Know Your Customer and Anti-Money Laundering Policy
INNOTECH LABS LTD

Last Updated: 07th January 2025

This Know Your Customer ("KYC") and Anti-Money Laundering / Counter Financing of Terrorism ("AML/CFT") Policy ("Policy") sets out the comprehensive framework adopted by Innotech Labs Ltd, operating under the brand name "Tokenprime", to prevent its platform, products, services, and delivery channels from being used for money laundering ("ML"), terrorist financing ("TF"), or proliferation financing ("PF").

Tokenprime operates an online platform that facilitates the buying, selling, transfer, and exchange of virtual digital assets ("VDAs" or "Crypto Assets") between users. Given the nature of virtual asset activities and their inherent exposure to ML/TF/PF risks, Tokenprime adopts a robust, risk-based, and continuously evolving compliance regime aligned with international best practices and the legal requirements of the Republic of Trinidad and Tobago.

This Policy is designed to: - Safeguard the integrity of Tokenprime's platform and operations; - Protect Tokenprime, its users, and stakeholders from financial crime risk; - Demonstrate Tokenprime's commitment to full regulatory compliance; - Provide transparency to users, regulators, auditors, and other competent authorities.

This Policy applies to all directors, senior management, officers, employees, contractors, agents, and users of Tokenprime.

The Platform is owned, managed, and operated by Innotech Labs Ltd, a company duly incorporated under the Companies Act, Chap. 81:01 of the Laws of the Republic of Trinidad and Tobago, with Company Number C2024021500005 and registered office at 5th Floor Savannah East, 11 Queen's Park East, Port of Spain, Trinidad and Tobago (hereinafter referred to as "Tokenprime", "the Company", "we", or "us").

Tokenprime is a Reporting Entity / Supervised Entity under the Prevention of Money Laundering Act, 2002 (as amended) and is registered with the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT").

This Policy is subject to and must be read in conjunction with Tokenprime's Terms of Use, Privacy Policy, and any other policies published on the Platform from time to time.

1. Compliance Officer and Alternate Compliance Officer

1.1 Appointment and Regulatory Approval

In accordance with the Financial Obligations Regulations, 2010, guidance issued by the Financial Intelligence Unit of Trinidad and Tobago (FIUTT) and Prevention of Money Laundering Act, 2002 (as amended) Innotech Labs Ltd ("Tokenprime" or "the Company") shall appoint a Compliance Officer (CO) and an Alternate Compliance Officer (ACO).

The appointment of the CO and ACO shall be made by Senior Management and shall be subject to prior approval by the FIUTT. No individual shall perform the functions of a Compliance Officer or Alternate Compliance Officer unless such approval has been formally granted by the FIUTT.

1.2 Role, Authority, and Independence

The Compliance Officer is the central point of responsibility for Tokenprime's AML/CFT framework and is vested with sufficient authority, independence, and access to information to effectively discharge their duties. The CO reports directly to Senior Management and, where necessary, to the Board of Directors.
The Compliance Officer is responsible for:

- Implementing and maintaining the AML/CFT Compliance Programme;
- Ensuring adherence to all AML/CFT legal and regulatory obligations;
- Receiving, reviewing, and assessing internal reports of suspicious transactions or activities;
- Making independent determinations on whether a Suspicious Transaction Report (STR) should be filed;
- Submitting STRs and other statutory reports directly to the FIUTT;
- Acting as the primary liaison with the FIUTT, supervisory authorities, and law enforcement agencies;
- Ensuring that AML/CFT training, internal controls, and record-keeping requirements are effectively implemented.

The Alternate Compliance Officer shall perform the functions of the Compliance Officer during periods of absence, unavailability, or conflict, thereby ensuring continuity of compliance and reporting obligations.

1.3 Ongoing Obligations and Updates

Tokenprime shall promptly notify the FIUTT of any changes relating to:

- The appointment, resignation, or replacement of the CO or ACO;
- Contact details, identification documents, or other material information pertaining to the CO or ACO;
- The registered or mailing address of the Company.

