
Company: 4XHub Ltd
No: LL16731
License No: MB/20/0055
Date Updated: October 2022

Anti-Money Laundering and Counter-Terrorism Financing Program

Introduction and Part A

4XHub Ltd

INTRODUCTION

1. ABOUT THE AML/CTF ACT

- 1.1 The *Anti-Money Laundering (“AML”) and Anti-Terrorism Financing (“CTF”) and Proceeds of Unlawful Activities Act 2001 (“AML/CTF Act”)* and the *Guidelines on Money-Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Labuan Key Reporting Institutions (“Guidelines”)*’s broad purpose is to regulate financial transactions in a way that helps identify, mitigate and manage money laundering and terrorism financing risks.
- 1.2 The AML/CTF Act provides general principles and obligations while detailed operating rules are covered in Guidelines issued by the Labuan Financial Services Authority (“LFSA”). Bank Negara Malaysia sets AML/CFT policy in Malaysia, adopting a risk-based supervisory approach and issuing periodic guidance to Malaysian financial institutions in line with the recommendations of the Asia/Pacific Group on Money Laundering. LFSA acts as the regulatory authority for the capital market and regulates the Labuan International Business Financial Centre, the special economic zone on the island of Labuan.
- 1.3 The Guidelines applies to persons licensed or registered to carry on any activity under the Labuan Financial Services and Securities Act 2010 (“LFSSA”) (“Labuan KRI”).
- 1.4 4XHub Ltd (“4XHub”) is licensed and registered to carry on such activities and is therefore a Labuan KRI. The activities to be carried out are vulnerable to abuse by criminals for money laundering or terrorism financing purposes.
- 1.5 The Guidelines adopts a risk-based approach. This approach means that the reporting entity decides how best to identify, mitigate, and manage the risk of money laundering and terrorism financing through its business. Reporting institutions therefore need to undertake a comprehensive assessment of these risks relative to their businesses. Reporting institutions need to be able to demonstrate that they have carried out such an assessment and have a documented program in place to identify, mitigate and manage the risk of their products or services being used to facilitate money laundering or terrorism financing.

2. ADOPTION

- 2.1 4XHub adopts Parts A and B of this Program as its AML/CTF Program (“Program”) for the purposes of the Guidelines. On and from October 2022, 4XHub must comply with the Program, as varied from time to time.

VERSION NUMBER	DATE UPDATED	NOTES
----------------	--------------	-------

1	October 2022	New AML/CTF Compliance Program prepared in consultation with Marcus Tan & Co.
---	--------------	---

3. RECORDS RELATING TO 4XHUB'S AML/CTF PROGRAM

3.1 The AML/CTF Compliance Officer ("**AML/CTF CO**") ensures that the following records are retained:

- (a) this Program and each variation to it;
- (b) the Board of Directors' approval of the Part A of this Program, and each variation to Part A of this Program;
- (c) LFSA's feedback and correspondence, if applicable;
- (d) external and internal AML/CTF reviews; and
- (e) correspondence with external lawyers on AML/CTF issues.

3.2 The records referred to in Section 3.1 of this Program are be retained:

- (a) in the case of records relating to the adoption of each variation to this Program and 4XHub's Program, during the period it or any part of it remains in force and for seven (7) years after it ceases to be in force; and
- (b) for the period determined by the AML/CTF CO for all other records.

4. PENALTIES

4.1 Failure to comply with the obligations under the AML/CTF Act may result in civil or criminal penalties.

4.2 Offences under the AML/CTF Act may attract penalties which shall not exceed a fine of three million ringgit or imprisonment for a term not exceeding five years or both.

5. DEFINITIONS

5.1 Words and phrases defined in the AML/CTF Act, LFSSA or the Guidelines have the same meaning when used in this Program unless otherwise specified.

DEFINITIONS	
Authorised Officer	in accordance with section 2 of the LFSSA, an authorised officer is an officer duly authorised by LFSA under subsection 3(2) of the LFSSA.
Beneficial Owner	<p>Refers to any natural person(s) who ultimately owns or controls a customer and/or the natural person on whose behalf a transaction is being conducted. It also includes those natural persons who exercise ultimate effective control over a legal person or arrangement.</p> <p>Reference to “ultimately owns or control” or “ultimate effective control” refers to situations in which ownership or control is exercised through a chain of ownership or by means of control other than direct control.</p>
Digital Currency	Means a digital representation of value that functions as a medium of exchange and is interchangeable with any money, including through the crediting or debiting of an account, but does not include electronic money.
Politically Exposed Persons (“PEP”)	<p>Refers to:</p> <ul style="list-style-type: none"> (a) foreign PEPs – individuals who are or who have been entrusted with prominent public functions by a foreign country. For example, Heads of State or Government, senior politicians, senior government, judicial or military officials, senior executives of state-owned corporations and important political party officials; (b) domestic PEPs – individuals who are or have been entrusted domestically with prominent public functions. For example, Heads of State or Government, senior politicians, senior government (includes federal, state, and local government), judicial or military officials, senior executives of state-owned corporations and important political party officials; or (c) persons who are or have been entrusted with a prominent function by an international organisation which refers to members of senior management. For example, directors, deputy directors and members of the Board or equivalent functions. <p>The definition of PEPs is not intended to cover middle ranking or more junior individuals in the foregoing categories.</p>

<p>Non-photographic identification document</p>	<ul style="list-style-type: none"> (a) a birth certificate; (b) a citizenship certificate issued by the Government; (c) a citizenship certificate issued by a foreign government that, if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator; or (d) a birth certificate issued by a foreign government, the United Nations, or an agency of the United Nations that, if it is written in a language that is not understood by the person carrying out the verification, is accompanied by an English translation prepared by an accredited translator.
<p>Photographic identification document</p>	<ul style="list-style-type: none"> (a) a national registration identity card issued by the Government for the purpose of proving the person's full name, residential address, date of birth, nationality, age which contains a photograph of the person in whose name the document is issued; (b) a passport issued by the Government; (c) a passport or a similar document issued for the purpose of international travel, that: <ul style="list-style-type: none"> (i) contains a photograph and either: <ul style="list-style-type: none"> A. the signature of the person in whose name the document is issued; or B. any unique identifier of the person in whose name the document is issued; (ii) is issued by a foreign government, the United Nations, or an agency of the United Nations; and (iii) if it is written in a language that is not understood by the person carrying out the verification - is accompanied by an English translation prepared by an accredited translator.
<p>Reasonable measures</p>	<p>means appropriate measures which are commensurate with the money laundering or terrorism financing risks.</p>

6. PURPOSE AND APPLICATION OF PART A

- 6.1 Part A of this Program (“**Part A**”) is designed to identify, mitigate, and manage the money laundering or terrorism financing risk which 4XHub may reasonably face in the provision of our services.
- 6.2 Part A applies to all aspects of 4XHub’s business, to which the AML/CTF Act and the Guidelines are applicable and to any functions which are outsourced to third parties.
- 6.3 All 4XHub’s staff are given a copy of Part A of this Program and provided with necessary training so they understand the nature and purpose of our business relationship with 4XHub’s customers and 4XHub’s obligations under the AML/CTF Act and the Guidelines.

