Anti-Money Laundering and Counter Terrorism Financing Program

Our Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Program outlines our commitment to preventing financial crime and supporting a safe and transparent property industry. This AML/CTF Program is comprised of two parts:

- Part 1 – the Policy,
- Part 2 – the Process Document.

Version Control

This Program is maintained as a controlled document. When updates are made, the version table below is updated to reflect the change. Previous versions are retained for 7 years.

Version	Date approved	Approved by	Summary of changes
1.0	17 June 2026	Kai Zhu	AML/CTF Program document

When this document is updated and re-uploaded to the FlowAML Compliance Hub, add a new row to identify the version, approval details, and a summary of changes since the previous version.

Contents

To refresh this table of contents: click anywhere inside it, then press F9 (or right-click and choose Update Field).

1. Introduction

1.1 Purpose of this Program

This document sets out the Anti-Money Laundering and Counter-Terrorism Financing Program (AML/CTF Program) for Teamlink Pty Ltd. Our business provides designated services for the purchase, sale or transfer of real estate. These are a 'designated service' under the AML/CTF Act 2006 and are referred to as 'designated services' throughout this document.

The purpose of the Program is to establish the principles, processes and controls that Teamlink Pty Ltd uses to stop its services being misused for money laundering, terrorism financing or proliferation financing (collectively referred to as ML/TF risks). It has been built to meet the AML/CTF Act 2006 (as amended by the Anti-Money Laundering and Counter-Terrorism Financing Amendment Act 2024), the AML/CTF Rules 2025, and guidance issued by the Australian Transaction Reports and Analysis Centre (AUSTRAC).

The Program works alongside Teamlink Pty Ltd's:

- Risk assessment, which describes the ML/TF risks the business faces
- Process documents and forms, which set out the day-to-day steps for meeting its obligations.

Once approved, the Program must be followed.

1.2 Approval and Adoption

This Program is approved by Teamlink Pty Ltd's senior manager. The governing body oversees the Program and takes reasonable steps to keep it effective.

1.3 Scope and Application

All Teamlink Pty Ltd staff must comply with this Program in the course of their duties. Where a service provider (such as AML Partners) carries out an activity under this Program, Teamlink Pty Ltd remains ultimately responsible for compliance with the AML/CTF Act.

2. Key Principles

This Program is built on the following principles:

- It uses a risk-based approach matched to Teamlink Pty Ltd's ML/TF risk profile.
- It enables Teamlink Pty Ltd to identify, manage and reduce the risks set out in its risk assessment.
- It protects Teamlink Pty Ltd's reputation, integrity and ability to operate.
- It supports cooperation with law enforcement to help detect and disrupt criminal activity.
- It fosters a culture where all staff understand and meet their AML/CTF obligations.

3. Key terms and references

Forms and processes

Teamlink Pty Ltd uses the FlowAML software solution, operated by AML Partners, together with the process documents to put this Program into practice. In this document, a form refers to a digital form completed within FlowAML, unless stated otherwise.

Material change

A material change means an update to a process or document that affects how Teamlink Pty Ltd meets its AML/CTF obligations or manages ML/TF risk. Routine software updates, minor workflow tweaks, and fixes like typos or links are not material changes.

Reasonable

Where we use the word reasonable, such as reasonable steps or reasonable grounds for suspicion, this means what a reasonable person in Teamlink Pty Ltd's position would have done or suspected on the available facts. A reasonable person is a hypothetical person showing ordinary judgement in the circumstances.

Escalating to the compliance officer

Escalating to the AML/CTF compliance officer covers matters detected by:

- the compliance officer, who actions the matter themselves
- other staff and AML Partners, who escalate it through FlowAML using the unusual activity report function for potential suspicious matters, or the escalation function for all other matters.

Timeframes

Most actions, processes and forms have a completion timeframe. Where none is given, it must be completed as soon as practicable considering the circumstances in the individual case.

4. Outsourced AML/CTF arrangement

Teamlink Pty Ltd has engaged AML Partners as its outsourced AML/CTF service provider to perform the operational AML/CTF activities required under this Program. This arrangement is supported by the FlowAML software solution operated by AML Partners.

4.1 Scope of outsourcing

Under this arrangement:

- Teamlink Pty Ltd collects initial customer information (including property address and customer contact details) and refers each customer and transaction to AML Partners through the FlowAML platform.
- AML Partners performs the AML/CTF process steps on behalf of Teamlink Pty Ltd. This includes initial customer due diligence, sanctions, PEP and adverse media checks, beneficial ownership tracing, source of funds and source of wealth checks, and the preparation of escalations and reports.
- AML Partners escalates all customers, transactions, and findings back to Teamlink Pty Ltd's AML/CTF Compliance Officer for review, decision and acceptance.
- AML Partners maintains the FlowAML platform, records, audit logs and supporting systems used to evidence compliance with this Program.

4.2 Roles and responsibilities

Activity	Who performs	Decision by Teamlink Pty Ltd's Compliance Officer
Initial customer due diligence (CDD)	Teamlink Pty Ltd collects onboarding information (including property address and customer contact details). AML Partners verifies identity; performs sanctions, PEP and adverse media checks; traces beneficial ownership; conducts customer risk assessment and compiles findings.	Review findings; accept or reject; authorise commencement of designated services.
Ongoing CDD and customer monitoring	Teamlink Pty Ltd monitors transactions and behaviour and flags changes. AML Partners identifies trigger events and prepares updated recommendations.	Review and accept ongoing CDD outcomes; approve risk rating changes; direct any further action.
Enhanced CDD	Conduct additional checks (source of funds, source of	Decide whether to start or continue providing designated

Activity	Who performs	Decision by Teamlink Pty Ltd's Compliance Officer
	wealth, expanded adverse media); prepare enhanced CDD findings.	services; obtain senior manager approval for high-risk customers, foreign PEPs, high-risk domestic PEPs and high-risk international organisation PEPs.
Suspicious matter reports (SMRs)	Teamlink Pty Ltd detects and escalates potential suspicious matters via unusual activity report.	Completes the unusual activity report review. Form reasonable grounds for suspicion; notify governing body; complete SMR submission to AUSTRAC within statutory timeframes.
Threshold transaction reports (TTRs) and cross-border movement (CBM) reports	Teamlink Pty Ltd identifies and escalates reportable transactions.	Prepares TTR or CBM report submission to AUSTRAC within statutory timeframes.
Sanctions hits	Detect potential sanctions matches and escalate immediately.	Confirm match; direct cessation of services; complete SMR submission to AUSTRAC within statutory timeframes; notify Australian Sanctions Office and Australian Federal Police as required.
Offboarding	Identify offboarding triggers; prepare offboarding recommendation with supporting evidence.	Approve offboarding decisions; record reasons; oversee implementation by Teamlink Pty Ltd personnel.
Annual compliance report (ACR)	Compile data and prepare draft ACR.	Review, accept and submit ACR to AUSTRAC by 31 March; provide a copy to the governing body.
Record keeping	Maintain all CDD, transaction, escalation, and audit records securely within FlowAML for 7 years.	Access records as required; provide records to AUSTRAC, governing body, and independent evaluators on request.

4.3 Retained responsibilities of the Reporting Entity

This outsourcing arrangement does not transfer Teamlink Pty Ltd's legal obligations under the AML/CTF Act. Teamlink Pty Ltd remains the reporting entity and is ultimately responsible for AML/CTF compliance.