2. Compliance Programme

2.1 Purpose and Nature of the Compliance Programme

Tokenprime maintains a documented AML/CFT Compliance Programme approved by Senior Management, which sets out the policies, procedures, systems, and controls designed to prevent and detect money laundering, terrorist financing, and proliferation financing.
The Compliance Programme is tailored to the nature, scale, complexity, and risk profile of Tokenprime's business, including its provision of virtual asset-related services. It is designed to be dynamic and responsive to changes in regulatory expectations, emerging risks, and business operations.

2.2 Core Components

The Compliance Programme includes, at a minimum:

- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) measures;
- Procedures for identifying and internally escalating suspicious transactions or activities;
- Adoption of a Risk-Based Approach to monitoring customers and transactions;
- Clearly defined roles and responsibilities for AML/CFT compliance;
- Independent testing of the AML/CFT framework;
- Record-keeping and retention procedures;

- Measures relating to high-risk customers, products, services, and jurisdictions.

2.3 Implementation and Review

The Compliance Programme is implemented immediately upon approval and is communicated to all relevant staff. It is reviewed at least annually, or more frequently where required, to ensure continued effectiveness and alignment with Applicable Laws and FIUTT guidance.

3. AML/CFT Training

3.1 Training Philosophy and Scope

Tokenprime recognises that AML/CFT training is a fundamental pillar of an effective compliance framework. Accordingly, AML/CFT training is provided to all directors, officers, employees, and relevant contractors, with training content tailored to the individual's role and level of responsibility.

3.2 Training Content

AML/CFT training covers, inter alia:

- Legal and regulatory obligations under the AML/CFT framework of Trinidad and Tobago;
- Customer Due Diligence and Enhanced Due Diligence requirements;
- Identification of ML, TF, and PF red flags relevant to virtual asset activities;
- Internal reporting procedures and escalation protocols;
- Obligations relating to confidentiality and tipping-off;
- Consequences of non-compliance for the Company and individuals.

3.3 Frequency and Records

Training is conducted on an ongoing basis and at least annually. Tokenprime maintains a Training Register documenting attendance, content, facilitators, and dates of training sessions.

4. Risk-Based Approach

4.1 Adoption of a Risk-Based Framework

Tokenprime adopts and applies a comprehensive Risk-Based Approach ("RBA") to the prevention and detection of money laundering, terrorist financing, and proliferation financing ("ML/TF/PF"), in accordance with Regulation 7 of the Financial Obligations Regulations, 2010, guidance issued by the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT"), and the recommendations of the Financial Action Task Force ("FATF").

The Risk-Based Approach recognises that not all customers, products, transactions, delivery channels, or jurisdictions present the same level of ML/TF/PF risk. Accordingly, Tokenprime assesses and classifies risks to ensure that compliance controls, due diligence measures, monitoring intensity, and resource allocation are proportionate to the level of risk identified.

The objective of Tokenprime's RBA is to:

- Identify, understand, and document ML/TF/PF risks inherent in its business;

- Apply appropriate and proportionate mitigation measures;
- Enhance the effectiveness of AML/CFT controls without unduly restricting legitimate activity; and
- Ensure ongoing adaptability to emerging risks, typologies, and regulatory expectations.

4.2 Enterprise-Wide ML/TF/PF Risk Assessment

Tokenprime conducts and maintains a documented enterprise-wide ML/TF/PF Risk Assessment, which forms the foundation of its Risk-Based Approach. This assessment is approved by Senior Management and is reviewed periodically, and at least annually, or upon the occurrence of material changes to Tokenprime's business model, products, services, customer base, or operating environment.

The Risk Assessment takes into account:

- The nature, size, complexity, and scale of Tokenprime's virtual asset activities;
- The degree of anonymity, speed, and cross-border nature of virtual asset transactions;
- Findings from National Risk Assessments, sectoral risk assessments, and typology reports issued by the FIUTT, FATF, or other competent authorities.

4.3 Risk Identification

Tokenprime identifies ML/TF/PF risks across all relevant risk factors, including but not limited to the following:

(a) Customer Risk

Customer risk is assessed based on characteristics such as:

- Individual versus legal entity customers;
- Politically Exposed Persons (PEPs), their family members, and close associates;
- Non-resident or non-national customers;
- Customers with complex or opaque ownership or control structures;
- Customers operating in cash-intensive or high-risk industries.

