Aliro

Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Program – AML/CTF Policy

March 2026

AML/CTF Policy

Contents

Revision Header

This policy is to be reviewed and approved on an annual basis by the Board of Directors. In particular, Aliro's services and their designation (under section 6 of the Act) are required to be annually reviewed.

Revision No.	Revision Date	Revision Comments	Prepared By:	Approved By:
1	August 2018	Initial Version	Compliance Officer	Board
2	October 2020	Periodic review	Compliance Officer	Board
3	June 2021	Periodic review	Compliance Officer	Board
4	January 2023	Periodic review	Compliance Officer	Board
5	October 2024	Independent Review conducted by OneAML. Recommendations incorporated into AML Program	Compliance Officer	Board
6	March 2026	Update with legislative changes	Compliance Officer	Board

1. AML/CTF Program

This Anti-Money Laundering/Counter-Terrorism Financing (AML/CTF) Program outlines the policies and procedures in place to allow for Aliro Group Limited ("Aliro"), as the lead entity of the Aliro Reporting Group ("Aliro Group" or "us"), to support Aliro in meeting its obligations under the AML/CTF Act 2006 and the AML/CTF Amendment Act 2024 (together the "Act") and the AML/CTF Rules 2025 (the "Rules").

The documents forming the overall AML/CTF Program include:

- This AML/CTF Policy
- Reporting Group ML/TF/PF Risk Assessment
- Customer Verification Procedures

2. Version Control

Version number	Date of change	Summary of changes	Date of Approval	Name of Approvers
1.0	31 March 2026	Initial AML/CTF Program implementation due to AML/CTF reforms	TBC	

3. Money Laundering, Terrorism Financing and Proliferation Financing (ML/TF/PF)

Money Laundering

Money laundering is the process by which persons engaged in criminal activities attempt to conceal the true origin and ownership of the proceeds of their activities. If money laundering is successful, those proceeds can lose their apparent criminal identity and appear legitimate.

When criminal activity generates substantial profits, the individual or group involved must find a way to control the funds without attracting attention to the underlying source of those funds. Criminals do this by disguising the sources of funds they control, typically by converting such funds into other assets forms in the legitimate financial system.

In summary, the money launderer seeks to:

- place money into the legitimate financial system or retail economy, without arousing suspicion (a stage often referred to as 'placement')
- move the money around, often in a series of transactions so it becomes more difficult to identify its original source (a stage referred to as 'layering')
- reintroduce the money into the legitimate economy as if derived from an apparently clean source (a stage referred to as 'integration')

Businesses such as ours can be knowingly or unwittingly co-opted into facilitating money laundering at any one or more of these stages. For this reason, the law requires we have processes to either frustrate money laundering activity or failing that at the very least track and record the verified identity of the Customers of our Designated Services so that law enforcement agencies can later access that information.

Some examples of how Aliro Group can facilitate Money Laundering include:

- Investment of funds from investors derived from illegal activities (referred to as 'proceeds of crime') in Aliro Group's Managed Investment Schemes in order to legitimise the funds.
- Investment of proceeds of crime by criminal organisations in Aliro Group's Managed Investment Scheme by using false identity documents or through a third party such as a relative or an unwitting participant recruited by the criminal organisation as a 'money mule'.

By having procedures to more effectively identify the Customers of our Designated Services, and a Program to manage and mitigate ML risk, we provide both a deterrent to persons considering the misuse of our services but also generate records that provide an audit trail that may be relied upon by law enforcement agencies entitled to access the information.

Terrorism Financing

The United Nations 1999 International Convention for the Suppression of the Financing of Terrorism explains terrorist financing as an offence whereby a person:

> '....by any means, directly or indirectly, unlawfully and willingly, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
>
> (a) an act which constitutes an offence within the scope of and as defined in one of the treaties listed in the annex to the Convention; or
>
> (b) any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking any active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing an act.'

Whilst engaging in terrorism financing activity is of itself an offence, the Act is also concerned to ensure that legitimate businesses are not knowingly or unwittingly used in facilitating the commission of such offences. For this reason, we are required to maintain processes designed to identify and report suspected terrorism financing activity or, at the very least, track and record the verified identity of the Customers of our Designated Services so that law enforcement agencies may later be able to later access that information.

Some examples of how Terrorism Financing can occur include:

- financial support – in the form of donations, community solicitation and other fundraising initiatives (e.g. donations raised by charities and non-profit organisations); or
- revenue generating activities – income may be derived from criminal activities but also from legitimate economic activities such as real estate and securities investments or generated via normal business activity.

Proliferation Financing

Proliferation Financing is defined by the Department of Foreign Affairs and Trade ("DFAT") as the act of providing funds or financial services for the manufacture, acquisition, possession, development, or transport of nuclear, radiological, chemical, or biological weapons ("Weapons of Mass Destruction" or "WMD") and their means of delivery, in violation of national or international laws.

Proliferation Financing occurs when a person:

a) makes available an asset; or
b) provides a financial service; or
c) conducts a financial transaction; and

the person knows that, or is reckless as to whether, the asset, financial service or financial transaction is intended to, in whole or in part, facilitate the proliferation of WMDs, regardless of whether the activity occurs or is attempted.

When acting on directions from customers to disburse funds in accordance with instructions received we need to be aware of circumstances where those funds may be intended for TF/PF activities or are paid in a manner in which it may later be difficult to trace the ultimate destination of those funds. By limiting the manner in which we are permitted to disburse funds and ensuring that the immediate destination of payments by us are therefore more readily traceable we will be able to better manage and mitigate the risk of misuse of our services to facilitate TF/PF activity.

4. Reporting Group

A reporting group is a group of persons that includes one or more reporting entities. Reporting groups have a lead entity and ordinary members (members). These reporting groups allow groups of reporting entities to share and centralise AML/CTF functions, including to:

- share resources
- reduce costs
- identify, assess, manage and mitigate money laundering, terrorism financing and proliferation financing risks (ML/TF/PF risks) more effectively.

Reporting groups can also include businesses that are not reporting entities, such as where a control relationship exists (i.e. parent/subsidiary arrangements, trust-managed structures, vertically integrated structures). These businesses are not subject to AML/CTF obligations or AUSTRAC supervision. They can assist reporting entities in the group by carrying out AML/CTF obligations on their behalf.

Aliro Group Limited (**Aliro**) has been appointed as the lead entity of the Aliro Group and is the central point of accountability for the Aliro Group's AML/CTF compliance. Aliro has obtained the relevant consents from the other relevant members of the Aliro Reporting Group to be a lead entity. Should Aliro cease to have the consent of the relevant members, a new lead entity will be appointed within 28 days and notified to AUSTRAC. The AML/CTF

Compliance Officer and Senior Manager for Aliro are also appointed to each of the reporting entities forming the Aliro Group (where there is more than one Reporting Entity). Reporting entities within the Aliro Group must, where relevant, appropriately share information with other members of the Aliro Group for the following purposes:

i) carrying out Customer Due Diligence (CDD);
ii) appropriately identifying, assessing, managing and mitigating ML/TF/PF risks that such Reporting entities may reasonably face in providing their designated services; and
iii) to comply with their obligations imposed by the Act, regulations and Rules and this Policy.

Any information shared between members of the Aliro Reporting Group for the purposes of this Policy must be kept confidential and used appropriately, including to prevent any tipping off contravention (see Section 13 below).

The following Aliro Group entities reporting entities:

Entity	**Reporting Entity (Y/N)**
Aliro Group Limited	Y (Lead Entity)
Aliro Trusco 1 Pty Ltd	Y
Aliro Trusco 2 Pty Ltd	Y

The following Aliro Group entities do not provide designated services (not reporting entities):

Entity	**Reporting Entity (Y/N)**
Aliro Management Pty Ltd	N
Valoro Group Pty Ltd	N

The AML/CTF Program applies to all reporting entities noted in the Aliro Group above.

5. Governance

Governing Body

The governing body is the person or group primarily responsible for the governance and executive decisions of the business. The Board of Directors (the "Board") of ALIRO has been assigned as the governing body of the Aliro Group reporting group.

