policy aims to prevent and mitigate the risks associated with money laundering and terrorist financing activities.

2. Scope

This policy applies to all employees, contractors, and third-party service providers of Prime Business LLC, including those involved in the development, implementation, and maintenance of financial IT solutions.

3. Policy Statement

Prime Business LLC is committed to conducting its business in compliance with all applicable AML and KYC laws and regulations. We will implement comprehensive measures to identify, assess, and manage the risks associated with money laundering and terrorist financing in the financial technology sector.

4. KYC Procedures

4.1 Customer Identification

We will collect and verify the identity of our clients through:

- **Government-issued Identification**: Passport, driver’s license, or national ID.
- **Proof of Address**: Recent utility bill, bank statement, or lease agreement.
- **Business Verification**: For corporate clients, we will require registration documents, tax identification numbers, and ownership structure.

4.2 Risk Assessment

Clients will be categorized based on risk levels:

- **Low Risk**: Standard verification procedures apply for clients with minimal risk factors.
- **Medium Risk**: Enhanced due diligence required for clients in high-risk industries or jurisdictions.
- **High Risk**: Ongoing monitoring and additional scrutiny for clients exhibiting suspicious behavior or those involved in complex financial transactions.

4.3 Ongoing Due Diligence

We will conduct periodic reviews of client accounts to ensure that customer information is up-to-date and that transaction patterns remain consistent with the client’s profile.

5. AML Procedures

5.1 Transaction Monitoring

We will implement automated systems to monitor transactions for unusual patterns or suspicious activity. Key indicators include:

- Transactions that are inconsistent with the client’s known business activities.
- Unexplained spikes in transaction volume or value.

5.2 Reporting

Suspicious transactions will be promptly reported to the relevant authorities in accordance with local and international regulations. Employees are required to report any suspicious behaviors or transactions to the designated AML Compliance Officer.

5.3 Enhanced Scrutiny for High-Risk Transactions

All high-risk transactions will undergo enhanced scrutiny and may require additional documentation or approval before processing.

6. Training and Awareness

We will provide regular training sessions for employees on AML and KYC policies, including:

- Recognition of red flags for suspicious activities.
- Procedures for client onboarding and due diligence.
- Updates on regulatory changes and best practices in the financial IT sector.

7. Record Keeping

All customer identification documents and transaction records will be maintained for a minimum of five years, in compliance with regulatory requirements. Records will be stored securely and made accessible for audits as needed.

8. Compliance Officer

An appointed Compliance Officer will oversee the implementation of this policy, conduct regular audits, and ensure adherence to all relevant laws and regulations. The Compliance Officer will also serve as a point of contact for regulatory authorities.

9. Review and Updates

This policy will be reviewed annually and updated as necessary to reflect changes in regulations, business practices, or emerging risks specific to the financial technology sector.

10. Confidentiality

All information collected for KYC purposes will be handled with the highest level of confidentiality and in compliance with data protection regulations.