(b) Product and Service Risk

Risk arising from the nature of products and services offered, including:

- Types of virtual assets supported;
- Services that facilitate rapid movement, exchange, or transfer of value;
- Products that may obscure transaction origin, destination, or ownership.

(c) Delivery Channel Risk

Risk associated with how products and services are delivered, including:

- Non-face-to-face onboarding and digital verification processes;
- Reliance on third-party service providers or technology platforms;
- Automated or high-volume transactional environments.

(d) Geographic Risk

Risk associated with:

- Jurisdictions in which Tokenprime operates or from which customers originate;
- Countries identified by FATF, FIUTT, or other competent authorities as high-risk, non-cooperative, or subject to sanctions;
- Cross-border transactions involving multiple jurisdictions.

4.4 Risk Assessment and Classification

Each identified risk is assessed using a structured methodology that considers:

- The likelihood of ML/TF/PF occurring; and
- The potential impact on Tokenprime, the financial system, and regulatory compliance.

Based on this assessment, risks are classified into defined categories (e.g. low, medium, or high risk). The classification informs:

- The level of customer due diligence required;
- Transaction monitoring thresholds and frequency;
- Approval and escalation requirements; and
- Ongoing review and update cycles.

4.5 Risk Mitigation Measures

Tokenprime develops and implements risk mitigation measures that are proportionate to the level of risk identified. Such measures include, but are not limited to:

- Simplified Due Diligence for lower-risk customers where permitted by law;
- Enhanced Due Diligence for higher-risk customers, transactions, or relationships;
- Increased transaction monitoring and scrutiny;
- Senior management approval for onboarding or continuing high-risk relationships;
- Restrictions or prohibitions on certain products, services, or jurisdictions where risk cannot be adequately mitigated.

4.6 Ongoing Monitoring and Review

Tokenprime continuously monitors customer relationships, transactions, and activities to ensure consistency with the customer's risk profile and stated purpose of the relationship. Risk profiles are reviewed and updated:

- Periodically, based on the assigned risk category;
- Upon the occurrence of triggering events (e.g. unusual transactions, changes in ownership, geographic exposure, or customer behaviour); and
- In response to emerging risks, regulatory guidance, or internal findings.

The outcomes of monitoring and review activities feed back into the Risk Assessment process, ensuring that Tokenprime's Risk-Based Approach remains dynamic, effective, and aligned with regulatory expectations.

5. Internal Controls

5.1 Purpose and Control Environment

Tokenprime maintains a comprehensive system of internal controls designed to ensure the effective implementation, operation, and enforcement of its AML/CFT obligations in accordance with the Prevention of Money Laundering Act, 2002 (as amended), the Financial Obligations Regulations, 2010, and guidance issued by the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT").

The internal control framework forms an integral part of Tokenprime's overall governance structure and is designed to:

- Support the identification, assessment, mitigation, and monitoring of ML/TF/PF risks;
- Ensure consistent application of AML/CFT policies and procedures;
- Promote accountability, transparency, and regulatory compliance across all business functions; and
- Safeguard the integrity, confidentiality, and availability of customer and transaction data.

Senior Management is responsible for establishing a strong control environment and ensuring that adequate resources, systems, and oversight mechanisms are in place to support effective AML/CFT compliance.

5.2 Customer Due Diligence Controls

Tokenprime develops and implements customer due diligence ("CDD") controls to establish and verify the identity of all customers prior to the commencement of a business relationship and, where applicable, prior to the execution of transactions.

CDD controls include:

- Procedures for identifying natural persons and legal entities using reliable, independent source documents, data, or information;
- Verification of beneficial ownership and control structures for legal persons and arrangements;
- Ongoing due diligence measures to ensure customer information remains accurate, complete, and up to date; and
- Controls to prevent anonymous or fictitious accounts or relationships.

Where the risk assessment identifies higher ML/TF/PF risk, Tokenprime applies Enhanced Due Diligence ("EDD") measures commensurate with the level of risk, including additional verification, source of funds or source of wealth inquiries, and heightened monitoring.