The Board will maintain oversight of AML/CTF compliance and take reasonable steps to ensure compliance by the Aliro Group reporting group. This includes:

- Appointing an eligible AML/CTF compliance officer to the business
- Ensuring senior manager roles with AML/CTF responsibilities are appropriately staffed
- Overseeing Aliro Group's compliance with:
    - AML/CTF policies,
    - the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 and the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024 (the Act),
    - the Anti-Money Laundering and Counter-Terrorism Financing Rules 2025 (the Rules), and
    - regulations (AML/CTF obligations).
- Taking reasonable steps to ensure that Aliro Group is:
    - appropriately identifying, assessing, managing and mitigating its ML/TF/PF risk
    - Complying with its AML/CTF policies
    - Complying with its AML/CTF obligations
- Questioning and reviewing matters included in compliance reports, where appropriate
- Taking reasonable steps to address non-compliance and any failure to identify and assess risks.

Taking reasonable steps includes ensuring that Aliro Group:

- has appropriate assurance and monitoring processes built into the program
- puts in place independent reviews of AML/CTF capabilities and compliance at appropriate intervals
- adopts a strong AML/CTF culture
- engages, resources and empowers appropriate people to meet its obligations
- escalates compliance issues appropriately to its governing body, particularly when changes to resourcing or wider business practices are required

The Board will receive reports from the AML/CTF Compliance Officer at least quarterly, and in any case at least once every 12 months about:

- compliance with Aliro Group's AML/CTF policies and obligations;
- the extent to which Aliro Group's AML/CTF policies are appropriately managing and mitigating ML/TF/PF risks that it may reasonably face in providing its designated services; and
- Aliro Group's compliance with the AML/CTF Act, regulations and Rules.

The Compliance Officer and Senior Manager must submit a compliance report (AML CTF Compliance Report) to the Board quarterly outlining the following at a minimum:

- Ongoing compliance with AML/CTF laws;
    - Monitoring regulatory developments with AML/CTF laws;
    - Ongoing compliance with the Aliro Group's AML/CTF Program;
- Any notifications made to AUSTRAC;
- Exceptions and incidents arising from customer due diligence activities or monitoring arrangements;
- Amendments to any aspect of the AML/CTF Program that have been approved or undergoing review
- Updates and outcomes of periodic review AML/CTF risk assessments;
- PEP approvals and findings (if any) of any material risks;
- Non-standard account approvals, rejections and summary metrics;
- Any recommendations for review of the AML/CTF Program; and
- Any other information required by the Board to enable it to fulfill its responsibilities under the AML/CTF Act.

These reports will be tabled as part of the Risk & Compliance update in the Board report for the relevant period.

The Board must also receive written notification of any updates to the risk assessment as soon as practicable after the update is made.

AML/CTF Compliance Officer

The AML/CTF Compliance Officer is responsible for communicating with AUSTRAC on Aliro Group's behalf. They will oversee and coordinate Aliro Group's day-to-day compliance with the Act, the Rules and Aliro Group's AML/CTF obligations.

The AML/CTF compliance officer's responsibility includes:

- overseeing and coordinating Aliro Group's day-to-day compliance with the Act, Rules and regulations
- giving reports to the Board at least once every 12 months on AML/CTF compliance

The AML/CTF Compliance Officer must meet eligibility requirements, including being:

- engaged at management level (employee or external appointee), with appropriate authority, independence, resources and expertise
- a resident of Australia if designated services are being provided at or through a permanent establishment in Australia
- a fit and proper person, including consideration of whether they:
    - have the competence, skills, knowledge, diligence, expertise and soundness of judgement to properly perform the role

- have the attributes of good character, honesty and integrity
- have been convicted of a serious offence
- are the subject of adverse findings by a regulatory body
- have been found to have engaged in serious misconduct by a regulatory body
- are bankrupt or have signed a personal insolvency agreement
- have a conflict of interest that creates a material risk they won't act properly in the role such as interests with an AML/CTF software company that may impact what vendor solution they select to complete transaction monitoring or screening or acting as the AML/CTF compliance officer of multiple other businesses which may affect their ability to act impartially.

Changes to the AML/CTF compliance officer must be notified to AUSTRAC within 14 days of the change. This will be notified by the Risk & Compliance team.

Delon Wainer (Head of Group Finance) has been appointed to the role of Aliro Group AML/CTF Compliance Officer.

Senior Manager

A senior manager, or multiple senior managers, must be appointed to make key AML/CTF decisions including approving AML/CTF programs, updates to these programs and certain business relationships.

A senior manager is an individual who makes, or is involved in making, decisions affecting all or a substantial part of the business, particularly their ability to make or influence strategic or operational decisions about how the business is conducted.

The Board is responsible for approving the appointment of a Senior Manager(s). Appointments will be documented through formal Board minutes or resolutions.

The Senior Manager is responsible for:

- approving Aliro Group's risk assessment
- approving the implementation of the AML/CTF Program
- implementing updates to Aliro Group risk assessments and the AML/CTF program
- approving certain business relationships before they're entered into.
- approving the entering into any written agreement or arrangement with a third party that will collect and verify CDD information for Aliro Group.
- approving designated services provided to foreign politically exposed persons (PEP), high-risk customers that are also a domestic PEP, and high-risk customers that are also an international organisation PEP (including where a customer is receiving the service on behalf of a person identified as one of these PEPs).

Approval required by the Senior Manager will be documented through electronic communication (i.e. emails), and retained for record keeping requirements.

Records of approvals (including dates of approval) relating to the AML/CTF Policy, Customer Verification Procedures and the Risk Assessments will also be documented in each document.

Sean Southon (COO) has been appointed to the role of Aliro Group Senior Manager.

6. Periodic Review Requirements

This Program must be reviewed by the [Compliance Officer/Senior Manager], and if required, updated in any of the following circumstances as soon as practicable:

- following a review of Aliro Group's ML/TF/PF risk assessment
- following an independent evaluation report that contains adverse findings in relation to Aliro Group's AML/CTF policies

- following AUSTRAC release of relevant risk information or regulatory guidance, including typologies and case studies that may impact Aliro Group's risk assessments.

In any event, this Program must be reviewed at least once every 3 years at a minimum.

Changes to the ML/TF/PF risk assessments should be updated in this AML/CTF Program within 14 days of the changes. This should be documented in writing, along with the date the changes were made. Any changes to this AML/CTF Program must be approved by a Senior Manager and then notified to the Board.

7. AUSTRAC Guidance

Where feedback has been received from AUSTRAC regarding Aliro Group's AML/CTF Program, the AML/CTF Compliance Officer must ensure they:

- consider any guidance material released by AUSTRAC, including anything circulated or published about the industries in which Aliro Group operates in and the risks associated with those industries.
- amend the Program to take into account any deficiencies identified in feedback provided by AUSTRAC
- develop a plan (with appropriate training) for implementation of the amendments incorporating the AUSTRAC feedback of the Program
- manage the conduct of the developed plan.

The process of escalating AUSTRAC feedback should be undertaken as follows:

1. **Initial Review:** AUSTRAC feedback is reviewed and assessed by the AML/CTF Compliance Officer to understand the nature of the feedback and determine if action is required.
2. **Documentation:** The communication received regarding the feedback will be logged in the Aliro Group Regulatory Correspondence Register, which is reported to the Board of Directors on a quarterly basis.
3. **Internal Discussion:** Feedback is discussed with the relevant Aliro Group teams for impact assessment and to determine the appropriate course of action. Where implementation of processes may be required, a project team will be assigned to oversee implementation (i.e. where deficiencies are identified by AUSTRAC).
4. **Formal Submission:** Where required, a formal response is prepared and reviewed by the AML/CTF Compliance Officer relating to the feedback. Legal Counsel will be consulted where appropriate or required.
5. **Follow-Up:** Further AUSTRAC correspondence will be monitored for any other actions.

8. Independent Evaluation Requirements

An independent evaluation of this AML/CTF Program must be completed at least once every 3 years consisting of the following:

- evaluation of how Aliro Group undertakes or reviews its ML/TF/PF risk assessment against the requirements the Act, the regulations and the Rules.
- evaluation of the design of Aliro Group's AML/CTF policies against the requirements of the Act, the regulations and the Rules
- test and evaluation of whether Aliro Group appropriately identified, assessed, mitigated and managed its money laundering, terrorism financing and proliferation financing risks (ML/TF/PF risks) and complied with its AML/CTF policies.

An evaluator must be assessed independent and suitable prior to being engaged to conduct an independent evaluation. Independence refers to the evaluator's ability to conduct evaluations without bias, influence or conflicts of interest. Suitable refers to the evaluator's knowledge of the AML/CTF obligations and compliance requirements, Aliro Group's business, and their experience in evaluating AML frameworks.

An evaluator can be internal (eg. A member of an internal audit team) or external to Aliro Group (eg. An external consultant). If an evaluator is internal, they must not have been involved in any of Aliro Group's AML processes

including the development and implementation of the AML/CTF program and be able to exercise independent judgement.