Teamlink Pty Ltd retains the following responsibilities:

- appointing and maintaining a suitable AML/CTF Compliance Officer
- maintaining a governing body with appropriate oversight of the AML/CTF program
- reviewing and accepting all findings prepared by AML Partners
- submission of SMRs, TTRs, CBM reports and the ACR to AUSTRAC
- approving customer onboarding decisions, risk rating changes, enhanced CDD outcomes and offboarding decisions
- notifying personnel of any directions arising from AML Partners' findings
- approving material changes to this Program
- approving the version control record when this Program is updated
- ensuring its personnel cooperate with AML Partners to provide information needed to complete checks.

PART 1

Policy Document

Teamlink Pty Ltd

5. Personnel

This section sets out how Teamlink Pty Ltd appoints, supports and manages the people responsible for its AML/CTF program. AML Partners performs the operational AML/CTF checks under the outsourcing arrangement (section 4), but Teamlink Pty Ltd remains responsible for appointing and maintaining its own AML/CTF roles.

What's in this section

This section covers three areas, summarised below.

Area	What Teamlink Pty Ltd does	Supporting tools
Align people to roles	Decide who holds each key role i.e. governing body, senior manager, compliance officer and customer-facing staff. Assign each role its AML/CTF responsibilities.	Roles and responsibilities recorded in FlowAML.
Check people are suitable	Confirm each person is suitable before appointment, keep checking suitability over time, and act where someone is no longer suitable.	Recorded and retained in Teamlink Pty Ltd's own HR or personnel records.
Train people	Deliver training so staff understand their obligations and can apply the program day to day.	FlowAML training modules, with completion tracked in the platform.

5.1 Fill key AML/CTF roles

This part ensures Teamlink Pty Ltd's people are appointed to AML/CTF roles, eligible for them, and able to perform their duties. In a single-employee business, one person holds all roles.

Appointing people to key roles

Teamlink Pty Ltd maintains eligible people in these key AML/CTF roles:

- governing body
- senior manager(s)
- AML/CTF compliance officer
- any other staff who help meet AML/CTF obligations, including customer-facing staff who monitor activity.

People are appointed by completing the relevant personnel due diligence (section 5.2) and recording each appointment in FlowAML.

A suitable compliance officer is appointed within 28 days (from 1 July 2026) of either starting to provide designated services, or the existing officer becoming ineligible, changing role or leaving. AUSTRAC is notified through AUSTRAC Online within 14 days of appointing a new compliance officer.

Role responsibilities

Each role's AML/CTF responsibilities are assigned and recorded in FlowAML, and Teamlink Pty Ltd checks that people continue to meet them.

5.2 Personnel due diligence

Personnel due diligence (PDD) confirms that everyone in a key AML/CTF role is suitable and able to meet their obligations.

Initial PDD

Initial PDD is completed:

- before a person starts or moves into a key AML/CTF role
- when something changes that may affect their suitability — for example criminal charges, financial distress, a conflict of interest, or suspicious behaviour.

PDD is conducted by Teamlink Pty Ltd using its own internal HR and pre-employment check policies and processes. FlowAML does not provide personnel due diligence functionality. The process used depends on the role:

Role	What the process requires
Single-employee business, or governing body that is also the compliance officer	A self-assessment of suitability against the fit-and-proper criteria, and a record of the decision. **Fit-and-proper criteria:** Suitability is assessed against six areas: capability, honesty and integrity, conflicts of interest, criminal history, adverse findings, and financial soundness. Where the person is a licensed real estate agent with a completed national criminal history check and no doubts about their integrity or identity, only capability and conflicts of interest need to be assessed.
Compliance officer (not also the governing body)	A national criminal history check (results within 6 months); an ordinary resident of Australia; have sufficient authority, independence and access to resources; and fit-and-proper assessment.
All other AML/CTF roles	Standard personnel checks scaled to the role and any doubts about the person's suitability.

Ongoing PDD

Where something may affect a person's ability to perform their role, Teamlink Pty Ltd reassesses their suitability, looking at both:

- integrity — such as criminal charges, major changes in finances, conflicts of interest or secondary employment
- competence — such as performance reviews, training outcomes and observed conduct.

People in AML/CTF roles self-report anything that may affect their suitability. Teamlink Pty Ltd collects and verifies any further information needed and records the outcome in its HR system alongside the initial PDD records.

When someone isn't suitable

Where a person isn't suitable for a role, Teamlink Pty Ltd takes one or more of these actions:

Issue	Action Description
Minor integrity concern	Reduce the risk of exploitation or move the person to a less sensitive AML/CTF role.
Significant integrity concern	Remove the person from AML/CTF duties.
Minor competency issue	Address through targeted training, a warning, disciplinary action, or a move to a simpler role.
Significant competency issue	Provide the support needed to build the required skills or replace the person with someone who has them.
No longer eligible (e.g. compliance officer is no longer an Australian resident)	Fill the role with an eligible person.

5.3 Personnel training

Teamlink Pty Ltd trains its people so they can carry out their AML/CTF roles. Training is delivered through FlowAML's digital training modules, which cover the topics set out below.

Initial training

Anyone starting or moving into an AML/CTF role completes training relevant to that role and its assigned responsibilities (as recorded in FlowAML). The compliance officer confirms new starters have finished the required training before giving them access to AML/CTF systems. Staff who don't complete mandatory training on time may face disciplinary action.

Ongoing training

The compliance officer reviews each person's competence in their role. Where someone is meeting their responsibilities, only training on material program changes is needed. Where gaps are found, targeted training is provided; if gaps can't be closed through training, the role is reassigned. All affected staff are trained on any material change to the program.

Training content and delivery

The compliance officer decides the content, format and frequency of training. Training helps staff understand:

- the ML/TF risks Teamlink Pty Ltd may face and the signs of criminal exploitation
- the AML/CTF obligations that apply to their role
- how to apply the program's processes to meet those obligations.

Training includes scenario-based exercises.

Role-specific training

For people in an AML/CTF role, training also covers how to:

- recognise ML/TF risks and indicators of criminal activity, and the risks Teamlink Pty Ltd will and won't accept (per the risk assessment)
- risk rate customers, identify suspicious matters, restrict services and offboard customers
- handle confidential reporting material and avoid tipping off
- meet CDD obligations during onboarding and throughout the relationship
- detect and escalate matters to the compliance officer
- meet any other responsibilities assigned to their role.

Reviewing training

The compliance officer refreshes training materials when ML/TF risks change, the program changes materially, or AUSTRAC issues relevant guidance — so training stays current with regulatory changes, emerging risks and updated business processes.

6. Customers

This section sets out how Teamlink Pty Ltd deals with customers, conducts customer due diligence (CDD), and reports to AUSTRAC. Under the outsourcing arrangement (section 4), AML Partners performs the operational CDD checks in FlowAML. Teamlink Pty Ltd' compliance officer reviews and accepts all findings before designated services start or continue and authorises all reporting to AUSTRAC.

A customer includes both the buyer and the seller of real estate, so CDD is completed on both the direct customer and any counterparty (for a seller's agent, the buyer; for a buyer's agent, the seller).

What's in this section

This section covers seven areas, summarised below.