5.3 Enhanced Due Diligence and High-Risk Controls

Tokenprime implements enhanced internal controls for customers, transactions, and activities assessed as high risk. These controls are designed to provide greater scrutiny and assurance and may include:

- Senior management approval prior to onboarding or continuation of high-risk relationships;
- Collection of additional information or documentation to substantiate identity, ownership, and source of funds;
- Increased frequency and intensity of transaction monitoring;
- Restrictions on certain transaction types, volumes, or jurisdictions; and
- Periodic review of the risk classification and ongoing suitability of the relationship.

5.4 Transaction Monitoring and Payment Controls

Tokenprime maintains systems and procedures to monitor transactions and customer activity on an ongoing basis to detect unusual, complex, or suspicious patterns inconsistent with a customer's profile or stated purpose of the relationship.

In accordance with FIUTT guidance, Tokenprime develops and implements payment-related controls, including:

- Defined thresholds for transactions that require additional review or approval;
- Measures to identify and assess the source of funds and, where relevant, source of wealth;
- Controls to mitigate risks associated with high-velocity, high-value, or cross-border transactions; and
- Escalation mechanisms for transactions requiring further investigation by the Compliance Officer.

5.5 Record-Keeping and Information Security Controls

Tokenprime maintains internal controls to ensure the secure creation, maintenance, retention, and retrieval of records relating to customer identification, transactions, and AML/CFT compliance.

Such controls include:

- Secure storage of records in electronic or physical form;
- Access controls to restrict information to authorised personnel only;
- Measures to protect data confidentiality, integrity, and availability;
- Systems to ensure records can be promptly retrieved in response to lawful requests from competent authorities.

5.6 Organisational Controls and Segregation of Duties

Where feasible, Tokenprime ensures appropriate segregation of duties to reduce the risk of error, conflict of interest, or misuse of authority. Key AML/CFT functions, including customer onboarding, transaction processing, monitoring, and reporting, are structured to ensure independent review and oversight.

Clear reporting lines, escalation pathways, and accountability frameworks are established and documented to support effective decision-making and compliance oversight.

5.7 Oversight, Review, and Continuous Improvement

The Compliance Officer is responsible for overseeing the effectiveness of the internal control framework and reporting material weaknesses, breaches, or emerging risks to Senior Management.

Internal controls are subject to:

- Ongoing monitoring through day-to-day operations;
- Periodic internal reviews;
- Independent testing as part of the AML/CFT audit process.

Findings from reviews, audits, regulatory feedback, or enforcement actions are used to enhance and strengthen internal controls on a continuous basis.

6. Reporting Obligations

6.1 General Reporting Framework

Tokenprime maintains robust reporting arrangements to ensure timely, accurate, and complete reporting of suspicious transactions, suspicious activities, and terrorist-related funds in accordance with the Prevention of Money Laundering Act, 2002 (as amended), the Anti-Terrorism Act, Chap. 12:07, the Financial Obligations Regulations, 2010, and guidance issued by the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT").

Reporting obligations form a critical component of Tokenprime's AML/CFT framework and are designed to:

- Support the detection and disruption of money laundering, terrorist financing, and proliferation financing;
- Ensure compliance with statutory reporting timelines and standards;
- Facilitate effective cooperation with the FIUTT and other competent authorities; and
- Protect Tokenprime and its employees from legal, regulatory, and reputational risk.

6.2 Internal Reporting of Unusual or Suspicious Activity

All directors, officers, employees, and relevant contractors are required to remain vigilant and to promptly report any transaction, activity, or behaviour that appears unusual, inconsistent with a customer's known profile, or otherwise gives rise to suspicion of ML/TF/PF.

Internal reports must be made **without delay** to the Compliance Officer and should include all relevant facts, documentation, and contextual information available to the reporting individual. Employees must not attempt to investigate or resolve the suspicion independently.

Tokenprime strictly prohibits tipping-off. No employee shall disclose to any customer or third party that a suspicion has been formed or that a report may be, or has been, made to the FIUTT.

6.3 Assessment and Determination of Suspicion

Upon receipt of an internal report, the Compliance Officer shall:

- Review and analyse the information provided;
- Consider the transaction or activity in the context of the customer's risk profile, transaction history, and known business purpose;

- Determine whether reasonable grounds exist to suspect that the funds or activity are linked to a specified offence, money laundering, terrorist financing, or proliferation financing.