On conclusion of an independent evaluation, a written report must be produced and provided to the Board of Directors and the Senior Manager(s) responsible for approving the AML/CTF Program. The report should include:

1. A summary of the evaluation process, including the aspects of the business reviewed and the evaluation method used;
2. Their findings in relation to how the business undertook or reviewed its ML/TF/PF risk assessment and the design of its AML/CTF policies;
3. Their findings about whether the business is complying with its AML/CTF policies; and
4. What they tested, the files they sampled, and how they conducted the tests or sampling.

Where an independent evaluation report contains adverse findings, records should be maintained on how Aliro Group has addressed the findings, including the reasons why certain updates have not been made in response to any adverse finding.

9. Designated Services Provided

A designated service is a service that is listed in section 6 of the Act (because it has been identified as posing a risk for money laundering and terrorism financing) and which meets the geographical link.

To be a designated service regulated under Australia's AML/CTF Act, the service must have a 'geographical link' to Australia (as well as being listed in section 6 of the Act). A service has a 'geographical link' to Australia if any of the following conditions apply:

(a) the service is provided to the customer at or through a permanent establishment of the entity in Australia;
(b) the entity is a resident of Australia and the service is provided at or through a permanent establishment of the entity in a foreign country (foreign branch); or
(c) the entity is a subsidiary of a company that is a resident of Australia and the service is provided at or through a permanent establishment of the entity in a foreign country (foreign subsidiary).

Aliro Group currently provides the following designated services under section 6 of the AML/CTF Act:

Item (under the Act)	**Designated Service (under the Act)**	**Customer (under the Act)**	**Aliro Group Example**
Table 1 Item 35	issuing or selling a security or derivative to a person, where: (a) the issue or sale is in the course of carrying on a business of issuing or selling securities or derivatives; and (b) in the case of an issue of a security or derivative—the issue does not consist of the issue by a company of either of the following: i) a security of the company (other than an interest in a managed investment scheme); or ii) an option to acquire a security of the company (other than an option to acquire an interest in a managed investment scheme); and	The person (i.e. the person)	Issue of units in a managed investment scheme operated by Aliro Group

	(c) in the case of an issue of a security or derivative—the issue does not consist of the issue by a government body of a security of the government body or of an option to acquire a security of the government body; and (d) in the case of an issue of a security or derivative—the issue is not an exempt financial market operator issue; and (e) such other conditions (if any) as are set out in the AML/CTF Rules are satisfied		
Table 1 Item 46	providing a custodial or depository service, where: (a) the service is provided in the course of carrying on a business of providing custodial or depository services; and (b) the service is not an exempt legal practitioner service.	The client of the service	Providing custodial services in relation to managed investment schemes

10. ML/TF/PF Risk Assessment

ML/TF/PF risk refers to the potential that a person could exploit a business's vulnerabilities to enable:

- money laundering, which makes money gained from illegal activities appear legitimate
- terrorism financing, which funds terrorist activity
- proliferation financing, which enables the spread of weapons of mass destruction.

Exploitation happens when criminals successfully target a business to:

- hide money or property to disguise its illicit origins and avoid being caught by law enforcement
- use money or property to engage in more crime.

Aliro Group's Program aligns with Aliro's Risk Framework to identify, mitigate and manage such risks. The Risk Management Framework is reviewed and updated on a periodic basis, reflecting changes to the risk environment. Money-Laundering and Terrorism Financing Risk is captured as a separate Enterprise item on the Aliro Group Risk Register.

Risk Assessment Methodology

The following impact and likelihood matrices have been used in conducting Aliro Group's risk assessments:

Impact ratings	**Impact of an ML/TF/PF risk occurrence**
Major	Significant impact – major damage or effect. Serious terrorism or extensive money laundering.
Moderate	Moderate level of money laundering or terrorism financing impact.
Low	Minor or negligible consequences or effects.

Likelihood ratings	**Impact of an ML/TF/PF risk occurrence**
Very likely	Almost certain to occur or will occur at a high frequency or probability. This might mean it's a known or recurring issue.
Likely	High probability it will occur, but not certain.
Unlikely	Unlikely to occur

Inherent risk rating based on impact and likelihood:

	Low Impact	**Moderate Impact**	**Major Impact**
Unlikely	Medium	High	High
Likely	Low	Medium	High
Very Likely	Low	Low	Medium

Risk response table based on inherent risk rating:

Inherent risk rating	**Risk description**
High	The risk represents a high inherent ML/TF/PF risk. We need to appropriately mitigate with our policies as a priority.
Medium	The risk represents a medium inherent ML/TF/PF risk. We need to appropriately mitigate and/or manage with our policies.
Low	The risk represents a low inherent ML/TF/PF risk. We need to appropriately manage with our policies.

ML/TF/PF Risk

A risk assessment must identify and assess the ML/TF/PF risks a business may reasonably face. This must cover both:

- the provision of designated services
- the plan to provide designated services.

Aliro Group has considered the ML/TF/PF risks that may arise from:

- The type of customers that designated services are provided to.
- The types of products and services being provided.
- How the designated services are provided to customers.
- Jurisdictions that clients may originate from.

Aliro Group has also assessed any planned designated services, customers, delivery channels or countries that could increase ML/TF/PF risk.

A risk assessment has been conducted for Aliro that identifies, assesses and evaluates its exposure to the ML/TF/PF risks, having regard to the designated services it provides and the risk mitigation measures in place. Aliro Group's Senior Manager has assessed Aliro as the only Reporting Entity of Aliro Group, providing all designated services offered by the members of the Aliro Group.

The AML/CTF Compliance Officer and Senior Manager will review Aliro's ML/TF/PF risk assessment at least every 3 years to identify and assess any new or changed ML/TF/PF risks that it may reasonably face in providing its designated services in the following circumstances and in the following timeframes:

Circumstance	**Timeframe**
There is a significant change to: a. The type of customers that designated services are provided to. b. The types of products and services being provided. c. How the designated services are provided to customers. d. Jurisdictions that clients may originate from.	• For a Significant Change that is within the control of the reporting entity—before the significant change occurs; or • For a Significant Change that is not within the control of the reporting entity—as soon as practicable after the significant change occurs;
AUSTRAC communicates to Aliro information that identifies or assesses risks associated with the reporting entity's provision of its designated services.	As soon as practicable after the information is communicated to Aliro.
Circumstances specified in the Rules (where applicable).	At the time, or within the period, specified in the Rules.

The ML/TF/PF risk assessment must be updated to incorporate and address any issues identified in the review. Where the update involves consideration of a significant change that is within the control of the Company, such update must be made before the significant change occurs or in other cases, as soon as practicable after the review is completed. The Senior Manager/Compliance Officer will document each review of the ML/TF/PF risk assessment. The ML/TF/PF risk assessment must be approved by the Senior Manager and submitted to the Board at its next quarterly meeting.

A summary of each risk category is as follows:

Customer Type	Customer Type risk is the level of money laundering, terrorism financing and proliferation financing (ML/TF/PF) risk that arises from the nature and characteristics of a customer (and its beneficial owners/controlling persons). It reflects how likely and how significantly a particular type of customer could use the Reporting Entity's services to facilitate ML/TF/PF.

Designated Services	Designated services risk is the level of ML/TF/PF risk that is inherent in the types of designated services a Reporting Entity offers, having regard to their features (e.g. speed, liquidity, anonymity, cross-border nature, ability to layer or integrate funds) and any associated technologies.
Delivery Methods	Delivery channel risk is the level of ML/TF/PF risk associated with the way designated services are delivered – for example face-to-face, non-face-to-face online, through intermediaries, agents or outsourcing arrangements – including the use of new or emerging technologies.
Jurisdiction	Jurisdiction (country) risk is the level of ML/TF/PF risk that arises from the countries connected to a customer, transaction or service – for example where the customer is located, where funds come from or go to, where counterparties are based, or where assets are held.

Refer to **Enterprise Risk Assessment** for the completed risk assessments.

11. Customer Due Diligence (CDD)

Customer Risk Ratings

Risk ratings must be assigned to all customers **prior** to the provision of designated services and monitored on an ongoing basis. These are based on Know Your Customer (KYC) information reasonably available to Aliro Group during initial CDD, and all ML/TF/PF risk factors present for that customer that identified during ongoing CDD.