Area	What happens	How FlowAML supports it
Initial CDD	Before a designated service starts, identify the customer type, collect onboarding details, complete initial CDD, and run extra checks for complex or high-risk customers.	Onboarding form, identity verification, and PEP, sanctions and adverse media checks run digitally in FlowAML.
Ongoing CDD	Monitor every customer for unusual activity that could require a Suspicious Matter Report. Refresh and re-verify CDD whenever a trigger event arises.	Ongoing monitoring and CDD is performed in FlowAML, including identity verification, PEP, sanctions and adverse media.
Pre-commencement CDD	Complete appropriate due diligence on customers already being served on 1 July 2026.	Pre-commencement records held in FlowAML.
High-risk and complex customers	Escalate high-risk customers, reportable matters, sanctions hits, complex ownership checks, and anything outside the risk assessment to the compliance officer.	Escalation and enhanced CDD managed in FlowAML.
Reporting	Report suspicious matters, threshold transactions and cross-border movements of $10,000 or more, and the annual compliance report.	Reports drafted in FlowAML for the compliance officer to authorise and submit.
Tipping off	Never let a customer know their behaviour is considered suspicious.	Confidential handling of reporting information in FlowAML.
Offboarding	Decline or stop services where a customer falls outside the risk appetite or would prevent Teamlink Pty Ltd meeting its obligations.	Offboarding decisions recorded in FlowAML.

6.1 Initial customer due diligence

AML Partners performs initial CDD and compiles the findings in FlowAML, then escalates them to Teamlink Pty Ltd's compliance officer, who decides whether to accept them and authorise designated services to begin. Initial CDD is done to identify customers, their representatives, beneficiaries and beneficial owners; identify each customer's ML/TF risk; and manage that risk.

When initial CDD is completed

For the direct customer, initial CDD is completed:

- Immediately after agency agreement signed and before listing activities

For the counterparty, initial CDD is completed:

- 28 days after the exchange of contracts or at least 3 days before the initially agreed day for settlement, whichever is earliest in a private treaty sale
- 28 days after the exchange of contracts or at least 3 days before the initially agreed day for settlement, whichever is earliest in an auction

When initial CDD can be delayed

Initial CDD may be delayed only for the counterparty – the party Teamlink Pty Ltd is not acting for – and only where completing it upfront would disrupt the ordinary course of business, never simply because the timing is inconvenient. When CDD is delayed, Teamlink Pty Ltd:

- completes initial CDD within the permitted timeframe above
- doesn't transfer, or allow or facilitate the transfer of, the customer's money, property or virtual assets, and doesn’t otherwise make money, property or virtual assets available to the customer (other than holding them)
- takes any other steps appropriate to manage the ML/TF risk.

How initial CDD is completed

To complete initial CDD, AML Partners:

- determines whether the customer is an individual, body corporate, partnership, unincorporated association, trust or government body
- collects onboarding details through the relevant FlowAML onboarding form
- performs the checks in the relevant FlowAML initial CDD forms

The following are escalated to the compliance officer to action before initial CDD is finished, and designated services pause until the officer confirms they can continue:

- potential suspicious matters
- high-risk customers

- complex beneficial ownership checks
- a positive sanctions match.

The following are escalated to the compliance officer to report, but services don't need to pause – any physical currency transaction, or cross-border movement of physical currency or bearer negotiable instruments, valued at $10,000 or more (or foreign-currency equivalent).

If a counterparty doesn't cooperate

Where a counterparty won't cooperate, Teamlink Pty Ltd:

- completes the onboarding form and initial CDD in FlowAML with the information available
- uses the delayed initial CDD option
- manages ML/TF risk through ongoing monitoring until settlement
- takes any other reasonable steps to gain cooperation, and records what was done.

6.2 Ongoing customer due diligence

Teamlink Pty Ltd manages each customer's ML/TF risk from first contact and throughout the relationship, monitoring activity and reviewing customer information periodically and when triggers arise.

Monitoring

Teamlink Pty Ltd monitors each customer for:

- unusual transactions and behaviours
- significant changes in the customer's ML/TF risk, their information, or the relationship
- any matter listed in the escalation and enhanced CDD policy.

Enough information is recorded in FlowAML to support effective monitoring, comparing customer activity against the risk factors and indicators in the risk assessment to establish what is unusual.

Periodic reviews

Where the relationship is ongoing, Teamlink Pty Ltd reviews and re-verifies the customer's information at a frequency appropriate to their risk, and whenever a trigger or doubt arises. Each new transaction is screened and the information held is confirmed to be current. One-off customers whose transaction has settled don't require ongoing review, as the relationship has ended.

Where a review finds information or a risk rating needs updating, the update is made. Where there is doubt about a customer's information, it is resolved before services continue; otherwise, it is updated as soon as practicable. Because most real estate transactions settle within 12 months, many customers won't need a periodic review.

Trigger-based reviews

A review using the trigger event review form is done when:

- the risk assessment changes in a way that affects how customer risk is assessed
- the customer's details or beneficial ownership change
- the customer requests a new designated service
- the customer becomes, or is found to be, a foreign PEP, a domestic PEP where the ML/TF risk of the customer is high, or an international organisation PEP where the ML/TF risk of the customer is high
- the customer becomes subject to targeted financial sanctions
- monitoring identifies unusual transactions or behaviours
- any other event casts doubt on the accuracy of the customer's information or risk rating.

Any updates identified are made so customer information stays accurate and complete.

Where a customer's ML/TF risk is low and enhanced CDD does not apply, Teamlink Pty Ltd may apply simplified customer due diligence measures in accordance with the AML/CTF Rules. Simplified CDD does not remove the obligation to monitor for unusual activity or to submit an SMR where required.

6.3 Pre-commencement customer due diligence

A pre-commencement customer is one Teamlink Pty Ltd was already serving on 1 July 2026. Initial CDD is not required on these customers upfront. Instead, Teamlink Pty Ltd monitors them for unusual activity that may require a Suspicious Matter Report, and for significant changes in the nature and purpose of the business relationship that may result in the ML/TF risk of the customer being medium or high. If a pre-commencement customer requests a new designated service after 1 July 2026, initial CDD is completed before that service begins.

6.4 Escalation and enhanced CDD

AML Partners identifies escalation events during CDD and monitoring, records them in FlowAML, and submits them to Teamlink Pty Ltd's compliance officer. The compliance officer decides what happens next – including whether services continue or stop, whether enhanced CDD findings are accepted, and whether senior manager approval is sought to keep serving a high-risk customer. Enhanced CDD must also be applied where a customer requests designated services that have no apparent economic or legal purpose, involve unusually complex or large transactions, or involve an unusual pattern of transactions. To apply this, Teamlink Pty Ltd follows the escalating matters to the compliance officer process.

Escalate to action — services pause

The following are escalated for the compliance officer to action, and services pause unless the officer says otherwise:

Event	Action Required
Potential suspicious matter	Teamlink Pty Ltd completes the unusual activity report review in FlowAML and prepares findings, including a draft SMR if needed. The compliance officer decides whether reasonable grounds exist — if not, staff may resume services; if so, the compliance officer authorises the SMR and reports to AUSTRAC within the required timeframes.
High-risk customer, or an SMR will be made and services will continue	AML Partners completes the enhanced CDD steps in FlowAML and prepares the findings. The compliance officer reviews them and obtains senior manager approval before staff resume services.
Something not in the risk assessment or outside risk appetite	AML Partners reviews the matter and prepares a recommended program update. The compliance officer and senior manager approves the update before staff resume services.
Complex beneficial ownership check	AML Partners map ownership and control, verify all beneficial owners and record results in FlowAML before staff resume services.
Customer on a sanctions list	AML Partners follows the sanctions screening process in FlowAML and escalates results. The compliance officer directs that the transaction does not continue and that the customer's property is not handled or made accessible and notifies the relevant authorities.

