Applicant Name:	Leo Tyndall
Application Number:	89562543
Attachment Name:	Anti-Money Laundering and Counter-Terrorism Financing Policy
Number of Pages:	60
Date Prepared:	1/08/2014
Special Status (if any):	

DOCUMENT INFORMATION

Document Name:	Anti-Money Laundering and Counter-Terrorism Financing Policy
Date:	1/08/2014
Document Version	1.0
Author:	Leo Tyndall
Approved:	Board

CHANGE CONTROL

Date:	Version:	Reason for Change:

Anti-Money Laundering and Counter-Terrorism Financing Policy

Tyndall Capital Pty Ltd.

TABLE OF CONTENTS

INTRODUCTION

1. OVERVIEW

1.1 The *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 (**AML/CTF Act**) received Royal Assent on 12 December 2006. The broad purpose of the AML/CTF Act is to regulate financial transactions in a way that will help identify, mitigate and manage money laundering (**ML**) and terrorism financing (**TF**) risks.

1.2 The AML/CTF Act provides general principles and obligations while detailed operating rules are covered in Rules made by the Australian Transaction Reports and Analysis Centre (**AUSTRAC**). AUSTRAC is the government agency responsible for administering the AML/CTF Act.

1.3 Money laundering involves the injection of funds generated from illegal activities into the legitimate financial system in order to hide or disguise the criminal source of those funds. Terrorism financing is the use of money, which may or may not be generated from criminal activity, for financing terrorist activities.

2. ABOUT THE AML/CTF ACT

2.1 The AML/CTF Act applies to persons who provide specified services (known as "designated services"). Persons providing designated services are called "reporting entities".

2.2 The AML/CTF Act adopts a risk-based approach. This approach means that the reporting entity will decide how best to identify, mitigate and manage the risk of money laundering and the financing of terrorism through its business. Reporting entities will therefore need to undertake a comprehensive assessment of these risks relative to their businesses. Reporting entities will need to be able to demonstrate to AUSTRAC that they have carried out such an assessment and have a program in place to identify, mitigate and manage the risk of their products or services being used to facilitate money laundering or the financing of terrorism.

3. SUMMARY OF GENERAL OBLIGATIONS

3.1 From 12 December 2007, reporting entities must:

(a) have and carry out prescribed procedures to verify a customer's identity before providing a designated service;

(b) adopt and maintain an AML/CTF program; and

(c) have an AML/CTF Compliance Manager.

3.2 From 12 December 2008, reporting entities must:

(a) report suspicious matters to the AUSTRAC CEO; and

(b) undertake ongoing customer due diligence.

4. DEFINITIONS

Source of Section Content	
Document	**Sections**
AUSTRAC Guidance Note: Risk management and AML/CTF programs	6.6

4.1 Words and phrases defined in the AML/CTF Act or the AML/CTF Rules have the same meaning when used in the Tyndall AML/CTF Program unless specified otherwise.

4.2 **Politically Exposed Persons (PEPs**): individuals who are or have been entrusted with prominent public functions in a foreign country, for example Heads of State or of government, senior politicians, senior government, judicial or military officials, senior executives of state owned corporations, important political party officials. Business relationships with family members or close associates of PEPs involve risks similar to those with PEPs themselves. The definition is not intended to cover middle ranking or more junior individuals in the foregoing categories. (Financial Action Task Force,

Glossary to the 40 Recommendations).

5. DESIGNATED BUSINESS GROUP

5.1 Tyndall (a **Reporting Entity**) does not currently share obligations with another person, for the purposes of forming a Designated Business Group (DBG) under the AML/CTF Act and the AML/CTF Rules.

5.2 Another entity can join with Tyndall to form a Tyndall DBG if:

(a) that entity is:

(i) related to each other member of the Tyndall DBG within the meaning of section 50 of the *Corporations Act 2001* (Cth); and

(ii) either:

(A) a reporting entity; or

(B) a company in a foreign country which if it were resident in Australia would be a reporting entity; or

(C) providing a designated service pursuant to a joint venture agreement, to which each member of the Tyndall DBG is a party; and

(iii) not a member of another designated business group; or

(b) otherwise permitted by the AML/CTF Act or Rules.

5.3 In order to join the Tyndall DBG, a director or officer of the other entity will need to elect in writing (on behalf of that entity) to be a member of the Tyndall DBG by completing the election form as specified by AUSTRAC at the time. The AML/CTF Compliance Manager will provide the completed form to AUSTRAC in the method specified by AUSTRAC.

5.4 When any of the following changes in the Tyndall DBG occurs, the AML/CTF Compliance Manager must notify the AUSTRAC CEO in writing by completing the approved notification form (see Appendix B of the Tyndall AML/CTF Policy):

(a) a withdrawal of a member from the Tyndall DBG; or

(b) an election of a new member to the Tyndall DBG; or

(c) the termination of the Tyndall DBG; or

(d) any other change in the details previously notified to the AUSTRAC CEO in respect of the Nominated Contact Officer or the Tyndall DBG.