7. OVERSIGHT BY THE BOARD OF DIRECTORS AND BOARD OF DIRECTORS’ APPROVAL

- 7.1 Part A of this Program was approved and adopted by 4XHub’s Board of Directors (“**Board**”) on 10th October 2022
- 7.2 Part A is subject to ongoing oversight by the Board, senior management and 4XHub’s AML/CTF compliance officer of 4Xhub (“**AML/CTF CO**”), and
 - (a) The AML/CTF CO, in consultation with senior management, reviews Part A on at least an annual basis to ensure Part A is:
 - (i) drafted in accordance with the AML/CTF Act, the Guidelines and other applicable laws and regulations;
 - (ii) applicable and relevant to the functions of 4XHub’s business operations; and
 - (iii) any changes to 4XHub’s services have been reflected in Part A.
 - (b) The review of Part A is presented to the Board at the next Board meeting of the Board of Directors and AML/CTF CO; and
 - (c) Any changes to Part A are required to be reviewed and approved by the Board.
- 7.3 Part B does not require Board’s approval but is subject to ongoing oversight by the Board, senior management and 4XHub’s AML/CTF CO. Any changes to Part B are required to be reviewed and approved by the AML/CTF CO of 4XHub.
- 7.4 Quarterly meetings with the Board and senior management are held by the AML/CTF CO to report on the following:

- (a) significant changes to the AML or CTF risks affecting 4XHub;
- (b) compliance with this Program, the AML/CTF Act and the Guidelines by 4XHub;
- (c) the results of and any report produced for any internal or external review of this Program;
- (d) assessment of the AML and CTF risks associated with any new product, delivery channels, business partners and any operation of 4XHub, and whether the existing procedures and controls are appropriate and proportionate to the AML and CTF risks;
- (e) any feedback from LFSA and/or other relevant authorities; and
- (f) changes to relevant legislation.

8. 4XHUB'S AML/CTF COMPLIANCE OFFICER

- 8.1 4XHub has appointed Elsa Dewi Santika as 4XHub's AML/CTF CO for the purposes of the AML/CTF Act and the Guidelines.
- 8.2 4XHUB's AML/CTF CO is also a director of 4XHUB. The AML/CTF CO is always be part of the management of 4XHub, report directly to the Board, communicate regularly with senior management and possess sufficient skills and experience to carry out the roles of the AML/CTF CO.
- 8.3 The AML/CTF CO is responsible for implementing and over-seeing 4XHub's obligations under the AML/CTF Act and the Guidelines in accordance with its compliance procedures, including but not limited to:
 - (a) providing regulatory and/or legal updates in relation to the AML/CTF Act and the Guidelines – the AML/CTF CO shall regularly monitor the information, updates and/or circulars publishes by LFSA and other relevant authorities on their websites and take such information into account when implementing 4XHub's Program;
 - (b) ongoing monitoring of the implementation of the Program;
 - (c) considering and incorporating feedback from employees and clients;
 - (d) ensuring overall compliance with the AML/CTF Act, LFSSA and the Guidelines;
 - (e) investigating suspicious matters, issues or incidents in 4XHub's operation which may give rise to ML/TF risks;

- (f) maintaining records; and
 - (g) conducting employee risk awareness training in accordance with 4XHub’s obligations under the AML/CTF Act and the Guidelines.
- 8.4 The AML/CTF CO is authorised to act independently and to delegate any of their responsibilities under this Program to another 4XHub employee, agent or responsible third party provided if it is reasonable to do so. The AML/CTF CO also liaises with 4XHub’s external compliance consultant.
- 8.5 If 4XHub or any employee or representative of 4XHub receives correspondence or enquiries from LFSA or any relevant authority, those enquiries are to be directed to the AML/CTF CO at first instance.

9. REVIEW OF THE PROGRAM

9.1 **Internal Reviews:** The AML/CTF CO must regularly assess 4XHub’s ML and TF risk and take steps to have this Program modified appropriately.

INTERNAL REVIEWS	
Responsible Person:	AML/CTF CO
Frequency:	Quarterly (unless otherwise indicated based on the factors listed below)
When an internal review must be conducted:	
<ul style="list-style-type: none"> (a) Where a significant change in the ML or TF risk relating to the services provided by 4XHub has been identified; (b) prior to 4XHub introducing a new activity to the market; (c) prior to 4XHub adopting a new method of delivering an activity; (d) prior to 4XHub adopting a new technology or developing technology used for the provision of an existing or new activity; and (e) where the AML/CTF CO identifies changes arising in the nature of the business relationship, control structure or beneficial ownership of 4XHub’s customers. <p>The above issues must also be considered during each independent review.</p>	

9.2 **Independent Reviews:** The AML/CTF CO must engage an experienced internal or external third party to conduct an independent review of this Program.

INDEPENDENT REVIEWS	
Responsible Person:	AML/CTF CO - report the results of the independent review to the Board of 4XHub. Reports detailing the review (both internal and external) and the results provided to the Board and senior management for consideration and discussion. The reports then form the basis of a timetable to address the findings within the timeline set by the Board.
Frequency:	Annually or as otherwise determined by the Board.
Who should do the external review?	<p>The independent party conducting the review must be independent and:</p> <ul style="list-style-type: none"> (a) have not been involved in undertaking any of the functions or measures required to be carried out under this Program; (b) have not been involved in the design, development, implementation, maintenance or management of this Program; (c) have not been involved in the development of 4XHub’s risk assessment or related internal controls; (d) have access to the employees of 4XHub and is able to make enquiries of any employee; (e) have access to the records, personnel and property of 4XHub within the context of 4XHub’s obligations under the <i>Personal Data Protection Act 2010</i>; (f) be impartial and objective in performing their duties and should not be inappropriately influenced by management of 4XHub; and (g) be appropriately qualified to conduct the review.
What should be covered in the review?	<p>The independent party, while carrying out the independent review, must:</p> <ul style="list-style-type: none"> (a) assess the effectiveness of Part A having regard to the ML and TF risk of 4XHub; (b) assess whether Part A complies with the Guidelines; (c) assess whether Part A has been effectively implemented;

(d) assess whether 4XHub has complied with Part A;

The independent party, while carrying out the independent review, may also:

- (a) assess the risk management resources available to 4XHub including, but not limited to funding and staff allocation;
- (b) identify any future needs relevant to the nature, size and complexity of 4XHub;
- (c) assess the ongoing risk management procedures and controls to identify any failures – the following factors should be taken into account:
 - (i) any market information relevant to the global AML/CTF environment which may have an impact on the ML or TF risk faced by 4XHub;
 - (ii) failure to include all mandatory legislative components in the Program;
 - (iii) failure to gain approval of the Program from 4XHub's Board;
 - (iv) insufficient or inappropriate employee due diligence;
 - (v) frequency and level of risk awareness training not aligned with potential exposure to ML/TF risk(s);
 - (vi) changes in business functions which are not reflected in this Program;
 - (vii) failure to consider feedback from the relevant authorities (for example, advice regarding an emerging ML/TF risk);
 - (viii) failure to undertake an independent review (at an appropriate level and frequency) of the content and application of this Program;
 - (ix) legislation incorrectly interpreted and applied in relation to a customer identification procedure;
 - (x) customer identification and monitoring systems, policies and procedures that fail to:
 - A. prompt, if appropriate, for further identification and/or verification to be carried out when the ML/TF risk posed by a customer increases;
 - B. detect where a customer has not been sufficiently identified and prevent the customer from receiving the service;

- C. take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;
 - D. take appropriate action where the identification document provided is neither an original nor a certified copy;
 - E. recognise foreign identification issued by a high-risk jurisdiction;
 - F. record details of identification documents, for example, the date of issue;
 - G. consult appropriate resources in order to identify high-risk customers;
 - H. identify when an expired or old identification document has been used;
 - I. collect any other name(s) by which the customer is known;
 - J. be subject to regular review;
- (xi) lack of access to information sources to assist in identifying higher risk customers (and the jurisdiction in which they may reside), such as PEPs, terrorists and narcotics traffickers;
 - (xii) lack of ability to train staff consistently and correctly and/or third parties, particularly in areas with high turnover in:
 - A. customer identification policies, procedures, and systems; and
 - B. identifying potential AML/CTF risks; and
 - (i) assess the acceptance of documentation that may not be readily verifiable.

If the independent reviewer determines it is appropriate, the review may also:

- (a) assess whether the risk-based procedures and processes adopted in 4XHub's Program have changed such that alterations need to be made;
- (b) assess whether Part B is sufficient to cover the ML/TF risks posed by existing and potential customers of 4XHub; and
- (c) assess whether any additional changes need to be made to this Program because of changes to the AML/CTF Act and Guidelines and the AML/CTF environment generally.

10. REGULATOR FEEDBACK

- 10.1 Where a prevailing authority provides 4XHub with feedback regarding performance in the management of ML/TF risk, any receipt of such feedback is immediately referred to the AML/CTF CO for attention.
- 10.2 The AML/CTF CO assesses the relevant authority's feedback to determine if any changes to this Program are required and implement any such changes as soon as reasonably practicable with the Board's approval.

11. WHAT IS MONEY LAUNDERING?

- 11.1 Money laundering ("**ML**") is the process used to disguise the illegal origin of the proceeds of illegal activities such as drugs trafficking, tax evasion, smuggling, theft, terrorism, arms trafficking, and corrupt practices. It is the name given to the process by which illegally obtained funds are given the appearance of having been legitimately obtained.
- 11.2 Whilst initially there was a focus on cash transactions there has recently been a growth in awareness of the sophistication used by money launderers to structure transactions to prevent detection and investment by them in a range of assets within the financial services sector.
- 11.3 There are three main stages of ML:
- (a) **Placement** – the physical disposal of the proceeds e.g., deposit into an account. This is usually when the illegal funds or assets are first brought into the financial system.
 - (b) **Layering** – creating complex layers of financial transactions to separate the proceeds from their source and hide any audit trail to maintain anonymity e.g., transferring investments from one product to another. Many different techniques can be used to layer the funds including use of corporations and trusts. The funds may be shuttled through a web of many accounts, companies, and countries in order to disguise their origins.
 - (c) **Integration** – taking the proceeds of ML and placing them back into the financial system so that they appear to be normal business proceeds with apparent legitimacy e.g., settling money into a trust without links to the previous illicit funds with the trust then making investments.

12. WHAT IS TERRORISM FINANCING?

- 12.1 Terrorism financing (TF) is often the reverse of ML whereby funds within a legitimate source are put into the financial system and redirected into the hands of terrorist organisations. Where those funds are the proceeds of illegal activities including fraud and criminal activities, they may also be captured by AML controls.
- 12.2 Terrorist organisations obtain money from several legitimate and illegitimate sources, such as:
- (a) **Illegal Activities** – terrorists obtain funds from illegal activities, such as drug trafficking, smuggling, kidnapping and extortion.
 - (b) **Rich Individuals** - it is increasingly apparent that rich individuals are a critical source of terrorist financing.
 - (c) **Charitable and Religious Institutions** – charitable and religious institutions can be a source of terrorist funding. They are ideal conduits because they are very lightly regulated and do not need to provide a commercial justification for their activities.
 - (d) **Commercial Enterprise** – terrorist organisations may run or own otherwise legitimate commercial enterprise to generate profits and commingle illegal funds. These include jewellery businesses, trading companies, convenience stores, real estate ventures and investment management firms.
 - (e) **State Sponsors** – several rogue nations have been known to provide assistance, financial support and safe harbour to terrorist organisations.

13. SERVICES PROVIDED BY 4XHub

- 13.1 4XHub carries out such licensed and regulated activities under the LFSSA.
- 13.2 4XHub has undertaken assessment of the ML/TF risks associated with its services considering the following factors:
- (a) nature, size and complexity of its business;
 - (b) type of ML/TF risk that 4XHub might reasonably face;
 - (c) customer types, including any politically exposed persons;
 - (d) types of services provided;
 - (e) methods by which those services are delivered;

- (f) jurisdictions in which those services are delivered;
- (g) responsible third parties to whom 4XHub outsource its AML/CTF obligations;
- (h) any significant changes in ML/TF risk;
- (i) any ML/TF risk posed by:
 - (i) new services – the assessment is conducted prior to the introduction of the new services;
 - (ii) new delivery method - the assessment is conducted prior to the introduction of the new delivery method; and
 - (iii) new or developing technologies used in the provision of the services - the assessment is conducted prior to the introduction of the new technologies.

13.3 **Significant Changes to the Customer's Business:** if 4XHub notices that any of the following significant changes to the customer's business have taken place, 4XHub obtains further details in writing from the customer to satisfy itself that the customer does not present an unacceptable risk. Significant changes can be identified as one of the following:

- (a) changes in the nature of the customer's business or business relationship;
- (b) changes in the customer's control structure;
- (c) changes in the customer's beneficial ownership; or
- (d) changes in the way a customer conducts transactions.