Escalate to report — services continue

The following are escalated for the compliance officer to report, and services don't pause:

Situation	Action Description
Physical currency transaction of $10,000 or more (or foreign-currency equivalent)	Submit a threshold transaction report via AUSTRAC Online within 10 business days.
Cross-border movement of physical currency or bearer negotiable instruments of $10,000 or more (or equivalent)	Submit a cross-border movement report via AUSTRAC Online within the required timeframes.

All information given to the compliance officer must be accurate and complete enough for them to act. The officer then passes on whatever each staff member needs for their role, including whether they can keep serving the customer.

6.5 Reporting

AML Partners detects, investigates and drafts reports (SMRs, TTRs and CBM reports). Teamlink Pty Ltd's compliance officer forms reasonable grounds for suspicion, notifies the governing body where required, and authorises submission of every report to AUSTRAC within the timeframes below.

Who does what

All staff detect potential suspicious matters, threshold transactions and cross-border movements through monitoring, and escalate them to the compliance officer.

The compliance officer makes sure reports are accurate, complete, unaltered, in the approved form, and submitted on time; investigates escalations; submits SMRs after notifying the governing body; reviews and submits TTRs and CBM reports; tells staff what they need to know; and reports to AUSTRAC and the governing body at least annually.

The governing body oversees compliance, reviews the officer's reports, and ensures there are enough resources and systems to meet reporting obligations.

Suspicious matter reports (SMRs)

The compliance officer uses the unusual activity report review in FlowAML to decide whether an SMR is required. An SMR is submitted where a designated service is being provided or requested and there are reasonable grounds to suspect that information may be relevant to an offence, that a person isn't who they claim to be, or that someone is planning a money laundering, terrorism financing or proliferation financing offence.

Where grounds exist, the SMR is submitted via AUSTRAC Online within 24 hours for terrorism-financing suspicions, or 3 business days for all others. Further SMRs are submitted if new suspicions arise. Where services continue after an SMR, the escalation and enhanced CDD policy is followed.

Only the compliance officer, governing body, senior manager, and anyone who needs it to meet obligations (such as legal counsel) may access SMR information. Teamlink Pty Ltd avoids anything that could amount to tipping off.

Threshold transaction reports (TTRs)

The compliance officer submits a TTR where a designated service involves $10,000 or more in physical currency (or equivalent), via AUSTRAC Online within 10 business days of the transaction.

Cross-border movement (CBM) reports

The compliance officer submits a CBM report for movements of physical currency or bearer negotiable instruments of $10,000 or more (or equivalent): before carrying them in or out of Australia, before mailing or shipping them, or within 5 business days of receiving them from overseas.

Annual compliance report (ACR)

Teamlink Pty Ltd prepares and submits an ACR to AUSTRAC by 31 March via AUSTRAC Online, following the annual compliance report process, and gives a copy to the governing body.

6.6 Tipping off

Teamlink Pty Ltd won't disclose information about a suspicious matter where doing so could reasonably be expected to prejudice an investigation.

What isn't disclosed

Teamlink Pty Ltd doesn't disclose, where it could prejudice an investigation:

- that an SMR has been made or is required
- any report, draft, or record prepared for SMR purposes, including unusual activity reports
- any document containing SMR information
- that it has given, or must give, information to a law enforcement or investigations authority
- that a customer is under investigation.

This information may be shared with the AUSTRAC CEO or an AUSTRAC entrusted person.

Dealing with customers

Where more information is needed, Teamlink Pty Ltd explains only that it's required to meet AML/CTF obligations — never that the request relates to suspicious activity or an investigation. If a customer is offboarded for suspicious activity and asks why, genuine reasons are given that don't reveal the suspicion.

Who can know about an SMR

Only the compliance officer, governing body, senior manager, and anyone who needs it to meet obligations (such as legal counsel, AUSTRAC or law enforcement) may access SMR information, which is stored securely. After an SMR, the compliance officer tells the person who raised the concern only what they need for their role and any directions (such as offboarding), without revealing that an SMR was made.

6.7 Offboarding

AML Partners identifies offboarding triggers and prepares a recommendation with supporting evidence. Teamlink Pty Ltd’s compliance officer decides every offboarding, and senior manager approval is obtained for each one. Teamlink Pty Ltd follows this policy when declining or stopping services to customers outside its risk appetite or where continuing would breach its obligations.

Risk appetite

The ML/TF risks Teamlink Pty Ltd will and won't accept — and how it avoids those it won't — are set out in the risk appetite columns of the risk assessment. Avoidance measures may include limiting or conditioning services, or declining or offboarding a customer.

Brokering agreement terms

Teamlink Pty Ltd's standard brokering agreement allows it to decline customers outside its risk appetite, stop acting for them, refuse or delay services where CDD information isn't provided, adjust services to manage risk, and report suspicious matters despite confidentiality obligations.

When offboarding is considered

Offboarding is considered where the risk assessment requires it, where a senior manager won't approve starting or continuing under the escalation and enhanced CDD policy, or where a customer fails to provide required information in a reasonable time.

Decisions and records

A senior manager approves offboarding decisions. Teamlink Pty Ltd records the reasons for offboarding or keeping a customer and all information requests and responses with dates.

How a customer is offboarded

As under the tipping off policy, where offboarding follows suspicious activity and the customer asks why, genuine reasons are given that don't reveal the suspicion. A direct customer and a counterparty are offboarded by stopping services, for example, telling the seller the sale can't be brokered with that buyer.

7. Maintain our AML/CTF Program

This section sets out how Teamlink Pty Ltd keeps its AML/CTF program current and effective. AML Partners supports this by monitoring AUSTRAC communications, flagging changes that may need a program update, and preparing recommendations. Teamlink Pty Ltd's compliance officer, senior manager and governing body review and approve all changes.

What's in this section

This section covers five areas, summarised below.

Area	What happens	Supporting process
Maintain the program	Keep the program current as ML/TF risks change. When a review is triggered, the compliance officer records updates and obtains senior manager approval.	Maintain your AML/CTF program; risk assessment and AUSTRAC communications processes in FlowAML.
Effectiveness checks	Check the program works and is being followed, and report to the governing body at least yearly.	Annual compliance report to the governing body.
Independent evaluations	Run an independent evaluation at least every 3 years and act on any findings.	Independent evaluation conducted by a suitably qualified, independent party. Findings and any resulting action plan recorded and retained.
Record keeping	Keep enough records to meet obligations and show compliance to AUSTRAC.	Records held securely in FlowAML for 7 years with audit logs.
AUSTRAC enrolment	Keep enrolment details accurate and current.	AUSTRAC enrolment process.

7.1 Maintain our AML/CTF program

Teamlink Pty Ltd keeps its program current, accurate and compliant. Where an event below occurs, it's escalated to the compliance officer to review and, if needed, update the program.