When assigning a customer risk rating for CDD, we must use the information and factors in our ML/TF/PF risk assessment and consider how these apply to the individual customer. This includes all of the following:

- the kind of customer (eg. Individuals, companies, trusts, partnerships)
- what kind of designated services we are providing to the customer (as per Section 7)
- the delivery channels we will use to provide designated services to the customer (eg. online, in-person)
- what countries we will provide our designated services in or through

Risk factors in these categories impacting the customer risk should be identified, with each factor assigned with a rating. In determining a risk rating, the likelihood and impacts of these factors relating to the customer should be considered.

The presence of particular risk factors, and the customer's overall risk rating, will then determine:

1. Any subsequent KYC information to be collected and/or verified for initial CDD; and
2. The monitoring process for ongoing CDD.

Low Risk

Low Risk customers are those for whom, based on information obtained at onboarding, the risk of money laundering, terrorism financing or proliferation financing is considered limited and consistent with normal retail or vanilla wholesale activity, and where no specific higher-risk indicators are present. Standard CDD measures are sufficient and enhanced CDD is not required.

Some factors in determining whether a customer is Low Risk may include (but not limited to):

Customer Type	Natural person(s) in their own name, with clear, straightforward profile (e.g., salaried employees, retirees). Simple proprietary limited company or family trust with transparent ownership and control and no complex structures.

	Ultimate beneficial owners (UBOs) are easily identified, verified and not acting through multiple layers or opaque jurisdictions. No PEPs, no sanctioned parties, no adverse media of concern.
Products & services	Use of standard, plain-vanilla investment products, consistent with stated objectives and profile. No cash-intensive activity and no unusual or complex transaction patterns anticipated at onboarding.
Geography	Customer and beneficial owners resident in, and funds expected to flow to/from, low-risk or FATF-compliant jurisdictions, with no sanctioned or high-risk country connection.
Delivery channel	Relationship established face-to-face or via a controlled, vetted intermediary (e.g. known AFSL licensee / platform) with full CDD documentation obtained.

Medium Risk

Medium Risk customers are those where one or more factors indicate an elevated but manageable level of ML/TF/PF risk, but where there are no red-flag high-risk indicators such as PEP status, sanctions exposure, highly complex structures or high-risk jurisdictions. Standard CDD is applied, together with targeted additional enquiries where appropriate; ECDD is typically not mandatory unless specific high-risk triggers are present.

Some factors in determining whether a customer is Medium Risk may include (but not limited to):

Customer Type	Private companies, unit trusts, or partnerships with more than one layer of ownership but still ultimately transparent after enquiry. Professional or commercial customers operating in moderately higher-risk industries (e.g. some types of trading businesses, higher cash turnover, but not inherently high-risk sectors like casinos, MSBs, etc.). UBOs identified and verified, but with a minority foreign ownership in generally medium-high risk countries. Low-level adverse media that can be reasonably explained and mitigated.
Products & services	Use of more flexible or higher-value products (e.g. bespoke mandates, leverage, ability to move funds between products) consistent with client profile. Anticipated transaction volumes higher than typical retail, but in line with business activities.
Geography	Some limited exposure to medium-risk jurisdictions (e.g. cross-border investors in otherwise vanilla structures), but: - no direct link to sanctioned countries, and - no predominant nexus with FATF-identified high-risk or non-cooperative jurisdictions.
Delivery channel	Introduced by external intermediaries that are regulated but not part of your group, or relationship established using non face-to-face methods with robust electronic verification and controls.

High Risk

High Risk customers are those where initial CDD identifies significant ML/TF/PF risk indicators, including but not limited to complex or opaque structures, high-risk jurisdictions, PEP status, sanctions / proliferation-related exposure, or activity inconsistent with the customer's stated profile. Such customers require enhanced customer due diligence (ECDD) and closer ongoing monitoring, and may be declined where risk cannot be mitigated to an acceptable level.

Business relationships with High Risk customers must be reviewed and approved by the Senior Manager.

Some factors in determining whether a customer is High Risk may include (but not limited to):

Customer Type	Entities operating in inherently high-risk sectors, e.g.: - money or value transfer, unregulated FX/remittance, - gambling / gaming,

	- cash-intensive businesses with weak transparency, - certain high-risk crypto / virtual asset related activity. Trusts or corporate structures with multiple layers, nominee arrangements or unexplained dependency on professional "fronts". Difficulty identifying or verifying UBOs; indications of beneficial ownership obfuscation. Customer or UBO is: - a Politically Exposed Person (PEP) or close associate / family member of a PEP, or linked to adverse media concerning financial crime, corruption, terrorism, proliferation or significant regulatory breaches.
Products & services	Anticipated large or unusual transaction volumes or patterns, not obviously consistent with the stated source of wealth and purpose of the relationship. Expected use of complex or layered transactions, frequent cross-border movements, or structures that make tracing beneficial ownership/funds unduly difficult.
Geography	Customer, UBO, key controller or primary source/destination of funds is linked to: - sanctioned countries, high-risk or non-cooperative jurisdictions, or - countries of proliferation concern (e.g. WMD-related sanctions exposure).
Delivery channel	Non face-to-face onboarding without robust, independent verification. Use of unregulated or lightly-regulated introducers or intermediaries where reliance cannot be placed on their CDD.

Initial CDD

Risk ratings will be assigned to a customer on initial CDD prior to the provision of a designated service by establishing the following matters on reasonable grounds:

- the identity of the customer and any person on whose behalf the customer is receiving a designated service (such as a beneficiary of a trust or foreign equivalent)
- the identity of any person acting on behalf of the customer, and their authority to act
- if the customer isn't an individual, the identity of any beneficial owners or controllers of the customer (i.e. individuals holding either directly or indirectly, more than 25% of the interests of the customer)
- whether the customer, any beneficial owners of the customer, any person on whose behalf the customer is receiving the designated service or any person acting on behalf of the customer is a politically exposed person (PEP), or designated for targeted financial sanctions
- the nature and purpose of the business relationship or occasional transaction
- the source of funds and source of wealth of foreign PEPs, high-risk domestic or international organisation PEPs
- if required to apply enhanced CDD, the customer's source of funds and source of wealth, if this is relevant to the nature of the customer's ML/TF/PF risk.

"Reasonable grounds" is an objective standard: Aliro Group must be able to explain how the conclusion was reached based on the information available at the time, such that a reasonable person with similar knowledge/training would likely reach the same view.

To establish these matters, Aliro Group must:

a) take reasonable steps to establish that the customer is who they claim to be
b) identify the customer's ML/TF/PF risk
c) collect know your customer (KYC) information that's appropriate to the customer's ML/TF/PF risk
d) verify KYC information, using reliable and independent data, that's appropriate to the customer's ML/TF/PF risk.

Establishing the required matters on reasonable grounds should consist of the following steps:

1. Collect KYC information from the customer, through the use of an onboarding form.
2. Identify the customer's ML/TF/PF risk based on the KYC information collected.
3. Determine if the customer is a PEP or designated for targeted financial sanctions.
4. Determine if enhanced CDD is required.
5. Determine if simplified CDD or deemed compliance provisions can be applied.
6. Collect additional KYC information as appropriate to the customer's ML/TF/PF risk, and to mitigate and manage that ML/TF/PF risk.
7. Verify KYC information using reliable and independent data, that is appropriate to the customer's ML/TF/PF risk.

Document Collection and Verification Process

When conducting CDD, we must ensure that we collect the following:

- the minimum KYC information that for the type of customer we are dealing with
- more KYC information about:
    - a customer who is high ML/TF/PF risk than we would for a customer who is low ML/TF/PF risk
    - persons associated with a high-risk customer (such as a beneficial owner) than we would of a low-risk customer
    - a customer whose request for a designated service seems unusual. For example, KYC information about their occupation, income, countries of citizenship.

Collecting KYC information involves **gathering** information. This is done using a customer onboarding form. Information may also be gathered from other sources and does not have to be collected directly from the customer. No identification documentation is necessarily required to be gathered at this collection stage, but this is the best way to gather the relevant information.

Verifying KYC information involves **checking** reliable, independent source documentation, data or information that confirms the accuracy and truth of the KYC information that was obtained during the collection process.

Collection and verification of identification information can happen in parallel. For example, we may sight an individual's identity document and record relevant information instead of requiring them to input their details into an onboarding form.