13.4 **New Services:** prior to a new service being introduced to the market by 4XHub, the AML/CTF CO assesses it to determine whether it involves the provision of a service. When it is determined by the AML/CTF CO that a new service involves the provision of a service, the AML/CTF CO assesses the ML/TF risk involved in the provision of the new service.

13.5 Board approval must be received before a new service is introduced to the market. The Board must be given a copy of the risk assessment conducted before the approval is granted.

14. RISK ASSESSMENT AND MANAGEMENT MATRIX

14.1 4XHub has put in place a Risk Assessment and Management Matrix (“**AML/CTF Matrix**”) which outlines our assessment of various ML/TF risks associated with our services and the measures we put in place to control such risks. The AML/CTF Risk Matrix is attached at Annexure A of the Program.

RISK ASSESSMENT AND MANAGEMENT MATRIX	
Responsible Person:	AML/CTF CO - review and update the AML/CTF Matrix to ensure that the following items are contained in the AML/CTF Matrix and updated regularly.
Risk identification of the main ML/TF risks:	<ul style="list-style-type: none"> (a) Customer types (b) Products & services (c) Business practices & delivery methods (d) Countries we deal with
Risk Assessment / Measurement of the risk:	<ul style="list-style-type: none"> (a) Likelihood – chance of risking happening (b) Impact – the amount of loss or damage if the risk is to occur (c) Likelihood x impact – the level of risk or risk score
Mitigating and managing the risk:	<ul style="list-style-type: none"> (a) Minimise and manage the risks (b) Application of strategies, policies and procedures (c) Existing systems and controls (d) Risk plan
Risk Monitoring and Review:	<ul style="list-style-type: none"> (a) Development and implementation of monitoring process (b) Record keeping (c) Review of risk plan and this Program (d) Independent review

15. EMPLOYEE DUE DILIGENCE PROGRAM

15.1 New Employees

- (a) The AML/CTF CO must be informed of all prospective new employees before they are issued with an employment contract with 4XHub. The prospective employee is informed that their employment is subject to the result of their background checks.
- (b) The AML/CTF CO must undertake a risk assessment for all newly created roles or previously existing roles that are to be filled with a new employee to determine whether they are able to facilitate the commission of a ML/TF offence.
- (c) For all new employees, regardless of their position, 4XHub must carry out all the following checks, prior to an offer of employment being made:
 - (i) collect and verify their identification documents as if they are a new client;
 - (ii) obtain a copy of their working visa (where the employee is not a Malaysian citizen);
 - (iii) carry out at least two (2) reference checks;
 - (iv) obtain copies of all tertiary educational qualifications or if none, the person's highest educational qualification;
 - (v) carry out a criminal history check; and
 - (vi) carry out a bankruptcy/credit check.
- (d) If 4XHub determines the results to any of these procedures are not satisfactory, 4XHub will not offer that person employment. Results which are not satisfactory may include:
 - (i) a criminal history check which returns a result including fraud, dishonest conduct or other ML/TF offences;
 - (ii) the prospective employee is currently bankrupt;
 - (iii) the prospective employee does not hold a valid working visa;
 - (iv) the identity of the prospective employee cannot be verified; or

- (v) the references obtained by 4XHub uncover evidence that the prospective employee has been involved in activities which may constitute an ML/TF risk to 4XHub.

15.2 Existing Employees

- (a) Where 4XHub proposes to transfer or promote an existing employee to a new role, a risk assessment is undertaken of that role to determine whether they can facilitate the commission of a ML/TF offence.
- (b) Where an employee is transferred or promoted to a role that may put them in a position to facilitate the commission of a ML/TF offence in connection with the provision of a service, the AML/CTF CO:
 - (i) obtains an updated copy of the employee's working visa (where the employee is not a Malaysian citizen); and
 - (ii) carries out any other identification, reference, criminal history checks, bankruptcy or credit checks that are deemed necessary by the AML/CTF CO.
- (c) Employees who fail to comply with the procedures above are reported to 4XHub's Board. Appropriate disciplinary action, including termination of employment, occurs where it is deemed necessary.

15.3 Copies of employee checks undertaken must be kept in accordance with the 4XHub's Document Retention Policy.

15.4 Managing Non-Compliance

- (a) 4XHub, on an ongoing basis, monitors compliance with this Program.
- (b) If an employee fails to comply with this Program, the matter is referred to the AML/CTF CO immediately. The AML/CTF CO may then take any of the following actions:
 - (i) undertake an internal spot check on the employee's performance to check compliance with 4XHub's policies and procedures;
 - (ii) implement a higher level of supervision of the employee;
 - (iii) provide a warning to the employee for non-compliance with procedures and breach of the Program; or
 - (iv) if breaches are repeated without reasonable excuse, consider transferring or dismissing the employee in consultation with the Board.

16. RISK AWARENESS TRAINING PROGRAM

- 16.1 4XHub implements a Risk Awareness Training Program (“**RATP**”) designed to ensure each employee receives appropriate ongoing training on the ML/TF risk that 4XHub may face.
- 16.2 The RATP is designed to enable employees to understand:
- (a) 4XHub’s obligations under the AML/CTF Act and the Guidelines;
 - (b) the consequences of non-compliance with the AML/CTF Act and the Guidelines;
 - (c) the type of ML/TF risk that 4XHub might face and the potential consequences of such risk; and
 - (d) those processes and procedures provided for by this Program which are relevant to the work carried out by the employee.
- 16.3 All new employees are required to undergo the RATP as part of their induction process. All employees that are in positions identified as having ML/TF risk are required to undertake training on an annual basis, or whenever the AML/CTF CO considers necessary, for example when a new product or delivery channel is introduced.
- 16.4 The AML/CTF CO is responsible for maintaining the training register for both the induction training and any ongoing training conducted for each employee.
- 16.5 **Ongoing Compliance Training** – The AML/CTF CO may decide when compliance training by an external compliance consultant is necessary. The AML/CTF CO must, upon completion of the training, makes the training materials available to all employees. From time to time some employees, depending on the nature of their role and responsibilities, may be required to undertake additional training as directed by the AML/CTF CO.
- 16.6 **In-house AML/CTF Seminars** – The AML/CTF CO may decide when to organise the in-house AML/CTF seminars. The AML/CTF CO organises such seminars on a regular basis so that employees who come back to work from leave can refresh their knowledge.
- 16.7 **Non-attendance of Training Sessions** – Non-attendance at any training sessions, without reasonable excuse, is reported to the Board and the AML/CTF CO takes any disciplinary action they consider necessary.

16.8 **Compliance Policies** – all new employees receive a copy of this Program and all compliance policies of 4XHub within a reasonable time of commencing employment. All employees are expected to review these compliance policies on a regular basis and are required to complete a declaration stating that they have read the compliance policies.