Event	When to update	How to update
A significant change to the services provided, delivery channels, technologies, customer types, or countries dealt with	If within Teamlink Pty Ltd's control, before providing the service; otherwise as soon as practicable	Use the country risk process for new country risks, or the inherent risk process for others. Record updates via the maintain your program form within 14 days, with senior manager approval for any material change.

Event	When to update	How to update
Any event showing the program isn't compliant or doesn't address ML/TF risks	If within control, before providing the service; otherwise as soon as practicable	Correct the deficiencies in policies, procedures, systems and controls.
AUSTRAC communicates about relevant ML/TF risks	As soon as practicable	Follow the AUSTRAC communications process.
An independent evaluation makes an adverse finding	As soon as practicable	Develop an action plan and obtain senior manager approval before implementing.
A periodic review is due	Every 3 years	Comprehensively review the program against current obligations and risks.

Teamlink Pty Ltd monitors and actions relevant AUSTRAC communications through the AUSTRAC communications process. When the risk assessment is updated, written updates go to the governing body, approved changes are shared with staff in relevant AML/CTF roles, and training is delivered where the change affects their work. The compliance officer makes sure staff understand the changes and tracks training completion.

7.2 Periodic effectiveness checks

The compliance officer periodically checks the program is working and reports to the governing body at least once a year.

When checks happen

Periodic checks cover SMRs, TTRs, compliance officer and senior manager functions, and all CDD processes (initial, ongoing, enhanced and pre-commencement). Where the compliance officer and governing body remain reasonably satisfied the program is effective and record why, checks can be less frequent — but happen at least yearly to inform the governing body report. Extra checks may be run after independent evaluation findings, unusual personnel activity, or other compliance issues.

Corrective actions

Any actions arising from a periodic check need senior manager approval before implementation. If a corrective action doesn't fix the issue, a new one is developed and implemented.

Documentation and reporting

Periodic check outcomes are available to the senior manager, governing body and AUSTRAC on request. The governing body reviews the reports and directs further action where issues remain unresolved.

Reporting to the governing body

The compliance officer reports to the governing body at least yearly, following the annual report to the governing body process, covering: the reporting entity's compliance with its AML/CTF policies; the extent to which the AML/CTF policies are appropriately managing and mitigating the risks of money laundering, financing of terrorism and proliferation financing; the reporting entity's compliance with the Act, the regulations and the AML/CTF Rules; training; risk assessment outcomes and emerging risks; customer onboarding numbers including high-risk customers and PEPs; sanctions screening results; SMR, TTR and CBM report volumes; and AUSTRAC communications and actions taken. This report isn't required where the business is a sole trader and the compliance officer is also the governing body.

7.3 Independent evaluations

Teamlink Pty Ltd has its program independently evaluated at least every 3 years, or more often if the governing body considers it necessary given the size, nature and complexity of the business.

Choosing an evaluator

The evaluator must have suitable experience and knowledge of the business, industry, ML/TF risks and obligations; not have been involved in building, running or using the program; be independent of the areas being evaluated; and have access to all relevant materials.

What the evaluation covers

The evaluator reviews: the steps taken by Teamlink Pty Ltd in undertaking or reviewing its ML/TF risk assessment, and whether those steps meet the requirements of the Act, the regulations and the AML/CTF Rules; whether the risk assessment is current; the design of the AML/CTF policies against the requirements of the Act, the regulations and the AML/CTF Rules; the compliance of Teamlink Pty Ltd with its AML/CTF policies (including sampling CDD files, reporting records, monitoring outputs and governance documents); whether Teamlink Pty Ltd is appropriately identifying, assessing, managing and mitigating the risks of money laundering, financing of terrorism and proliferation financing; whether any non-compliance is isolated or systemic, with recommendations; and the effectiveness of the risk controls.

Reporting and actions

The evaluator gives a written report to the senior manager responsible for approving program changes, and to the governing body if separate. All adverse findings are reviewed. Where findings are accepted, Teamlink Pty Ltd creates an action plan using the independent evaluation response form; the senior manager approves it, and the compliance officer implements it under the senior manager's oversight.

7.4 Record keeping

AML Partners keeps records of all AML/CTF activities performed for Teamlink Pty Ltd in FlowAML. Records are stored securely for 7 years and are available to Teamlink Pty Ltd's compliance officer, governing body, independent evaluators and AUSTRAC on request.

What's kept and for how long

AML Partners keeps in FlowAML the AML/CTF compliance records it generates for Teamlink Pty Ltd — including the risk assessment and its updates, CDD records, screening results, escalations, and anything needed to show a process was followed. CDD records are kept for 7 years after the relationship ends or after the last transaction.

Transaction records are kept by Teamlink Pty Ltd in its own systems, as these arise from the underlying property transactions rather than the checks performed in FlowAML. These include records provided by the customer and the minimum needed to reconstruct a transaction (date and time, type, amount and currency, customer information, and payment method), and are kept for 7 years from creation or receipt. All other records are kept for 7 years from when a previous version is no longer needed to prove compliance.

All records — whether held in FlowAML or by Teamlink Pty Ltd — are stored securely and accessible only to authorised people, kept confidential, auditable, accurate and unaltered, and held in English (or readily convertible to English).

7.5 AUSTRAC enrolment

Teamlink Pty Ltd enrols with AUSTRAC and keeps its enrolment details current.

Initial enrolment

Teamlink Pty Ltd applies to enrol no later than 29 July 2026 if it provides a designated service on 1 July 2026, or otherwise within 28 days of first providing a designated service after that date.

Managing enrolment

Teamlink Pty Ltd completes all mandatory fields in the AUSTRAC Business Profile, notifies the governing body in writing once enrolment or updates are done, and keeps the information current. It updates the profile within 14 days of any change to the business or its designated services, or to its earnings for the past 12 months. This is done through the AUSTRAC enrolment process, with records kept as that process requires.

PART 2

Process Document

Teamlink Pty Ltd

8. About this Process Document

This document sets out the processes Teamlink Pty Ltd follows to meet its AML/CTF obligations. This document supports and aligns with the Policy document (Part 1).

Under the outsourcing arrangement (see section 4), the operational steps in each process below are shared between Teamlink Pty Ltd and AML Partners.

Customer due diligence processes

9. Rate customer risk and conduct ongoing CDD

This process sets out how a customer's ML/TF risk rating is set at onboarding and reviewed over the course of the relationship.

It also describes how ongoing CDD and monitoring are scaled to the customer's risk rating.

Applying an ML/TF risk rating

Step	Action Description
1	AML Partners assesses which medium and high-risk factors apply, using the customer's onboarding information, the identity verification completed in FlowAML, the risk factors in the risk assessment, and any other information we hold. Applicable factors are recorded in FlowAML.
2	The customer's overall risk rating (low, medium or high) is determined in FlowAML based on the factors recorded.

Applying risk-based ongoing CDD

Teamlink Pty Ltd monitors each customer from first interaction through to the end of the relationship. The steps are set out below.

Step	Action Description
1	Teamlink Pty Ltd monitors the customer's behaviour and use of its designated services throughout the relationship, watching for: unusual transactions or behaviour; signs the risk rating may have changed; physical currency transactions of $10,000 or more; and cross-border movements of physical currency or bearer negotiable instruments of $10,000 or more.
2	Where any of these occur, Teamlink Pty Ltd uses the escalation triggers in FlowAML to decide whether to escalate the matter to the compliance officer.