Refer to the **Customer Verification Procedures** for specific customer identification procedures for:

- Individuals
- Sole Traders
- Body corporate, partnership or unincorporated association
- Trusts
- Government Bodies

Delayed initial CDD

We may be able to start providing a designated service to a customer before the initial CDD is completed if the designated service is any of the following (applicable to Aliro Group):

1. Provided at or through a permanent establishment in Australia

   Verification of some KYC information may be delayed where the designated service is provided at/through an Australian permanent establishment. If CDD is delayed, Aliro Group must complete verification before we:

   - transfer, or allow or facilitate the transfer of money, property or virtual assets for or on behalf of the customer

- otherwise make money, property or virtual assets available to the customer (other than holding it in an account or on deposit from the customer).

Initial CDD must be completed as soon as reasonably practicable and within 20 business days of starting to provide the customer with the designated service.

This also means that we can start providing a designated service **after we've collected, but before we verify**, the KYC information about the customer, including:

- the identity of persons acting on behalf of, or receiving the service on behalf of, the customer
- the identity of beneficial owners
- the status of politically exposed person (PEP) / targeted financial sanctions (TFS) (for customer and relevant parties)
  the nature/purpose of the relationship/transaction (where ECDD applies).

Before commencing a service with delayed CDD on this basis, Aliro Group must:

- if the customer is an individual – take reasonable steps to establish that the customer is the person the customer claims to be;
- identify the ML/TF/PF risk of the customer, based on KYC information about the customer that is reasonably available to Aliro Group before commencing to provide the designated service (such as through public domains including media outlets and regulatory databases);
- collect KYC information about the customer that is appropriate to the ML/TF/PF risk of the customer; and
- establish on reasonable grounds the identity of the customer and the identity of any person acting on behalf of the customer and their authority to act.

2. <u>a certain financial market transaction that must be performed rapidly</u>

Aliro Group may commence before completing initial CDD where all of the following apply:

- the designated service is acquiring or disposing of a security, derivative or foreign exchange contract on a declared financial market (within the meaning of the Corporations Act 2001)
- the designated service is provided at or through a permanent establishment in Australia
- this must occur quickly because of financial market conditions relevant to the transaction.

The service must not involve the acquisition of an interest in a managed investment scheme to which section 1019B of the Corporations Act 2001 applies.

While CDD is delayed, Aliro Group must not:

- accept physical currency or virtual assets to fund the service
- allow the customer to transfer/part with disposal proceeds
- resell/transfer/part with acquired assets on the customer's behalf
- allow recrediting or refunds of the purchase price.

Initial CDD must be completed as soon as reasonably practicable and within 5 business days of starting to provide the customer with the designated service.

Before commencing a service with delayed CDD, Aliro Group must form **reasonable grounds** that:

a) delaying CDD is essential to avoid interrupting the ordinary course of business;
   - Examples of when it may be essential to delay initial CDD to avoid an interruption to the ordinary course of business may include:
     - for customers in an emergency, such as family and domestic violence or natural disasters who don't have access to identity documents
     - Where a large time-sensitive transaction involving multiple customers may be delayed due to the initial CDD delay

b) the delay creates low additional ML/TF/PF risk, and Aliro Group is likely to be able to obtain the required CDD information.

"Reasonably practicable" is assessed objectively on the circumstances, and Aliro Group must be able to evidence the steps taken to complete CDD at the earliest possible time.

Requests to delay initial CDD must be approved by a Senior Manager, along with supporting documentation and rationale for the request. In any case, initial CDD must be completed as soon as reasonably practicable and within 20 business days of starting to provide the customer with the designated service.

If a delayed CDD results in a customer being assessed as outside of Aliro Group's risk appetite or has been unable to fully verify their identity to Aliro Group's satisfaction, we will take appropriate action to minimise ML/TF/PF risk, including (but not limited to):

- returning funds directly to the customer
- preventing any more designated services from being provided to the customer
- reversal of units issued to the customer (depending on Constitution discretion/powers)

Identifying individuals who do not have standard identification

Some individuals may be unable to provide standard identification due to barriers accessing or obtaining documents, circumstances outside their control, or inconsistencies across documents (e.g., name or date of birth). This may occur, for example, where an individual is Aboriginal and Torres Strait Islander, affected by a natural disaster or family and domestic violence, a refugee/asylum seeker/recent migrant, from a culturally and linguistically diverse background, living remotely, an older Australian, in hospital long-term, not registered at birth, or experiencing digital exclusion/inaccessibility.

Where Aliro Group needs to establish identity for initial CDD and standard identification cannot be provided or validated, Aliro Group may use alternative identification procedures. Aliro Group must first confirm the individual cannot either:

- provide the standard identification required for the service/transaction; or
- confirm the standard identification is correct where details do not match (e.g., date of birth, address, name).

Alternative identification may be used for short-term barriers (e.g., natural disaster or family and domestic violence) so designated services can be provided while the individual replaces or updates standard identification. Standard identification should be obtained as soon as practicable once available.

Other sources may be used where approved by a Senior Manager.

Ongoing CDD

Aliro Group will monitor its customers in accordance with the risks assigned to the customer as part of the initial CDD process. The following measures will be undertaken for customers with ongoing business relationships:

Low Risk	Customers will be subject to ongoing transaction monitoring. A reassessment of the customer will only be undertaken where red flag indicators have been identified as part of ongoing transaction monitoring.
Medium Risk	A reassessment of the customer will be conducted at least every 3 years, or where red flag indicators have been identified as part of ongoing transaction monitoring.
High Risk	A reassessment of the customer's risk will be conducted at least annually, or where red flag indicators have been identified as part of ongoing transaction monitoring. Where customers have been identified as a PEP, searches will also be refreshed semi-annually.

Reassessments will include reviewing:

- The customer's transactions and behaviours that may indicate that the customer's ML/TF/PF risk rating assigned from the initial CDD has changed
- Any changes to the nature of the relationship with the customer during the business relationship.
- Information available from independent sources
- Any SMRs that have been submitted relating to the customer
- adverse media hits, sanctions/PEP change, unusual transaction patterns, ownership changes

The reassessment will consider if the customer's risk rating remains applicable. Where a revised risk rating is required, initial Senior Manager approval will be obtained.

Where there may be indications that a customer's KYC information may require updating, a reverification of the customer's KYC information may be completed.

Transaction Monitoring

We will monitor transactional activity by our customers on an ongoing basis in order to detect activity or behaviour that may be indicative of Suspicious Matters (which may give rise to a Suspicious Matter Reporting Obligation) or other abnormal or atypical activity that may be suggestive of any of the following:

- circumstances that indicate a customer may not be who they initially had claimed to be
- circumstances that directly indicate a customer may be seeking the delivery of our services:
    - in connection with the commission of a ML or TF offence
    - in connection with the commission of any other offence against any laws of the Commonwealth, States or Territories of Australia
    - the existence in relation to a prospective Customer of one or more of the 'Red Flag' risk indicators set out in Appendix A to this document

Customers that are subject to transaction monitoring may:

- be required to provide additional KYC information
- be subject to enhanced due diligence
- result in a Suspicious Matter Reporting Obligation

Transactions may be paused until Aliro Group are satisfied that the activity or behaviour are not of a suspicious nature. In circumstances where Aliro Group cannot satisfy ourselves of the matter, Aliro Group's relationship with the customer may be reassessed.

If at any time, we have reasonable grounds to doubt whether an existing customer is the person they claim to be, we must within 14 days of formation of that opinion, take appropriate and reasonable steps to satisfy ourselves as to the true identity of the customer including undertaking further Identification and Verification Procedures. Failure to satisfy ourselves as to the true identity of a customer will give rise to a Suspicious Matter Reporting Obligation.

Refer to section 13 for further information on Transaction Monitoring.

Politically exposed persons

Politically exposed persons (PEPs) are individuals entrusted with prominent public functions and influence, and those closely connected to them. Because of their positions or associations, PEPs can present elevated bribery and corruption risk (e.g., influence over public spending, procurement, approvals and grants). PEP status does not imply wrongdoing; ML/TF/PF risk must be assessed case by case.

Whilst it does not mean that PEPs are automatically involved in unlawful activity, the ML/TF/PF risks of each customer, including PEPs, should be assessed on a case-by-case basis.

PEP categories

Identified PEPs will be assessed as any of the following:

1. Foreign PEP: Holds a prominent public office or function in the legislature, executive or judiciary of a foreign country (see AUSTRAC list: https://www.austrac.gov.au/amlctf-reform/reforms-guidance/amlctf-program-reform/customer-due-diligence-reform/politically-exposed-persons-reform).\
2. Domestic PEP: Holds a senior office or position in Australian government institutions (see AUSTRAC list above).
3. International organisation PEP: Holds a prominent function/office in a public international organisation (e.g., head, deputy head or board member of a UN body).