The determination of suspicion is an objective assessment based on reasonable grounds and does not require proof that a criminal offence has occurred.

6.4 Suspicious Transaction / Suspicious Activity Reporting to the FIUTT

Where the Compliance Officer determines that reasonable grounds for suspicion exist, a Suspicious Transaction Report ("STR") or Suspicious Activity Report ("SAR") shall be submitted to the FIUTT in the prescribed form and manner.

In accordance with FIUTT guidance, such reports shall be filed **within fourteen (14) days** of the date on which the suspicion was formed.

STRs/SARs shall be:

- Complete, accurate, and clear;
- Supported by relevant transactional data and contextual information; and
- Submitted solely by the Compliance Officer or, in their absence, the Alternate Compliance Officer.

Tokenprime shall maintain appropriate records of all internal reports, assessments, and external submissions in accordance with its record-keeping obligations.

6.5 Reporting of Terrorist Funds and Sanctions-Related Matters

Where Tokenprime knows or suspects that funds, assets, or transactions are linked to terrorism, terrorist organisations, or persons designated under applicable sanctions regimes, Tokenprime shall:

- Report the matter **immediately** to the FIUTT;
- Comply without delay with any lawful freezing, restraint, or prohibition orders issued by competent authorities;
- Refrain from conducting any transaction involving the affected funds except as permitted by law; and
- Cooperate fully with the FIUTT, law enforcement agencies, and other competent authorities.

Immediate reporting obligations apply irrespective of the value of the funds or whether a transaction has been completed.

6.6 Confidentiality and Protection of Reporting Persons

All reports, related information, and communications with the FIUTT are treated as strictly confidential. Tokenprime ensures that:

- The identity of employees who make internal reports is protected to the extent permitted by law;
- Information relating to STRs/SARs is restricted to authorised personnel only; and
- No adverse action is taken against any employee for making a report in good faith.

6.7 Ongoing Monitoring Following Reporting

The submission of an STR or SAR does not, in itself, terminate Tokenprime's obligations. Following reporting, Tokenprime may:

- Increase monitoring of the customer or activity;
- Apply enhanced due diligence measures;
- Restrict, suspend, or terminate the business relationship where appropriate and lawful; and
- Take any additional action required to mitigate ML/TF/PF risk.

All actions taken post-reporting shall be documented and aligned with regulatory expectations and internal policies.

7. Terrorist Funds Reporting (TFR)

7.1 Purpose and Legal Basis

Tokenprime maintains specific measures and procedures for the identification, reporting, and handling of terrorist funds in accordance with the Anti-Terrorism Act, Chap. 12:07, the Prevention of Money Laundering Act, 2002 (as amended), the Financial Obligations Regulations, 2010, and guidance issued by the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT").

Terrorist Funds Reporting ("TFR") obligations are distinct from Suspicious Transaction or Activity Reporting and require immediate action where knowledge or suspicion exists that funds or assets are owned or controlled by, or are linked to, terrorist organisations, terrorists, or persons designated under applicable sanctions regimes.

7.2 Screening Against Designated Lists

Tokenprime conducts screening of customers, beneficial owners, authorised persons, and relevant counterparties against designated lists, including:

- Lists issued pursuant to United Nations Security Council Resolutions;
- Domestic designation lists published or recognised by competent authorities; and
- Any other sanctions or terrorist designation lists notified by the FIUTT or other competent authorities.

Screening is conducted:

- Prior to establishing a business relationship;
- On an ongoing basis during the course of the relationship; and
- Upon updates to applicable designation lists.

7.3 Identification of Terrorist Funds

Where Tokenprime identifies or reasonably suspects that it is in possession or control of funds or assets that are linked to terrorism, terrorist organisations, or designated persons, whether directly or indirectly, such funds shall be treated as terrorist funds for the purposes of this Policy.

Such identification may arise from:

- Screening alerts or list matches;
- Transaction monitoring activities;
- Information received from competent authorities; or
- Internal reports from employees.

Immediate reporting obligations apply regardless of the value of the funds or whether a transaction has been attempted or completed.