Step	Action Description
3	Where the relationship is ongoing, Teamlink Pty Ltd also reviews periodically whether the customer's CDD information and risk rating remain accurate.
4	If activity suggests the risk rating may no longer be accurate, AML Partners re-applies the steps under 'Applying an ML/TF risk rating' and updates the customer's record in FlowAML where the rating has changed.

The required level of ongoing monitoring increases with the customer's risk rating, as set out below.

Risk level	Actions during ongoing CDD
Low	Monitor the customer's behaviour and transactions to detect unusual activity throughout the relationship. Review information where a trigger or doubt arises.
Medium	Apply a higher level of monitoring than for low-risk customers, with closer attention to transactions and behaviour. Review information where a trigger or doubt arises.
High	Apply the highest level of monitoring, with the closest scrutiny of transactions and behaviour. Review information more readily where a trigger or doubt arises, and apply enhanced CDD where required.

10. Verify the nature and purpose of the relationship

This process sets out how Teamlink Pty Ltd verifies the nature and purpose of a customer relationship as part of CDD.

Step	Action Description
1	Teamlink Pty Ltd uses FlowAML to collect information from the customer about the nature and purpose of the relationship, including why they need the service.
2	AML Partners checks whether the stated nature and purpose can be confirmed from information already held, comparing it against the customer's occupation, activities and what would be normal in the circumstances.
3	AML Partners attempts to confirm the information using reliable, independent sources — including ASIC and other searches in FlowAML, and customer-specific sources such as the customer's website.
4	If further confirmation is needed, AML Partners asks the customer for supporting evidence — for example, evidence of their occupation or activities.

11. Check source of funds and source of wealth

This process sets out how AML Partners checks a customer's source of funds and source of wealth, where required as part of enhanced CDD or where the customer's risk profile warrants it.

Source of funds

Step	Action Description
1	AML Partners asks the customer where the funds for the transaction came from — for example, salary or wages, or another source such as the sale of an earlier property.
2	AML Partners collects supporting evidence in FlowAML. Acceptable evidence includes: reliable independent sources (such as government databases or credible media); a signed letter from the customer's certified practicing accountant; payslips or an employer letter; an executor's letter confirming an inheritance; or a sale record or title deed.
3	AML Partners assesses whether the funds may have come from criminal activity, are inconsistent with the customer's profile, or cannot be linked to a legitimate source. If so, AML Partners escalates to the compliance officer in FlowAML who decides on submitting an SMR within the required timeframe.

Source of wealth

Step	Action Description
1	AML Partners asks the customer how they built their overall wealth and assets. Most customers will have accumulated wealth from a mix of sources over time — for example, employment, investments, or inheritance.
2	AML Partners collects evidence in FlowAML. Examples include: independent online sources; a signed letter from a certified practicing accountant confirming sources of wealth; pay summaries from current and former employers; an executor's letter; or a sale record or title deed from a property sale.
3	AML Partners assesses whether the wealth may have come from criminal activity, is inconsistent with the customer's profile, or is largely unexplained. If so, the Unusual activity report review is completed in FlowAML and an SMR is submitted to AUSTRAC where required.

12. Screen customers against sanctions lists

This process sets out how AML Partners screens customers, representatives and beneficial owners against targeted financial sanctions lists.

Personnel carrying out a sanctions check

Step	Action Description
1	AML Partners runs PEP, sanctions and adverse media checks digitally through FlowAML, using lists supplied by MemberCheck.
2	If a close match is identified on the list, Teamlink Pty Ltd stops engaging with the customer immediately, does not provide any services, and does not deal with or release any of their assets.
3	AML Partners escalates the matter in FlowAML, notifying the compliance officer immediately.
4	All sanctions checks are recorded against the customer's file, including details of the customer, the matched person or entity, the 'last updated' date of the list, and the screening result.

Responding to positive sanctions check

Step	Action Description
1	The matter is escalated in FlowAML to the compliance officer, who confirms the positive match and records the decision in the system.
2	Once confirmed, Teamlink Pty Ltd informs the senior manager(s) and governing body, ceases all customer activity, freezes any customer assets under its control, and notifies the Australian Sanctions Office and the Australian Federal Police. Where the match also gives rise to a suspicious matter, an SMR is submitted to AUSTRAC — within 24 hours for terrorism-financing suspicions, or within 3 business days for other suspicions.

13. Screen for politically exposed persons (PEPs)

This process sets out how AML Partners screens for current and former politically exposed persons (PEPs) as part of initial and ongoing CDD. PEP checks cover:

- the customer (if they're an individual)
- anyone representing the customer
- all beneficial owners of the customer.

Step	Action Description
1	AML Partners screens the customer, representatives and beneficial owners against PEP lists in FlowAML to identify any domestic PEP, foreign PEP, international organisation PEP, or related person of a PEP.
2	Where screening returns a potential match, AML Partners verifies whether it is a true match by reviewing the individual's details and supporting sources returned in FlowAML (up to the first 5 pages of results).
3	A confirmed foreign PEP is treated as high-risk, with enhanced CDD completed in FlowAML and senior manager approval obtained before services commence or continue. A confirmed domestic PEP or international organisation PEP where the ML/TF risk of the customer is high is also treated as high-risk, with enhanced CDD completed and senior manager approval obtained. Where a customer was previously a PEP, senior manager approval is required in accordance with the AML/CTF policies. AML Partners escalates the findings to the compliance officer in FlowAML for review and acceptance before services continue.
4	AML Partners records the PEP check results against the initial CDD record, including the lists screened (global and domestic), the sources reviewed, and the outcomes.

14. Check for adverse media

This process sets out how AML Partners checks for adverse media about customers, their representatives, beneficial owners, and any person the customer is acting on behalf of. The check helps inform the customer's ML/TF risk rating and identify any signs of suspicious behaviour.

Step	Action Description
1	AML Partners conducts the adverse media search digitally in FlowAML, using the same search tooling as the sanctions check.
2	AML Partners checks that the media sources are reliable and independent — including reports of settled criminal convictions, charges, executed law-enforcement powers, arrests, or findings of fact in civil proceedings verified by court or government references. Spent or expunged convictions are not considered.
3	AML Partners assesses the relevance of any reports — in particular, whether the alleged offences are profit-generating (such as money laundering, fraud, corruption, drug trafficking, people smuggling or other serious or organised crimes). Minor or non-profit-generating offences carry less weight. Any other relevant misconduct findings are also considered.
4	A significant profit-generating offence or other material adverse finding contributes to the customer's ML/TF risk rating and is considered for any SMR reporting (including in relation to representatives, beneficial owners, or persons on whose behalf the customer is acting).

15. Identify beneficial ownership and control

This process sets out how AML Partners traces the ownership and control of a non-individual customer, identifying every entity and individual in the chain through to the natural persons who ultimately own or control the customer.

Steps

AML Partners starts from the customer entity and works through any intermediate layers of ownership and control.