16.9 **Document Retention Policy** – the AML/CTF CO must encourage all employees to read and understand the Document Retention Policy. Employees who fail, without reasonable excuse, to read the Document Retention Policy are reported to the Board who takes disciplinary action as they consider necessary.

17. OUTSOURCING

OUTSOURCING	
Outsourcing – due diligence requirements:	<p>Prior to 4XHub outsourcing any of its AML/CTF obligations, it:</p> <ul style="list-style-type: none"> (a) has an agreement in place with the party to whom the activities are outsourced (“Third Party Providers”); (b) where relevant, requires the Third-Party Providers to whom the activities are outsourced to implement the policies and procedures outlined in this Program; (c) assesses the ML/TF risk associated with the outsourcing of the particular activity; (d) conducts due diligence on the activities outsourced to ensure that outsourcing these activities and services does not increase the ML/TF risk 4XHub faces; (e) conducts due diligence on the Third-Party Providers to ensure that outsourcing activities to these parties does not increase the ML/TF risk 4XHub faces; (f) ensures that all Third-Party Providers understand: <ul style="list-style-type: none"> (i) 4XHub’s obligations under the AML/CTF Act and the Guidelines; (ii) the consequences of non-compliance with the AML/CTF Act and the Guidelines; (iii) the type of ML/TF risk 4XHub might face and the potential consequences of such risk; and (iv) those processes and procedures provided for by this Program that are relevant to the work carried out by the employee.

<p>Additional due diligence requirements where outsourcing customer identification functions:</p>	<p>In addition to the due diligence requirements above, 4XHub:</p> <ul style="list-style-type: none"> (a) conducts due diligence on the Third-Party Providers to ensure they hold the appropriate licences and/or registrations with all relevant regulators; (b) ensures Third Party Providers have an AML/CTF Policy in place which complies with the AML/CTF Act and the Guidelines; and (c) ensures the agreement in place between 4XHub and Third-Party Providers permits access to the KYC records of 4XHub’s clients. <p>When assessing the ML/TF risk associated with a Third-Party Provider undertaking customer identification procedures on its behalf having regard to the following factors:</p> <ul style="list-style-type: none"> (a) the existence and quality of Third-Party Providers’ AML/CTF Policy; (b) the resources of Third-Party Providers, including the number of staff and access to technological resources; (c) the outcome of due diligence undertaken in respect of Third-Party Providers; and (d) quotes received and references from former and current partners of Third-Party Providers.
<p>Reviews:</p>	<ul style="list-style-type: none"> (a) The AML/CTF CO undertakes annual reviews of all Third-Party Providers to assess whether the Third-Party Provider: <ul style="list-style-type: none"> (i) has performed their functions within the scope of the agreement with 4XHub; (ii) maintains appropriate resources, licences and registrations; (iii) has met their AML/CTF obligations under the AML/CTF Act and the Guidelines; (iv) has caused an increase in the ML/TF risk 4XHub faces.

17.1 4XHub maintains a separate External Services Providers.

18. PROVISION OF SERVICES THROUGH PERMANENT ESTABLISHMENTS IN FOREIGN COUNTRIES

18.1 4XHub does not provide services through permanent establishments in foreign countries.

18.2 If at any time 4XHub begins to provide services at or through permanent establishments in foreign countries, the AML/CTF CO will review this Program in its entirety, prepare a risk assessment and propose any necessary changes to the Board for approval. The Board will, in consultation with senior management and any external compliance consultant, review and consider the proposed changes considering of any ML/TF risks imposed by provision of services through a permanent establishment in that particular jurisdiction.

19. RECORD KEEPING OBLIGATIONS RELATING TO CUSTOMER IDENTIFICATION AND THE PROVISION OF SERVICES

19.1 When a customer identification procedure is required to be undertaken in accordance with Part B, a record of the following must be made:

- (a) the procedures undertaken; and
- (b) information obtained while carrying out the procedure.

19.2 A copy of these records is retained for at least seven (7) years after 4XHub has ceased to provide services to the customer.

19.3 Records retained under this section (whether in electronic or hard copy form) must be easily identifiable, easily located and easily retrievable, to:

- (a) provide the record to the relevant authority within a reasonable period; and
- (b) demonstrate to the relevant authority that 4XHub has complied with all obligations under the AML/CTF Act.

19.4 A copy of any other record made by 4XHub or received from a customer in relation to the provision of a service to the customer must be retained for seven (7) years after the record is made or received.

19.5 Details of record keeping, and handling are set out in 4XHub's Document Retention Policy.

20. TRANSACTION MONITORING

20.1 4XHub's transaction monitoring program consists of three steps:

- (a) Monitoring all customer transactions in accordance with 4XHub's policies, systems and procedures;
- (b) Identifying all suspicious transactions; and

(c) Taking the appropriate action.

20.2 The AML/CTF CO reviews the transaction monitoring system in consultation with the Board and 4XHub’s external compliance consultant.

20.3 The AML/CTF CO has the primary responsibility for transaction monitoring for both 4XHub. All transaction reports are reviewed by the Board on a quarterly basis.

20.4 All 4XHub’s employees receive training in transaction monitoring as part of the RATP.


20.5 4XHub shall provide reports to the relevant authority in an approved form that contains the required information.

21. SUSPICIOUS MATTER REPORTING

21.1 4XHub adopts a ‘Red Flag’ policy which requires employees to complete a Red Flag Indicator Sheet (please refer to Annexure B of this Program) for each new client and as a procedure to conduct ongoing transaction monitoring. 4XHub’s policies and procedures for suspicious matter reporting are set out in the table below.

SUSPICIOUS MATTER REPORTING	
Responsible Person	AML/CTF CO
Supervision	The Board of 4XHub has overall responsibility and oversight of 4XHub’s transaction reporting and monitoring program. The Board conducts monthly review of all SMRs submitted during the previous month to identify systemic issues.
1. What are the Suspicious Matter Reporting obligations?	
General Rules	4XHub must submit a SMR to the relevant authority if: (a) 4XHub commences to provide, or proposes to provide, a service to a person; or (b) a person requests 4XHub provides a service (of a kind ordinarily provided by us), or (c) a person makes an enquiry to 4XHub as to whether it would be willing provide a service (of a kind ordinarily provided by 4XHub);