Related Persons

A PEP also includes:

- a family member of a PEP; or
- a close associate known through public/readily available information to have joint beneficial ownership, hold beneficial ownership on behalf of a PEP, or maintain other close business relations with a PEP.

Screening

Before providing a designated service, we must establish on reasonable grounds whether any of the following is a PEP:

- the customer
- any person acting on behalf of the customer
- any beneficial owner of the customer
- any person on whose behalf the customer is receiving a designated service.

PEPs should be identified through the following:

1. Declared upfront by the customer (i.e. customer form)
2. Identified through PEP scans conducted by Aliro Group
3. Identified through adverse media checks conducted by Aliro Group

The results of PEP scans must be documented in Aliro Group's review of each customer as part of the KYC process and maintained in accordance with record maintenance requirements.

High-risk PEPs

A PEP is high risk if they are a foreign PEP or hold a high-ranking position. Where a PEP has been assessed as high-risk:

- the PEP's source of funds and source of wealth must be established on reasonable grounds (refer to Source of funds and source of wealth); and
- Approval must be obtained from a Senior Manager to proceed with providing a designated service to the customer. If an existing customer becomes a PEP, Senior Manager approval must also be obtained to continue a business relationship with the customer.

Individuals identified as PEPs must be monitored every 6 months to confirm they continue to be PEPs for the duration of the business relationship. This should be done by performing PEP scans and adverse media checks on the customer.

Sanctioned Individuals

Sanctions are measures that a government or the United Nations Security Council imposes in response to a situation of international concern. The Department of Foreign Affairs and Trade (DFAT) maintains a Consolidated List of all persons and entities designated for TFS under Australian sanctions laws. The Consolidated List can be found here: https://www.dfat.gov.au/international-relations/security/sanctions/consolidated-list.

Aliro Group must not deal with assets owned or controlled by a person designated for TFS. We also must not make assets available to them. Breaking Australia's sanctions laws can be a serious criminal offence. Penalties of up to 10 years' imprisonment and significant fines apply for contraventions.

To manage this risk, Aliro Group must conduct sanctions checks concurrently with PEP and adverse media screening, including (but not limited to) the following lists:

- Department of Foreign Affairs and Trade (DFAT)
- European Union Financial Sanctions (EUFS)
- European Union: Europol
- International Interpol
- United Nations Security Council Consolidated List
- United Kingdom: HMT Financial Sanctions
- US OFAC – Department of Treasury
- US Department of State (DOS)

If a person is identified as designated for TFS during an existing relationship, this should be escalated immediately to the AML/CTF Compliance Officer for review. Confirmed sanctions may require that any assets the customer owns or controls be frozen and not dealt with or made available (directly or indirectly) without a sanctions permit.

The AML/CTF Compliance Officer must then:

1. Contact the Australian Sanctions Office
2. Report this to the Australian Federal Police as soon as practicable.

An SMR must be submitted with AUSTRAC if Aliro Group has information relevant to a contravention of Australia's sanctions laws.

Enhanced CDD

Enhanced CDD (ECDD) must be applied where a customer's ML/TF/PF risk is high, identified during initial CDD or through ongoing CDD. A customer may be reassessed as high risk due to monitoring alerts (e.g. adverse media), changes to KYC information, or changes in requested/used designated services.

The AML Compliance Officer and Senior Manager must be notified where ECDD is required to be undertaken.

ECDD must be conducted in the following circumstances:

1. An SMR is required and Aliro Group intends to continue providing a designated service. (ECDD is not required for customers mentioned but not suspected—e.g. fraud victims—unless needed to manage their ML/TF/PF risk.);
2. The customer requests unusual, large or complex transactions, transactions with no apparent economic/legal purpose, or an unusual transaction pattern;
3. The service forms part of a nested services relationship (not applicable to Aliro Group);
4. The customer or a relevant party is a foreign PEP (customer, beneficial owner, person receiving the service on behalf of the customer, or person acting on behalf of the customer); or
5. The customer or a relevant party is located in or formed in a FATF high-risk jurisdiction or jurisdiction under increased monitoring. The list of countries can be found on the FATF website (https://www.fatf-gafi.org/en/home.html).

ECDD measures must be proportionate to the risk driver and may include:

- additional KYC collection/verification,
- obtaining transaction/service purpose,
- verifying source of funds/wealth,
- enhanced understanding of ownership/background/financial position,
- intensified monitoring, and
- annual relationship review.

Completed ECDD on customers must be approved by a Senior Manager. Where necessary, a Senior Manager may elect to:

- refuse the provision of a designated service to a customer subject to ECDD where this falls outside Aliro Group's risk appetite; or
- pause designated services to a customer until any additional requests for ECDD information have been satisfied.

Source of funds and source of wealth

Source of funds refers to how and where the money for a specific transaction was obtained. Collecting and verifying it helps confirm the funds are legitimate and consistent with what Aliro Group knows about the customer and the purpose of the designated service.

Source of wealth refers to how the customer accumulated their overall net worth (e.g., economic, business or commercial activities and other contributing circumstances). It is relevant where there is doubt about the customer's overall financial background.

We will request source of funds/wealth information where:

- initial or ongoing CDD identifies ML/TF/PF risk relating to the origins of funds or wealth
- transactions or behaviour are unusual, or the customer's ML/TF/PF risk changes
- there is suspicion assets are derived from criminal activity
- the designated service could conceal or disguise assets
- transactions are unusually large/complex or follow an unusual pattern.

To establish the source of funds and source of wealth, we may:

- review information we already hold about the customer (eg. obtained during the onboarding process)
- collect, where appropriate, additional information to identify how the customer obtained the funds for the designated service or accumulated their wealth (e.g., salary/wages, business income, dividends/investments, sale proceeds, gifts/inheritance)
- verifying, where appropriate, any of the information using reliable and independent sources (eg. Web search, media checks).

When collecting and verifying this information, we must be satisfied that:

- there is a legitimate source for the customer's funds or wealth
- the information provided is consistent with what we expect of the customer.
- the customer's funds or wealth are not from unlawful activity.

The AML/CTF Compliance Officer is responsible for determining if source of funds or wealth are required.

Reliance on customer identification by a third party

Where a customer has already undergone KYC by another Reporting Entity for a designated service, Aliro Group may rely on that to avoid duplicating collection and verification. Reliance may be under an ongoing arrangement or on a case-by-case basis.

Aliro Group may only rely on a third party that is either:

- an Australian Reporting entity with measures in place to comply with their obligations under Parts 2 (Customer Due Diligence) and 10 (Record-keeping requirements) of the Act.; or
- an entity regulated in a FATF-aligned foreign jurisdiction for CDD and record-keeping, subject to Aliro Group's jurisdiction ML/TF/PF risk assessment and risk appetite.

Before relying on third party KYC, Aliro Group must assess:

a) the type and level of ML/TF/PF or other serious crime risks that Aliro Group may reasonably be expected to face in its provision of designated services; and
b) the nature, size, and complexity of the third party's business, including its products, services, delivery channels, and customer types; and
c) the level of ML/TF/PF or other serious crime risks in the country or countries in which the third party operates or resides;

Aliro Group must also obtain a signed attestation from them confirming:

- They are a Reporting Entity under Australian AML/CTF laws, or are regulated by a country under FATF
- Details of its enrolment with the relevant regulator
- They have not had any breaches relating to the ML/TF/PF laws (Australian or foreign)
- They have conducted CDD requirements on the noted customer in line with Australian AML/CTF laws, including:
    - Collected and verified information relating to the identity to the customer
    - Collected and verified information of any individual investors holding more than 25% ownership of the customer (if not a natural person), or a controller where applicable
    - They will continue to maintain record of the KYC documentation in accordance with Australian AML/CTF laws (7 years), and will provide such information if requested.
    - PEP, sanctions and adverse media checks have been completed with no issues noted.

The Senior Manager must confirm their approval that the arrangement can be relied on. Documentation including the decision to rely on a third party must be maintained. Where an arrangement has been entered into, an assessment will be conducted and documented to ensure that all requirements have been met.

Assessments of any agreements or arrangements in place with third parties being relied on are required to be conducted at least every 2 years, having regard to:

a) the type and level of ML/TF/PF or other serious crime risks faced by Aliro Group; and
b) any material changes in the nature, size, and complexity of the third party's business, including its products, services, delivery channels, and customer types

Initial and reassessments are required to be documented within 10 business days after the day of completing the assessment.