7.5 Role of the Compliance Officer

The Compliance Officer is responsible for:

- Assessing potential terrorist fund indicators and screening alerts;
- Ensuring that reports are submitted promptly and accurately to the FIUTT;
- Acting as the primary liaison with the FIUTT and other competent authorities on TFR matters; and
- Ensuring that internal controls, training, and procedures support effective identification and reporting of terrorist funds.

7.6 Confidentiality and Prohibition on Tipping-Off

All matters relating to terrorist funds reporting are handled with the highest degree of confidentiality. Tokenprime strictly prohibits tipping-off and ensures that:

- No customer or third party is informed that a report has been made or is contemplated; and
- Information relating to TFR is disclosed only to authorised personnel and competent authorities, as required by law.

7.7 Ongoing Monitoring and Risk Mitigation

Following the reporting of terrorist funds, Tokenprime shall:

- Continue to cooperate fully with the FIUTT and law enforcement agencies;
- Apply enhanced monitoring to any related customer relationships or activities;
- Take appropriate steps to mitigate ongoing ML/TF/PF risks, including termination of relationships where lawful and appropriate.

8. Quarterly Terrorists Property Report (QTR)

8.1 Purpose and Legal Basis

Tokenprime complies with its statutory obligation to submit Quarterly Terrorists Property Reports ("QTRs") in accordance with the Proceeds of Crime Act ("POCA"), the Anti-Terrorism Act, Chap. 12:07, and guidance issued by the Financial Intelligence Unit of Trinidad and Tobago ("FIUTT").

The purpose of the QTR is to enable the FIUTT to monitor, on a continuous basis, whether financial institutions and supervised entities are in possession or control of terrorist property or assets linked to designated persons or organisations.

8.2 Scope of the Quarterly Reporting Obligation

As a Reporting Entity, Tokenprime submits a QTR to the FIUTT **every three (3) months**, irrespective of whether terrorist property has been identified during the reporting period.

The obligation to submit a QTR applies:

- Where Tokenprime is in possession or control of terrorist property; and
- Where Tokenprime confirms that it is **not** in possession or control of terrorist property.

A "nil" return is therefore required where no terrorist property is identified.

8.3 Designated List Review and Screening

For the purposes of preparing the QTR, Tokenprime:

- Consults all applicable designated lists, including those issued pursuant to United Nations Security Council Resolutions and any domestic designation lists recognised by the FIUTT;
- Cross-references designated persons and entities against its customer, beneficial owner, and transaction databases; and
- Documents the outcome of such screening activities.

Screening is conducted using a risk-based and systematic approach to ensure completeness and accuracy.

8.4 Submission of the QTR

The Quarterly Terrorists Property Report is:

- Prepared and submitted in the prescribed format and manner specified by the FIUTT;
- Submitted within the reporting timelines established by the FIUTT; and
- Signed or authorised by the Compliance Officer or, in their absence, the Alternate Compliance Officer.

Where terrorist property is identified, the QTR submission does not replace the obligation to immediately report terrorist funds under Section 7 of this Policy.

8.5 Roles and Responsibilities

The Compliance Officer is responsible for:

- Coordinating the preparation and submission of QTRs;
- Ensuring the accuracy, completeness, and timeliness of all quarterly submissions;
- Maintaining records evidencing screening and reporting activities; and
- Acting as the primary point of contact with the FIUTT for QTR-related matters.

8.6 Record Retention and Audit Trail

Tokenprime retains copies of all QTR submissions, supporting documentation, and screening results in accordance with its record-keeping obligations. These records are made available to auditors, the FIUTT, and other competent authorities upon lawful request.

8.7 Confidentiality and Tipping-Off

All information relating to QTR preparation and submission is treated as confidential. Tokenprime strictly prohibits tipping-off and ensures that no customer or third party is informed of the existence, content, or outcome of any QTR submission.

9. Independent Testing and Audit

9.1 Purpose and Regulatory Requirement

Tokenprime maintains an independent testing and audit function to assess the adequacy, effectiveness, and ongoing compliance of its AML/CFT framework. Independent testing is a mandatory component of Tokenprime's compliance obligations and serves as a key assurance mechanism for Senior Management, the Board of Directors, and supervisory authorities.