	<p>and 4XHub forms a suspicious <u>on reasonable grounds</u> that:</p> <ul style="list-style-type: none"> (a) a person (or their agent) is not the person they claim to be, or (b) information we have may be: <ul style="list-style-type: none"> (i) relevant to the investigation or prosecution of a person for: <ul style="list-style-type: none"> A. an offence against any law; B. an evasion, or an attempted evasion, of a taxation law; or C. a ML/TF offence; (ii) of assistance in the enforcement of laws relating to proceeds of crime; or (c) providing a service may be: <ul style="list-style-type: none"> (i) preparatory to committing an offence related to ML or TF, or (ii) relevant to the investigation or prosecution of a person for an offence related to ML or TF.
<p>Who is covered by the general rules?</p>	<p>Existing, new, or potential customers, or an agent of an existing, new or potential customer.</p>
<p>When to report to the relevant authority?</p>	<p>4XHub must report a matter to the relevant authority if a reasonable person would conclude from all the circumstances and information available that an SMR must be submitted.</p> <p>4XHub's employees and AML/CTF CO are NOT necessarily expected to know or to establish:</p> <ul style="list-style-type: none"> (a) the exact nature of any criminal offence the customer may be involved in, or (b) funds or property have been acquired through illicit or criminal means.
<p>2. Identification of Suspicious Activities and Suspicious Customer Behaviour</p>	
<p>Red Flag Policy</p>	<p>4XHub adopts a 'Red Flag' policy which requires employees to complete the Red Flag Indicators Sheet and put a red flag when a red flag indicator exists.</p>

Red Flag Indicators What happens when a Red Flag is identified?	<p>4XHub develops a list of Red Flag Indicators Sheet (Annexure B). This sheet is updated on an ongoing basis.</p> <p>4XHub requires a copy of Annexure B to be completed:</p> <ul style="list-style-type: none"> (a) for each new client – before the provision of a service; and (b) for existing clients – on a half yearly basis or whenever the AML/CTF CO considers necessary.
	<p>Reporting Line:</p>  <pre> graph LR Employee[Employee] --> Supervisor[Immediate Supervisor] Supervisor --> AML[AML/CTF CO] AML --> Authority[AUTHORITY] </pre>
	<p>Existence of 1 Red Flag:</p>
	<p>The employee responsible:</p> <ul style="list-style-type: none"> (a) conducts the enhanced due diligence procedures set out in this Program and refer the matter to the immediate attention of their supervisor – the employee must not discuss the matter with anyone else except his/her immediate supervisor or the AML/CTF CO; (b) the supervisor reports to the AML/CTF CO once the results of enhanced due diligence are received; and (c) the AML/CTF CO then makes an assessment on whether an SMR is required.
	<p>Existence of more than 1 Red Flag:</p> <ul style="list-style-type: none"> (a) the employee responsible conducts the enhanced due diligence procedures set out in this Program and refer the matter to the immediate attention of the supervisor – the employee must not discuss the matter with anyone else except his/her immediate supervisor or the AML/CTF CO. (b) the supervisor reports to the AML/CTF CO once the results of enhanced due diligence are received. (c) the AML/CTF CO then makes an assessment on whether an SMR is required.

<p>Suspicion in relation to the identity of a customer</p>	<p>If the AML/CTF CO is notified of a suspicion relating to the identity of the customer, the AML/CTF CO must, within fourteen (14) days commencing after the day on which the AML/CTF CO was notified of the suspicion, do one of the following for the purpose of enabling the 4XHub to be reasonably satisfied that the customer is the person that he or she claims to be:</p> <ul style="list-style-type: none"> (a) review all KYC information in respect of the customer; (b) re-verify, from a reliable and independent source, any KYC Information that has been obtained in respect of the customer; or (c) verify, from a reliable and independent source, any previously unverified KYC Information that has been obtained in respect of the customer. <p>If:</p> <ul style="list-style-type: none"> (a) after reviewing the enhanced due diligence information from a customer in accordance with this Program, the AML/CTF CO is still not satisfied that the customer is who they claim to be; or (b) the AML/CTF CO is unable to collect any additional information from the customer, (c) then the AML/CTF CO <u>must</u> make a SMR to the relevant authority.
<p>Suspicion in relation to an existing customer</p>	<p>If the AML/CTF CO forms a reasonable suspicion in respect of an existing customer of 4XHub, the AML/CTF CO must, within fourteen (14) days commencing after the day on which the AML/CTF CO formed the suspicion, carries out the applicable customer identification procedures in Part B.</p>
<p>3. Discussion or Communication about the SMR</p>	
<p>Immediate Supervisor or the AML/CTF CO</p>	<p>4XHub’s employees or representatives must ONLY discuss the matter with their immediate supervisor, or the AML/CTF CO when their immediate supervisor is not available, unless as otherwise authorised by the AML/CTF CO.</p> <p>After the employee forms an initial suspicion about a customer, he/she uses discretion when making further enquiries about the customer, to minimise the risk of the customer realising an SMR has been submitted about them.</p>
<p>4. Submitting an SMR</p>	

Assessment of the situation and SMR	<p>If 4XHub's AML/CTF CO receives a notification in relation to a suspicious matter, the AML/CTF CO must:</p> <ul style="list-style-type: none"> (a) assesses the information which led the employee to form a suspicion; and (b) determines whether a SMR should be lodged. <p>If the AML/CTF CO determines that a SMR must be lodged in relation to a customer, 4XHub:</p> <ul style="list-style-type: none"> (a) keeps all records of the results of any enhanced customer due diligence conducted; and (b) reports the suspicion to the relevant authority through submitting an SMR: <ul style="list-style-type: none"> (i) within twenty-four (24) hours after the time when the AML/CTF CO forms the relevant suspicion, if the matter relates to TF; or (ii) in all other cases, within three (3) business days after the time when the AML/CTF CO forms the relevant suspicion; (c) consults with the relevant authority and other relevant enforcement agencies to determine how best to deal with the customer, if required; and (d) continues to transact with the customer on the usual basis until further advised by the relevant authority and other relevant enforcement agencies.
--	--

5. Can 4XHub continue providing services if it has formed a suspicion about the customer?

The AML/CTF Act does not direct Labuan KRI to stop providing services to, or terminate a business relationship with, a customer, even if 4XHub has formed a suspicion about that customer. 4XHub determines whether to terminate the relationship with the customer based on its own risk-assessment, procedures, and controls.

The AML/CTF CO, after submitting an SMR, makes an assessment as to whether to continue transact with the customer. If 4XHub decides to continue the business relationship:

- (a) 4XHub must not disclose to the customer that it has formed a suspicion and/or communicated the suspicion to the authority – this is referred to as “tipping off” the customer; and
- (b) 4XHub must continue to comply with the AML/CTF Act in all future dealings with that customer, which may include submitting additional SMRs.

Tipping Off Provisions	4XHub must NOT disclose to any person (other than the relevant authority) that it formed a suspicion about a customer or that it submitted an SMR to the relevant authority. Doing so would constitute 'tipping off', which is an offence prohibited by section 35 of AML/CTF Act.
-------------------------------	--

22. TRANSACTION REPORTING – CASH THRESHOLD REPORTS

22.1 4XHUB does not engage in cash handling and therefore this section is not currently applicable to 4XHUB. However, if 4XHub does engage in cash handling, this section will apply.