This section does not cover outsourcing or agency arrangements, as these parties are not subject to oversight and supervision under Australian AML/CTF laws.

Outsourcing

Aliro Group may elect to outsource its CDD procedures. In these circumstances, Aliro Group remains ultimately responsible for outsourced services in accordance with the Act. The outsourced services provider must have documented AML/CTF Procedures that align with the requirements of this Program.

Aliro Group has implemented an Outsourcing Policy which includes various due diligence requirements on external service providers prior to their engagement. The key obligations Aliro Group imposes under this Program when CDD is outsourced are:

- an assessment of the operational competency of the proposed service provider prior to their appointment
- contractual documentation imposing obligations on the service provider to ensure they can comply with the Act
- a requirement that the service provider provides regular compliance certificates attesting to their compliance
- a monitoring program whereby the Company may come and inspect the service provides operating environment to test compliance with obligations
- periodic review of the service provider's AML/CTF procedures to ensure they are consistent with the requirements of this Program

Aliro Group will conduct sample testing on a periodic basis of completed KYC reviews to ensure that the appropriate risks have been considered in the onboarding of customers and its provision of designated services to these customers. Assurance reviews will include KYC procedures conducted by Aliro Group and service providers.

12. Personnel Due Diligence and Training

Roles and Responsibilities relevant to ML/TF/PF Risk

Personnel due diligence and training must be conducted for those who perform or will perform roles relevant to Aliro Group's AML/CTF obligations. This includes people employed at Aliro Group and people otherwise engaged to provide services for Aliro Group. For example:

- contractors or consultants
- volunteers or interns (paid and unpaid)
- people employed by service providers we use.

As Aliro Group's business deals with high volume and high value transactions on a day-to-day basis, all teams are required to undertake employee due diligence and AML/CTF training.

High Risk Roles

High-risk roles relating to ML/TF/PF risk include those that:

- may make an employee a target for collusion or coercion by criminal groups
- could pose a serious ML/TF/PF or non-compliance risk if fulfilled by someone with inadequate skills or integrity.

The following roles have been identified as high-risk:

Roles/Responsibilities	**Risk**
Payment Inputters	Processing of high value transactions
Payment approvers	Authorisation of payments to external parties
Head of Group Finance	Approval of high value transactions
COO	Ability to override/bypass internal controls Ability to approve high-risk customers

Due Diligence Requirements

Background checks are undertaken on all new employees regardless of their position. These checks include performing searches to ensure that the prospective employee:

- has the skills and knowledge to perform their roles effectively
- has not been convicted of any offences involving dishonesty, money laundering or terrorism financing by obtaining a National Criminal History Check (or equivalent in other jurisdictions)
- has not been the subject of disciplinary action by ASIC (or any equivalent regulator)
- is not a bankrupt; and has not taken advantage of the laws relating to bankruptcy
- querying if the employee has lived in a "high-risk" country, such as a country that is subject to international trade sanctions or unilateral Australian sanctions
- is not a PEP or related to a PEP (or if is, the risk is acceptable)

Background checks will be refreshed at least every 2 years for all staff members. Where exceptions have been identified, this will be reviewed by a Senior Manager to determine the appropriate course of action.

In addition, where an employee has been promoted or their role has changed so that they are involved in any money handling, cash payments, accounting, human resources or customer interactions, a refreshed employee due diligence process will be conducted.

The AML/CTF Compliance Officer is responsible for ensuring the that the employee due diligence process is completed appropriately and on an ongoing basis.

Training Requirements

Aliro Group has a risk awareness training program to provide its employees appropriate training in identifying transactions or clients which may be using our Designated Services to launder money or finance terrorism.

This risk awareness program is conducted at the following intervals:

- All new employees on induction
- Annually, for other employees that are involved in any money handling, cash payments, accounting, human resources or customer interactions, or where an employee's role has changed to include such responsibilities (where previously none)

Under the training program, employees need to be made aware of:

- Our obligations as a Reporting Entity under the Act and Rules including, but not limited to the requirement to report Suspicious Matters (this could include making a list of the 'Red Flags' and distributing them to Employees), Threshold Transactions and other compliance matters
- procedures and processes which must be carried out by the employee in accordance with this Program including, but not limited to CDD procedures
- the consequences of non-compliance with this Program
- the type of ML/TF/PF risks that we face and the consequences of failing to address these risks

Aliro Group may determine that it is appropriate for AML/CTF training to be provided within a reasonable period after commencement of their role. No new employee may undertake an unsupervised role or a role with medium or higher ML/TF/PF Risk without obtaining the appropriate AML/CTF training.

Aliro Group maintains records of training provided to and completed by employees. The AML/CTF Compliance Officer is responsible for ensuring the training program is appropriate and up to date.

13.AUSTRAC Reporting Obligations

Suspicious Matter Reports (SMR)

Section 41 of the Act provides that, we are required to report to AUSTRAC 'Suspicious Matters' that fit any of the descriptions set out in Appendix A of this Program. The Act also imposes prescribed time frames (within 3 day for Suspicious Matters and 24 hours for Terrorism Financing) for us to complete that reporting.

For the purpose of this Program, a 'Suspicious Matter' will be deemed to have occurred when there are reasonable grounds for us to suspect:

- That a Customer, or an agent purporting to act on their behalf, is not who they claim to be
- We have information that may be relevant to the investigation of an evasion of tax law, or the prosecution of a person for an offence against the laws of the Commonwealth, States or Territories of Australia, or may be of assistance in the enforcement of the Proceeds of Crimes Act 2002 (Cth) (or equivalent State or Territory legislation)
- The provision by us of a Designated Service has been used or may be used to assist the financing of a ML or TF offence
- The provision by us of a Designated Service may be relevant to the investigation or prosecution of a person for a ML or TF offence

Each Employee who forms a belief, or becomes aware of information to indicate that a Suspicious Matter may have occurred must notify the AML/CTF Compliance Officer of that belief.

Within 2 hours of receipt of a notification from an Employee, or if otherwise becoming aware of a possible Suspicious Matter the AML/CTF Compliance Officer must:

- Review and investigate the issue in order to decide whether or not a Suspicious Matter Reporting Obligation has been triggered within the meaning of the Act and Rules
- Consider whether it is appropriate to make the Customer subject to the enhanced due diligence procedures
- ensure that any further enquiries:
    - are conducted in a prudent manner using common sense, tact and discretion; and
    - do not give rise to a 'tipping off' offence (see below)
- seek guidance from AUSTRAC or professional legal advice if unsure
- keep a written record of any review and investigation undertaken.

If a SMR is required and lodged with AUSTRAC, the AML/CTF Compliance Officer will promptly inform the Senior Manager and the Board. Any SMR reported to AUSTRAC must be complete, accurate and free from unauthorised change.

Transaction Monitoring Program

The Transaction Monitoring process has been implemented as part of the payment workflow within Aliro Group's internal systems, and is manually conducted as part of the payments process by the payments team. Prior to process payments, the payments team is responsible for ensuring that the details surrounding a transaction do not consist of any red flag indicators under Appendix A of this AML/CTF Program, including (but not limited to):

- Non-standard transactions for high risk designated investors
- requests to pay redemption requests or distribution payments to third party bank accounts or bank accounts which do not match the name of the investor
- requests to pay redemption requests or distribution payments to customer accounts in jurisdictions other than where the investor is domiciled;
- new commitments received from bank accounts which are not in the name of the investor or in a jurisdiction other than where the customer is domiciled;
- transactions to or from high-risk countries or regions as determined by the Financial Action Task Force;
- transactions to or from prescribed foreign countries as determined by the Financial Action Task Force
- transactions to or from countries, persons or entities for which sanctions have been imposed by the Department of Foreign Affairs and Trade and other applicable sanction obligation of the jurisdiction of operations;
- payments to or from known tax havens which may indicate evasion of tax obligations;
- payments to or from known terrorist organisations as identified on the Australian National Security website
- any other unexpected account activity from a customer may indicate money laundering or terrorism financing.

Once the team is satisfied that the transactions have been considered against the red flag indicators, they are required to confirm within the Payments module (ECHO). Where red flag indicators have been identified, the AML/CTF Compliance Officer should be alerted to review the indicators.

Tipping Off

Aliro Group must not disclose information about an SMR (or any other required report) to anyone outside Aliro Group (the tipping off prohibition). It is an offence to disclose such information to a person other than AUSTRAC where the disclosure would or could reasonably be expected to prejudice an AUSTRAC investigation (s123). "Prejudice" includes conduct that could negatively affect an investigation—even if we do not know it will.