The objective of independent testing is to:

- Evaluate compliance with applicable AML/CFT laws, regulations, and FIUTT guidance;
- Assess the effectiveness of internal controls, risk management, and reporting mechanisms;
- Identify deficiencies, weaknesses, or emerging risks; and
- Recommend corrective actions and enhancements.

9.2 Frequency and Scope of Independent Testing

Independent testing of Tokenprime's AML/CFT framework is conducted **at least annually**, or more frequently where:

- Required by the FIUTT or another competent authority;
- Material deficiencies are identified;
- There are significant changes to Tokenprime's business model, products, services, or risk profile; or
- There are material changes in applicable laws or regulatory expectations.

The scope of independent testing includes, at a minimum:

- The AML/CFT Compliance Programme and related policies and procedures;
- Customer Due Diligence (CDD) and Enhanced Due Diligence (EDD) processes;
- Risk-Based Approach and risk assessment methodology;

- Transaction monitoring and suspicious activity detection;
- STR, TFR, and QTR reporting processes;
- AML/CFT training programme;
- Record-keeping and data retention practices;
- Effectiveness and independence of the Compliance Officer function.

9.3 Independence and Qualifications

Independent testing may be conducted by:

- An internal audit function that is operationally independent of AML/CFT compliance activities; or
- An external, suitably qualified, and independent professional or firm with demonstrated AML/CFT expertise.

Individuals involved in independent testing must not be directly responsible for the design, implementation, or operation of the AML/CFT framework being reviewed.

9.4 Reporting and Remediation

The findings, conclusions, and recommendations arising from independent testing are:

- Documented in a formal written report;
- Submitted to Senior Management and, where applicable, the Board of Directors; and
- Retained as part of Tokenprime's compliance records.

Senior Management is responsible for:

- Reviewing audit findings in a timely manner;
- Approving remediation plans and corrective actions; and
- Ensuring that identified deficiencies are addressed within defined timelines.

Where required, Tokenprime shall provide independent testing reports or remediation updates to the FIUTT.

10. Record Keeping and Registers

10.1 Record-Keeping Obligations

Tokenprime maintains comprehensive and secure records in accordance with applicable AML/CFT legislation and FIUTT guidance. Proper record-keeping supports effective monitoring, investigations, audits, and regulatory oversight.

Tokenprime retains records, in electronic or written form, for a minimum period of **six (6) years** from the date of:

- Completion of a transaction;

- Termination of a customer relationship; or
- Submission of a report to the FIUTT, as applicable.

10.2 Types of Records Maintained

Tokenprime retains, at a minimum, the following categories of records:

- Customer identification and verification data obtained through CDD and EDD processes;
- Beneficial ownership information;
- Account files and business correspondence;
- Records of all domestic and international transactions;
- Transaction monitoring alerts and investigation outcomes;
- Risk assessments and risk classification decisions;
- STR, TFR, and QTR submissions and supporting documentation;
- AML/CFT training materials and attendance records;
- Independent testing and audit reports.

Records are maintained in a manner that allows for timely retrieval and reproduction upon lawful request.

10.3 Registers Maintained by the Compliance Officer

The Compliance Officer maintains up-to-date registers to support oversight, auditability, and regulatory inspection, including:

- AML/CFT Training Register;
- Internal Suspicious Activity Register;
- STR Submission Register;
- Terrorist Funds Reporting (TFR) Register;
- Quarterly Terrorists Property Report (QTR) Register;
- Law Enforcement Agency (LEA) Enquiry Register.

Registers are accessible to Senior Management, auditors, and competent authorities upon lawful request, subject to confidentiality requirements.

10.4 Confidentiality, Security, and Data Protection

All AML/CFT records and registers are:

- Stored securely with appropriate access controls;
- Protected against unauthorised access, alteration, or loss; and
- Handled in accordance with Tokenprime's data protection and confidentiality obligations.

Information relating to suspicious activity, investigations, or reports submitted to the FIUTT is treated as strictly confidential and is disclosed only where legally permitted.

10.5 Availability to Competent Authorities

Tokenprime ensures that all required records and registers are made available promptly to the FIUTT, auditors, and law enforcement agencies in accordance with lawful requests, court orders, or statutory obligations.