22.2 Definitions:

(a) **physical currency** - the coin or printed money of Malaysia or another country which is designated as legal tender;

22.3 Under the AML/CTF Act, if 4XHub provides a service to a customer which involves the transfer of a 'physical currency' of RM25,000 or more (or the foreign currency equivalent), 4XHub must submit a cash threshold report (CTR) to the relevant authority.

22.4 All employees of 4XHub must notify their immediate supervisor of any transactions relating to 'physical currency with a value of RM25,000 or more (or the foreign currency equivalent) immediately.

22.5 The supervisor then reports to 4XHub's AML/CTF CO daily and the AML/CTF CO submits a CTR to the relevant authority.

22.6 The CTR must be in the approved form and sent in accordance with the requirements of the AML/CTF Act and rules. Please see details of the requirement in the table below.

23. REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER

23.1 Where 4XHub has provided or is providing a service to a customer and the AML/CTF CO believes, on reasonable grounds, that a customer has information that may assist 4XHub in the identification, management and mitigation of ML or TF risk, the AML/CTF CO may request the customer to provide them with any such information. The request must be provided in writing and notify the customer that if the request is not complied with, then 4XHub may do any or all of the following until the information covered by the request is provided:

(a) refuse to continue to provide a service;

- (b) refuse to commence to provide a service; or
- (c) restrict or limit the provision of the service to the customer.

23.2 If the customer does not comply with the request within a reasonable time, then the AML/CTF CO may determine that, until the information covered by the request is provided, 4XHub will take any of the actions available to him/her under the AML/CTF Act.

23.3 In these circumstances, the AML/CTF CO determines whether the matter should be reported to the relevant authority as a suspicious matter.

24. ONGOING CUSTOMER DUE DILIGENCE

24.1 4XHub monitors its own customers in accordance with this Section for the purpose of identifying, mitigating, and managing the ML/TF risk that the provision of a service at or through a permanent establishment in Malaysia may involve.

24.2 4XHub complies with the ongoing customer due diligence procedures outlined in the table below. For the avoidance of doubt, the 'Reporting Institution' referred to in the table below refers to 4XHub.

ONGOING CUSTOMER DUE DILIGENCE MANAGEMENT SYSTEM			
Types of customers that the Reporting Institution <u>will</u> provide services to:	(a) Individuals; (b) Companies; (c) Trusts; (d) Trustees and beneficiaries;	Types of customers that the Reporting Institution <u>will not</u> provide services to:	(a) Partnerships; (b) Associations; (c) Registered cooperatives; (d) Government bodies; and (e) Agents.
Review of Customer types:	The Reporting Institution's AML/CTF CO is responsible for reviewing and updating the customer types that the Reporting Institution provides services to on an ongoing basis.		
The Reporting Institution monitors customers by implementing systems to:			
(a) collect further KYC Information for ongoing customer due diligence processes;			

- (b) update and verify KYC Information for ongoing customer due diligence purposes;
- (c) monitor the transactions of customers; and
- (d) conduct enhanced customer due diligence in respect of high-risk customers and customers about whom a suspicion has been formed.

Grouping of customers:

As part of implementing systems for ongoing customer due diligence purposes, the Reporting Institution groups customers according to their level of risk, which has been assessed as part of the risk assessment procedures outlined in this Program. The risk grouping determines:

- (a) what further KYC Information needs to be collected for ongoing customer due diligence purposes in respect of a particular customer;
- (b) what level of transaction monitoring needs to be conducted in relation to a customer; and
- (c) whether the enhanced customer due diligence program needs to be applied.

The AML/CTF CO is responsible for the grouping of customers in accordance with the risk assessment procedures outlined in this Program. The AML/CTF CO reviews the grouping of customers monthly, and the Board conducts spot checks on the grouping of customers on a half-yearly basis.

ADDITIONAL KYC INFORMATION

Risk Assessment for New Activities and Technologies:

In undertaking the risk assessment for new activities and technologies, the AML/CTF CO determines whether any additional KYC Information or Beneficial Owner information should be collected from relevant customers either before any services are provided to the customer or during 4XHub's relationship with the customer. These requirements are incorporated into the relevant customer identification procedures.

Assessment on the level of ML/TF risk involved for different type of customers:

Based on the assessed level of the ML/TF risk involved in the provision of services provided by the Reporting Institution as at the date of this Program, 4XHub has determined that:

- (i) **Low Risk Customers** - no additional KYC Information needs to be collected;
- (ii) **Medium Risk Customers** - the AML/CTF CO determines what additional KYC Information or Beneficial Owner information will be collected as ongoing customer due diligence.

	<p>(iii) High Risk Customers –the AML/CTF CO determine what additional KYC Information or Beneficial Owner information will be collected as ongoing customer due diligence.</p> <p>In relation to collection of additional KYC information, please refer to the relevant customer type under Part B of the Program.</p>
New Customers:	In respect of a new customer, the additional KYC Information is collected at the same time as and in the same manner as the KYC Information is required to be collected under Part B. Failure to provide additional KYC Information is treated in the same way as the failure to provide any other KYC Information collected under Part B.
Existing Customers	In respect of an existing customer or Beneficial Owner, the Reporting Institution updates and re-verifies KYC Information by requesting additional KYC Information where the AML/CTF CO considers the KYC Information is no longer up-to-date, incomplete, or unreliable. The Reporting Institution may also request additional KYC information where the scope of the services provided to an existing customer changes.
When to update and re-verify KYC Information:	<p>The Reporting Institution updates and re-verify KYC Information in respect of a customer where:</p> <p>(a) the customer engages in a significant transaction or series of transactions with one or more reporting entities, where a significant transaction occurs if a transaction, or series of transactions conducted within any calendar month exceeds Ringgit Malaysia Two Hundred Fifty Thousand (RM250,000.00) of digital currency or exceeds Ringgit Malaysia Twenty-Five Thousand (RM25,000.00) physical currency in value; or</p> <p>(b) a significant change occurs:</p> <ul style="list-style-type: none"> (i) in the way the customer conducts transactions; (ii) in the nature of the customer’s business or business relationship; (iii) in the customer’s control structure;

	<ul style="list-style-type: none"> (iv) in the customer’s beneficial ownership; or (v) in the number of transactions carried out by a customer increase by 100% within a five (5) calendar day period. <p>Where one of the above circumstances arises in respect of a customer and the applicable customer identification procedure has not previously been carried out in respect of a customer (i.e. the customer is a pre-commencement customer), the Reporting Institution carries out the applicable customer identification procedure in accordance with Part B and collect the relevant additional KYC Information.</p> <p>Where a change in customer information relates to in the case of:</p> <ul style="list-style-type: none"> (a) individual customers, their: <ul style="list-style-type: none"> (i) name; or (ii) residential address; (b) a company: <ul style="list-style-type: none"> (vi) the company's name; or (vii) the company's registration number; (c) a trust: <ul style="list-style-type: none"> (viii) the trustee; or (ix) the name of the trust; and (d) in the case of a partnership, the identity of a partner; <p>the Reporting Institution will seek to verify the updated KYC Information using reliable and independent documentation in accordance with Part B of this Program.</p>
TRANSACTION MONITORING PROGRAM	
Responsible Persons:	The Board of Directors and the AML/CTF CO have overall responsibility and oversight of the Reporting Institution’s transaction-monitoring program.