Examples of when an investigation could be prejudiced include:

- telling a customer or their known associate that we have provided, or need to provide, an SMR or further information to AUSTRAC in relation to their activities
- telling a customer that we suspect they are using our services to engage in criminal conduct, or giving them enough Information that they understand we have formed such a suspicion requiring us to report to AUSTRAC
- accidentally disclosing Information publicly, for example if a staff member publishes the information on our website
- disclosing Information to someone who may share it more widely (eg. News journalists)

In such examples, the customer or an associate could be 'tipped off' that we are suspicious of their conduct and that we are required to submit an SMR or respond to a notice. This may prompt them to change their behaviour to avoid detection by law enforcement and make investigations more difficult.

We are not prohibited from disclosing Information to third parties under the new tipping off offence if it would not or could not reasonably be expected to prejudice an investigation (eg. legal advisors, AML consultants).

To reduce tipping-off risk, staff must escalate directly to the AML/CTF Compliance Officer before discussing externally or more broadly internally, and information will be restricted to authorised staff on a need-to-know basis.

Threshold Transaction Reports (TTR)

Section 43 of the Act provides that, we are required to report to AUSTRAC all 'Threshold Transactions'. A Threshold Transaction is a transaction involving the transfer of $10,000 or more (or the foreign currency equivalent) in physical currency or digital currency.

Each Employee who handles a Threshold Transaction must notify the AML/CTF Compliance Officer of that fact. Employees should ensure that they remain aware of structured transactions that may have been designed to circumvent TTR thresholds as part of ongoing transaction monitoring (refer to Appendix A for red flag indicators)

The AML/CTF Compliance Officer must:

- report all Threshold Transactions to the AUSTRAC CEO within ten Business Days after the transaction takes place using the AUSTRAC prescribed form. Any Threshold Transactions reported to AUSTRAC must be complete, accurate and free from unauthorised change.
- report to the Board at the next scheduled board meeting that a Threshold Transaction has occurred.

Cross-Border Movement Reports (CBMR)

Aliro Group does not engage in the carrying of monetary instruments into or out of Australia, and does not receive money by mail, freight or courier. As such, CBMR is not applicable.

International Value Transfer Services (IVTS)

Aliro Group does not provide a registrable designated remittance service or conduct transfers relating to money, virtual assets or other property. As such, IVTS is not applicable.

Compliance Reports

As a part the requirements under the Act, an AML/CTF compliance report must be provided to AUSTRAC with information about our compliance with the Act.

The Company's AML/CTF compliance report must be lodged online at https://online.austrac.gov.au

The AML/CTF Compliance Officer is responsible for overall lodgement of the Compliance Reports, and must provide AUSTRAC with information about the Company's compliance with the Act.

14. Record Keeping

Record keeping means creating, storing and managing full and accurate AML/CTF records to evidence compliance, support ML/TF/PF risk management, and assist regulators where criminal exploitation occurs.

The AML/CTF Compliance Officer is responsible for ensuring the that Aliro Group keeps copies of relevant records as set out below.

Aliro Group (and its agents) will keep records relating to AML/CTF matters for **7 years** from:

- for records relating to Aliro Group's AML/CTF Program, the day the record is no longer relevant to the relevant reporting entity's compliance with its obligations under the Act;
- for CDD records carried out by Aliro Group, the day the business relationship ends or the reporting entity completes the provision of the occasional transaction;
- for CDD records carried out and provided by an agent, the latter of the day the due diligence was conducted and the day Aliro Group ceased to provide any designated services to the customer;
- for transaction records (other than customer-provided transaction records), the day the record is created; and
- for customer-provided transaction records, the day the records were provided.

Records that must be kept are:

- AML/CTF Program records
- CDD records (including how matters were established on reasonable grounds)
- transaction records relating to designated services
- AML/CTF Compliance Officer and Senior Manager appointment and decision records (including appointments, basis for senior manager status, escalations, decision-maker, decision date and rationale).

Records must be sufficient to demonstrate compliance and enable reconstruction of individual transactions. Records may be hard copy or electronic and stored onsite or offsite in Aliro Group's usual formats. Sensitive information must be stored securely with access restricted to authorised staff on a need-to-know basis, and handled in accordance with the Privacy Act and Aliro Group's Privacy Policy (refer to Privacy Policy).

The following forms of documentation should be maintained as part of AML/CTF procedures conducted by Aliro Group:

Document	**Form**
A record made by Aliro Group of information relating the provision of a designated service to the customer	original, copy or an extract from the record
A document given to Aliro Group by the customer (or someone on behalf of the customer) relating to the provision or prospective provision of a designated service by us to the customer (if Aliro Group provides a designated service to that customer)	original or copy
A record of CDD procedures carried out in respect of a customer (if Aliro Group provides a designated service to that customer). This includes any procedures carried out by a third-party Reporting Entity or outsourced services provider.	original or copy

(The record must allow Aliro Group to demonstrate that the procedure has been carried out, and the information and documents collected in the course of the procedure)	
Information obtained in the course of carrying out CDD procedures (if we provide a designated service to that customer)	original or copy
Internal verification procedures of PEPs and TSFs (such as search results), including approval by the Senior Manager	original or copy
Documentation of compliance with obligations of the AML/CTF Program including: - AUSTRAC Enrolment - ML/TF/PF risk assessment - policies - responsibilities of governing bodies - AML/CTF compliance officers - program documentation and approvals.	original or copy
Employee recordsf	Original or copy
Documentation of the results of periodic and independent reviews	Original or copy

Appendix A – Red Flag Indicators

Transaction monitoring

The following red flag indicators will be considered as part of Aliro Group's ongoing business relationships with customers:

- The Customer engages, or seeks to engage, in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 reporting Threshold Transactions, especially if the cash or monetary instruments are in an amount just below the reporting or recording Threshold Transactions ("Structured Transactions").
- The Customer requests to pay or be paid in cash or cash equivalents.
- The Customer's account has a large number of ingoing or outgoing or electronic transfers that have no apparent business purpose.
- Receiving five or more applications from the same Customer during the same Quarter.
- Receiving three or more applications and three or more redemptions from the same Customer during the Quarter.
- A Customer exercising the Scheme's cooling-off period for an application more than once during a six-month period.
- A Customer changing bank account details more than once during a six-month period.
- The Customer maintaining multiple accounts or maintaining accounts in the names of family members or corporate entities, for no apparent purpose.

Suspicious Matter Reporting (SMR) Obligation

The following red flag indicators will trigger the need for an SMR by Aliro Group:

- indicates that the Customer may not be who they claim to be.
- might be relevant to the investigation of an evasion of tax law or the prosecution of a person for an offence against a Commonwealth, State or Territory law, or may be of assistance in enforcement of the Proceeds of Crime Act 2002 (Cth) (or criminal and State or Territory legislation).
- indicates that the provision of the designated service may be preparatory to the commission of a terrorism financing or money laundering offence.
- may be relevant to the investigation of or prosecution of a person for a terrorism financing or money laundering offence.

Other Suspicious Behavior

The following red flag indicators will be escalated to the AML/CTF Compliance Officer for review:

- The Customer showing unusual concern about our compliance with reporting requirements and the processes and procedures contained in the Program.
- The Customer engaging in transactions that lack business sense or apparent investment strategy, or are inconsistent with the Customer's stated investment objectives.
- The information provided by the Customer that purports to identify a legitimate source for funds is suspected to be false, misleading or substantially incorrect.
- The Customer appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person's identity.
- The Customer has difficulty describing the nature of their business or lacks general knowledge of their industry.
- The Customer (or in the case of a corporate entity, persons representing or purporting to act on behalf of the Customer) exhibits unusual concern, reluctance or refusal regarding compliance with our Program.
- The Customer (or a person publicly associated with the Customer) is known to have a criminal, or otherwise questionable, background or is the subject of news reports indicating involvement in possible criminal, civil, or regulatory violations.

Foreign Customers

- The Customer is revealed to have a substantial personal or business connection with, or makes payment from, or requests payment to, a financial institution account or provides an address in a Non-compliant Jurisdiction.
- The Customer is identified as a Politically Exposed Person. In addition, we will Verify or re-verify beneficial owner information in accordance with the identification requirements specified in Chapter 4 of the AML/CTF Rules, and seek senior management approval for:
    - continuing a business relationship with the customer;
    - whether a transaction on an account should be processes; and
    - whether the designated service should continue to be provided to the customer.
- The Customer is a person physically located in or a corporation incorporated in a prescribed foreign country.