Step	Action Description
1	AML Partners runs ASIC, Ultimate Beneficial Owner (AU), PEP, sanctions and adverse media checks in FlowAML to gather the information needed to identify beneficial owners.
2	AML Partners requests original documents (or reliable copies) showing ownership and control — for example, a company extract, partnership agreement, trust deed, or a certified ownership and control chart. Documents that can change must be no more than 6 months old. Where documents are unavailable or unclear, alternatives are requested and the reason recorded.
3	AML Partners checks the documents are original or reliable copies, current (no more than 6 months old if they can change), and from an independent and reliable source. If authenticity or accuracy is in doubt, AML Partners requests the original, all variations in chronological order, or third-party confirmation. Verification outcomes are recorded along with the documents provided and their source.
4	AML Partners identifies and traces every individual and entity that owns or controls the customer — including through shareholdings, voting rights, practical influence, and the power to appoint or remove directors or trustees. If the customer is a listed public company with public disclosure obligations (e.g. ASX), the process ends here and the findings are recorded.
5	If any owner or controller is another entity (for example, another company or trust), repeat Steps 1 to 3 for each intermediary entity. Keep tracing through each layer until you've identified and documented all individuals who ultimately own or control the customer.
6	AML Partners maps the customer's ownership and control structure against the initial CDD record — for example, as a flow chart or table showing each entity and individual, ownership percentages, and how each beneficial owner exercises control.
7	AML Partners checks whether any part of the structure matches the risk factors in the Risk assessment — such as nominee arrangements, offshore entities, or complex ownership. A nominee is not treated as the beneficial owner; ownership is attributed to the underlying beneficial owner.
8	AML Partners uses the structure to identify any individuals who directly or indirectly own 25% or more of the customer.

Step	Action Description
9	AML Partners identifies any individual exercising control over the customer, regardless of ownership percentage — including through decision-making authority or influence. The tables below provide reference categories of possible owners and controllers.
10	If no beneficial owners can be identified through Steps 8 and 9, or if none exist, we must identify and verify the CEO (or equivalent senior officer) for the customer and record the steps taken to identify beneficial owners, along with the reason why they couldn't be established.
11	AML Partners records the findings and any supporting workings against the initial CDD record.

Supporting information — Documents for each entity type

Entity type	Suggested documents
Body corporate	The company extract or annual statement indicating all shareholders and persons with control (or foreign equivalent); a copy of the constitution, charter or rules; ownership and control charts, if available.
Association	An extract from a register of incorporated associations (if relevant); a distribution of member statements; the constitution or rules; governance chart, if available.
Partnership	A copy of the partnership agreement and any amendments or variations; partnership structure charts, if available.
Trust	The trust deed (or relevant extracts) and any deeds of variation; a disclosure certificate that verifies information about the trust; letters or documents from an independent professional services firm.
Government body	List of individuals with governance responsibility (e.g. board, CEO, secretary); organisation charts, if available.

Supporting information — Possible beneficial owners

Entity type	Beneficial owners
Body corporate	Directors/board members; individuals who own more than 25% of shares; individuals with more than 50% of voting rights; individuals who determine financial or operational decisions (e.g. CEO, managing director).
Partnership	Individuals holding 25% or more of partnership interests; individuals who exercise control over the management, operations or finances; individuals with more than 50% voting rights; general partner in a limited partnership.

Entity type	Beneficial owners
Trust	All trustees who are individuals; for a corporate trustee, individuals who own or control the trustee; any settlors (if they can exercise control); any appointors, protectors, controllers or other individuals with control over elements of the trust. Unit trust: individuals holding 25% or more of units. Discretionary/family trust: individuals entitled to 25% or more of distributions. Bare trust: the beneficiary.
Association	All Responsible People, including members of the governing body, or those directing the strategic direction of the charity; any other individual with authority to direct decisions, access funds or control management and decision making.
Government body	Individuals with primary responsibility for governance and executive decisions (e.g. CEO, department secretary, board of commissioners); authorised signatories.

Personnel processes

16. Obtain a statutory declaration

This process sets out how Teamlink Pty Ltd obtains a statutory declaration from personnel taking on AML/CTF functions, covering any circumstances that may affect their suitability. It is carried out as part of Teamlink Pty Ltd's own HR and pre-employment processes.

Step	Action Description
1	Teamlink Pty Ltd gives the person written information setting out what they must declare — including any serious offence convictions (excluding spent or expunged convictions), other adverse findings, conflicts of interest, and whether they are willing and able to perform the duties of the role.
2	The person completes the statutory declaration — either a Commonwealth declaration or one from their state or territory of residence.
3	Teamlink Pty Ltd checks the declaration is complete and properly witnessed and signed. If anything is missing, the person is asked to correct it.
4	The declaration is retained in Teamlink Pty Ltd's HR system for at least 7 years.

17. Verify personnel identity

This process sets out how Teamlink Pty Ltd verifies the identity of personnel as part of its own HR and pre-employment due diligence.

Step	Action Description
1	Teamlink Pty Ltd carries out the personnel due diligence and records it in its HR system. The information collected includes legal name, any other names known by, date of birth, residential address, a unique identifier (licence or passport number) and any expiry date. Information already held may be used, or collected from the person with their consent.
2	Teamlink Pty Ltd obtains an original or reliable copy of one primary photographic ID document, or two primary non-photographic ID documents.
3	Teamlink Pty Ltd confirms the person's identity — checking their appearance against any photo ID provided, or examining the reference material in any non-photographic ID.
4	If any inconsistencies are identified, the person is asked to provide additional ID documents to resolve them.

Reporting processes

18. Prepare the annual report to the governing body

This process sets out how the AML/CTF compliance officer prepares the annual report to the governing body on how the program is operating and how effective it is.

The report summarises:

- key compliance activities
- testing results
- recommendations for improvement.

Step	Action Description
1	Record the report details: date, period covered, who prepared it, and who reviewed it (if applicable).
2	Set out the key recommendations for the governing body — including any changes to program resources, staffing or risk controls, and any new developments or emerging risks they should be aware of.
3	Summarise the key AML/CTF activities for the period: AUSTRAC communications; changes in ML/TF risk or customer profiles; training delivered; internal or external reviews; breaches identified and action taken; other incidents.
4	Summarise training delivered during the period — including whether it was delivered on time, any capability gaps, and how these were addressed.
5	Summarise the year's reporting: SMRs, TTRs, CBM reports and UARs submitted; internal escalations; high-risk customers; complex customers.
6	Provide an overview and trends for high-risk or complex customers serviced during the period.
7	Note any changes made to the program during the period: updates to the risk assessment; new or revised policies, processes or controls; system or data-handling changes; amendments arising from AUSTRAC feedback or regulatory updates.
8	Summarise the results of testing during the period — including customer onboarding and verification, SMR testing, and TTR testing (covering whether reports were timely, accurate and complete). Include findings from any assurance or independent reviews.
9	Record outcomes and any deficiencies, breaches or recurring issues found during effectiveness testing. Explain how these affect the ability to manage ML/TF risk, and what's been done or is planned to address them.

Step	Action Description
10	Provide a clear statement on: whether the AML/CTF policies are managing and mitigating ML/TF risks effectively; any areas needing review or enhancement; overall risk exposure relative to the ML/TF Risk assessment; and confidence in the effectiveness of the AML/CTF framework.
11	Attach all supporting documents referenced in the report: ML/TF Risk assessment updates; updated policies or process documents; any independent evaluation reports; copies of relevant AUSTRAC communications.
12	Complete the declaration confirming the information is accurate and complete.

19. Prepare and submit the annual compliance report (ACR)

This process sets out how the annual compliance report (ACR) is prepared and submitted to AUSTRAC.