	The Reporting Institution conducts transaction monitoring on a weekly basis.
Identification of Risk Factors:	<p>The AML/CTF CO must identify ML/TF risk factors relevant to customers of services and products provided by us. Such risk factors include the:</p> <ul style="list-style-type: none"> (a) value of the transaction exceeds Ringgit Malaysia Twenty-Five Thousand (RM25,000.00) of physical currency and Ringgit Malaysia Two Hundred Fifty Thousand (RM 250,000.00) in value; (b) volume of transactions conducted by a customer within a five (5) calendar day period has increased by more than one hundred per cent (100%); or (c) transaction involves a customer or third party who is a PEP.
Steps to Take After One or More Risk Factors Have Been Identified:	<ul style="list-style-type: none"> (a) An employee must immediately inform the AML/CTF CO when any ML or TF risk factor(s) are identified in relation to a customer or a customer's representative; (b) The AML/CTF CO then liaises with the Board in relation to any further action by the Reporting Institution including, but not limited to the items listed in the “Further Actions to take” section below. (c) Where an employee identifies a customer or third party of a kind specified in item (c) and (d) in “Identification of Risk factors” section above, the AML/CTF CO takes such appropriate action as is necessary, including seeking further information from the customer or their representative or from another source, to determine, with a reasonable degree of certainty, whether the customer or third party is that person.
Further Actions to Take:	<p>If it is determined, because of transaction monitoring, that:</p> <ul style="list-style-type: none"> (a) a customer should be placed in a higher risk grouping, the Reporting Institution will collect additional KYC Information if required with Section 24 of this Program; (b) KYC Information needs to be updated or verified in respect of a customer, 4XHub will update or verify the required information with Section 24 of this Program; (c) a customer is a high-risk customer, 4XHub will apply the enhanced customer due diligence program set out below; or

	(d) a suspicious matter report needs to be lodged in respect of a customer, 4XHub will follow the procedure outlined in Section 21 of this Program.
Training on Identification of Risk Factors:	In addition to the Risk Awareness Training referred to in this Program, the AML/CTF CO ensures that all employees of 4XHub who have direct contact with customers or their representatives, receive regular training in the identification of ML/TF risk factors.
Review and Update of 4XHub's Transaction Monitoring Program:	<p>The AML/CTF CO, in consultation with the Board, must regularly assesses 4XHub's transaction monitoring program and should take steps to have this modified appropriately:</p> <ul style="list-style-type: none"> (a) where there has been a significant change in the ML or TF risk relating to services provided by 4XHub; (b) prior to 4XHub introducing a new service to the market; (c) prior to 4XHub adopting a new method of delivering a service; (d) prior to 4XHub adopting a new technology or developing technology used for the provision of an existing or new service; and (e) where the AML/CTF CO identifies changes arising in the nature of the business relationship, control structure or beneficial ownership of 4XHub's customers.
ENHANCED CUSTOMER DUE DILIGENCE PROGRAM	
Responsible Persons:	The AML/CTF CO has overall responsibility and oversight of 4XHub's enhanced customer due diligence program.
Factors for Conducting Enhanced Customer Due Diligence Program:	<p>The ML/TF risk associated with a particular service, customer, delivery method or jurisdiction is high, including but not limited to when:</p> <ul style="list-style-type: none"> (a) the customer: <ul style="list-style-type: none"> (i) is engaged in business which involves a significant number of cash transactions or amounts of cash; or

	<ul style="list-style-type: none"> (ii) uses a complex business ownership structure for no apparent commercial or other legitimate reason, especially if the Beneficial Owners of the legal entity cannot be determined; or (iii) is based in, or conducts business through or in, a high-risk jurisdiction; or (iv) cannot provide information to verify the source of funds; or (v) requests an undue level of secrecy in relation to a service; or (vi) is a PEP; or <ul style="list-style-type: none"> (b) a service is being provided to a customer who is or who has a Beneficial Owner who is, a foreign politically exposed person; or (c) a suspicion has arisen for the purposes of section 14 of the AML/CTF Act; or (d) 4XHub is entering into or proposing to enter a transaction and a party to the transaction is physically present, or is a company incorporated in, a sanction country.
<p>Steps to Take After One or More Factors Above Have Been Identified:</p>	<p>Where one or more of the factors above arises, the AML/CTF CO arranges for one or more of the following due diligence procedures to occur:</p> <ul style="list-style-type: none"> (a) seek further information from the customer or from third party sources in order to: <ul style="list-style-type: none"> (i) clarify or update the customer’s KYC Information or Beneficial Owner information already collected from the customer, in accordance with ‘Additional KYC Information’ above under this Section. (ii) obtain any further KYC Information or Beneficial Owner information in accordance with ‘Additional KYC Information’ above under this Section, including where appropriate, taking reasonable measures to identify: <ul style="list-style-type: none"> A. the source of the customer’s and each Beneficial Owner’s wealth; and B. the source of the customer’s and each Beneficial Owner’s funds; and (iii) clarify the nature of the customer’s ongoing business with 4XHub Pty Ltd. (b) conduct more detailed analysis in respect of the customer’s KYC Information and Beneficial Owner information taking reasonable measures to identify:

- (i) the source of the customer's and each Beneficial Owner's wealth; and
- (ii) the source of the customer's and each Beneficial Owner's funds;
- (c) verify or re-verify KYC Information or Beneficial Owner information in accordance with the customer identification program outlined in Part B of this Program;
- (d) conduct more detailed analysis and monitoring in respect of the customer's activities and transactions – both past and future, including but not limited to:
 - (i) the purpose, reasons for, or nature of specific transactions;
 - (ii) the expected nature and level of transaction behaviour, including future transactions;
- (e) consider whether a Suspicious Matter Report ought to be lodged;
- (f) seek senior manager approval for:
 - (i) continuing a business relationship with a customer; and
 - (ii) whether a service should continue to be provided to the customer; and
- (g) consider whether a transaction or transactions should be processed.

Issued by the Board of 4XHub Ltd

October 2022