Step	Action Description
1	The compliance officer keeps the agency contact email current in AUSTRAC Online so notifications about the compliance report are received, and schedules a reminder at the start of each calendar year to prepare the report.
2	When AUSTRAC issues the notification, the compliance officer reviews the preview questions to prepare.
3	From 1 January, the compliance officer gathers the information needed, with AML Partners supplying the operational data, and completes the report questions over multiple sittings if needed.
4	The compliance officer reviews the report for accuracy and completeness, submits it to AUSTRAC via AUSTRAC Online by 31 March, provides a copy to the governing body, and retains the report for at least 7 years.

20. Escalate matters to the compliance officer

This process sets out the matters that need to be escalated to the AML/CTF compliance officer, how to escalate them, and what the compliance officer must do in response.

Where the compliance officer detects the trigger themselves, they follow the action steps directly.

Where someone else detects it, they escalate to the compliance officer, who then actions it. Any step without a stated timeframe is completed as soon as practicable.

Escalation triggers and actions

The table below sets out the triggers for escalation and the actions required to escalate matters to the compliance officer for review.

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
Customer is high-risk and/or an SMR will be made, and we decide to continue providing designated services	High-risk customers and transactions are escalated within FlowAML to the senior manager for review and acceptance.	Senior manager approval must be obtained before starting or continuing the designated service. Without approval, no further designated services may be provided.

Escalation trigger	How to escalate	How to action for the AML/CTF compliance officer
Potential suspicious matters	SMR obligations begin from the moment a designated service is provided, proposed or requested. Teamlink Pty Ltd raises an unusual activity report (UAR) in FlowAML where it suspects information may be relevant to an offence, a person isn't who they claim to be, or someone is planning an ML/TF offence. Services are held until directed.	The compliance officer reviews the UAR and submits an SMR where reasonable grounds exist — within 24 hours for terrorism-financing suspicions, or 3 business days for other suspicions. Escalating personnel are told only whether they can continue providing designated services, not about the SMR itself.
Positive sanctions check	Where a sanctions check returns a positive match on the customer, representatives, beneficial owners, or persons on whose behalf the customer is acting, AML Partners escalates the matter in FlowAML with all relevant information. Cease dealing with the customer and their assets, and hold services until directed.	The compliance officer reviews the matter, determines the action, and records the decision and actions in FlowAML.
Cross-border movements (CBM) of bearer negotiable instruments or physical currency	Where an international movement of physical currency or BNIs of $10,000 or more (or foreign-currency equivalent) is identified, Teamlink Pty Ltd completes the relevant form and escalates it to the compliance officer.	The compliance officer reviews the escalation and submits a CBM report via AUSTRAC Online – within 5 business days of currency received from overseas, or before any physical currency or BNIs are sent overseas.
Threshold transactions	Where a transaction involves physical currency of $10,000 or more (or foreign-currency equivalent), Teamlink Pty Ltd completes the relevant form and escalates it to the compliance officer.	The compliance officer reviews the escalation and submits a TTR to AUSTRAC within 10 business days of the transaction.

Program maintenance processes

21. Update country risk ratings

This process sets out how country risk ratings in the Risk assessment are kept up to date.

Step	Action Description
1	AML Partners maintains the country risk assessment in FlowAML, capturing the countries Teamlink Pty Ltd and its customers operate in. Country risk ratings populate automatically based on the Basel AML Index.

22. Update inherent risks and risk ratings

This process sets out how inherent risks and risk factors are added or reassessed in the Risk assessment, and how the appropriate rating is determined. Country risk ratings are covered separately.

Step	Action Description
1	AML Partners performs this in FlowAML's Risk assessment tool.
2	Obtain approval, then record the updates and changes to the Risk assessment in FlowAML.
3	Once approved, the changes are communicated to affected personnel as soon as practicable, with training provided if required. The previous version of the Risk assessment is retained in FlowAML for at least 7 years from the date of change.

23. Receive and action AUSTRAC communications

This process details the steps for receiving, assessing and actioning communications from AUSTRAC.

Step	Action Description
1	The AML/CTF compliance officer will: list themselves as the agency contact person through AUSTRAC Online; subscribe to AUSTRAC guidance updates.
2	If any other personnel receive or identify any communications directly from AUSTRAC, such as a letter, they must forward it to the AML/CTF compliance officer as soon as practicable.
3	Review the communication to determine if it's relevant to the agency's ML/TF risks. If so, review the Risk assessment and affected parts of the AML/CTF program to identify if updates are needed. Record the communication in the table under Risk assessment sources in the Risk assessment.
4	If updates are needed, draft proposed changes in line with the Maintain our AML/CTF program policy. Continue to Step 5. If no updates are needed, document that the communication was considered and the reason no updates are needed. This process is then complete.
5	Submit any proposed changes to the senior manager for review and approval before implementation. If the senior manager rejects proposed changes, record the reasoning and follow the process outlined in Section 4 of the Maintain your AML/CTF program form.
6	Once approved, update the relevant documents, systems and controls. Make sure updates are published and accessible to personnel. Provide communication and training to personnel if required.

24. Arrange an independent evaluation

This process sets out how an independent evaluation of the AML/CTF program is arranged, conducted and finalised.

Step	Action Description
1	Appoint a suitably qualified and independent evaluator and give them access to the relevant AML/CTF policies, systems and records.
2	The evaluator reviews the program for compliance and effectiveness, and provides a written report with findings and recommendations.
3	The evaluator submits the report directly to the senior manager (and the governing body, if separate). The senior manager and governing body review it as soon as practicable. If there are no adverse findings, go to Step 8.
4	Adverse findings are addressed using the independent evaluation response form. Where a finding isn't accepted, the rationale is documented; where accepted, an action plan is developed.
5	The senior manager and governing body document an action plan that categorises the findings, assigns each one to a responsible person, and sets the actions, timelines and responsibilities.
6	Action items are implemented and recorded against the Maintain your AML/CTF program form. The updated program is submitted to the senior manager for approval, then implemented — with personnel training where required.
7	Implemented updates are tested for effectiveness, and a written update is provided to the senior manager and governing body. If they aren't effective, the process repeats from Step 5 until it is.
8	Once complete and all findings addressed, the evaluation is closed and records are saved in the compliance records folder. The next evaluation due date is added to a compliance calendar or register.

25. Enrol and stay current with AUSTRAC

This process sets out how Teamlink Pty Ltd enrols with AUSTRAC and keeps its enrolment details current.

Enrol with AUSTRAC

Step	Action Description
1	Go to the AUSTRAC website to enrol and register.
2	For a new application, select “Sign up to enrol a new agency”. To continue an existing application, sign into AUSTRAC Online.
3	Complete the AUSTRAC Business Profile Form and submit it via AUSTRAC Online within 28 days of first providing a designated service from 1 July 2026. Agencies already providing a designated service on 1 July 2026 must submit by 29 July 2026. Save the confirmation, completed form and related correspondence in the compliance records folder, and notify the governing body that enrolment is complete.

Update AUSTRAC enrolment details

Step	Action Description
1	Sign into the AUSTRAC Online account.
2	Follow the AUSTRAC Online instructions to update the enrolment details.
3	Update the business profile with any new or changed information on designated services or the agency (within 14 days of the change), and the agency’s earnings for the preceding 12 months (within 14 days of any change). Save the confirmation, completed form and related correspondence, and notify the governing body.