5.5 Any of the changes listed in Section 5.4 must be approved by the Director of Tyndall.

5.6 The AML/CTF Compliance Manager must provide the notification to AUSTRAC no later than 14 business days from the date the change takes effect.

5.7 Members of the Tyndall DBG are referred to as **XXXX** or a **XXXX reporting entity** in this Policy.

6. AML/CTF PROGRAM

6.1 Each Tyndall reporting entity adopts Part A and Part B of this Policy as their joint AML/CTF program (**XXXX AML/CTF Program**) for the purposes of the AML/CTF Act.

7. RECORDS RELATING TO THE Tyndall AML/CTF PROGRAM

7.1 The AML/CTF Compliance Manager will ensure that the following records are retained for each of the Tyndall reporting entities:

(a) this Policy and the Tyndall AML/CTF Program and each variation to them;

(b) Director approval of this Policy and the Tyndall AML/CTF Program and each variation to them;

(c) AUSTRAC feedback and correspondence;

(d) external and internal AML/CTF reviews;

(e) correspondence with external lawyers on AML/CTF issues.

7.2 These records will be retained:

(a) in the case of records relating to the adoption of each variation to this Policy and the Tyndall AML/CTF Program, during the period it or any part of it remains in force and for 7 years after it ceases to be in force;

(b) for the period determined by the AML/CTF Compliance Manager for all other records.

8. AML/CTF COMPLIANCE REPORTING

8.1 The AML/CTF Compliance Manager, on behalf of Tyndall, must submit an AML/CTF Compliance Report to AUSTRAC within 3 months of the end of each reporting period (**Reporting Period**), or otherwise as specified by AUSTRAC.

8.2 The AML/CTF Compliance Report must cover each of Tyndall reporting entity's compliance with the AML/CTF Act and the AML/CTF Rules during the Reporting Period and take the form to be specified by AUSTRAC (if any).

PART A – GENERAL

9. INTRODUCTION

9.1 Part A of the Tyndall AML/CTF Program is designed to identify, mitigate and manage the risk that each Tyndall reporting entity may reasonably face that the provision of its designated services at or through a permanent establishment of that entity in Australia might involve or facilitate money laundering or the financing of terrorism.

10. ANALYSIS OF DESIGNATED SERVICES AND ML/TF RISK

10.1 In determining and putting in place appropriate risk-based systems and controls to identify, mitigate and manage ML/TF risks in Part A of the Tyndall AML/CTF Program, Tyndall has had regard to the following factors in relation to each Tyndall reporting entity:

(a) the nature, size and complexity of its business; and

(b) the type of ML/TF risk that it might reasonably face.

10.2 Tyndall has also considered the following factors when identifying each Tyndall reporting entity's exposure to money laundering and terrorist financing:

(a) customer types;

(b) the types of designated services provided;

(c) the methods by which those services are delivered; and

(d) the country in which those services are delivered.

10.3 Tyndall provides the following designated services (Tyndall **Designated Services**), in line with the provisions of the Tyndall Australian Financial Services Licence:

(a) Item 35 of section 6 of the AML/CTF Act; and

(b) Item 33 of section 6 of the AML/CTF Act.

10.4 Prior to a new service being introduced to the market by Tyndall, the AML/CTF Compliance Manager will assess it to determine whether it involves the provision of a designated service. Where it is determined that a new service involves the provision of a designated service, the AML/CTF Compliance Manager will assess the ML/TF risk involved in the provision of the designated service.

10.5 An assessment of the AML/CTF risk(s) posed to the Compliance Manager must also be conducted for:

(a) All new methods of designated service delivery prior to adopting them (for example, using a non-face-to-face method or the use of electronic funds transfers)

(b) All new or developing technologies used for the provision of a designated service prior to adopting them.

10.6 Director approval must be received before a new designated service is introduced to the market by Tyndall. The Director must be given a copy of the risk assessment conducted under section 10.5 before the approval is granted.

10.7 The following Risk Assessment Matrix takes into account:

(a) the nature, size and complexity of the business of Tyndall; and

(b) the type of ML/TF risk that might be reasonably faced by Tyndall.

Source of risk: AML/CTF Regulatory Risk						
A	Tyndall					
	Identification Type of ML/TF Regulatory Obligation	**Assessment** Likelihood	Impact	**Evaluation** Overall risk	Priority	**Treatment** Risk Mitigation and Control Procedures
A.1	Reporting Suspicious Matters	E	Cat.	Low	High	Refer to section 18 below.
A.2	Customer Identification Requirements	E	Maj.	Low	High	Refer to section 27 below.
A.3	Customer verification not done properly	E	Maj.	Low	High	Refer to section 20 below.
A.4	Failure to train staff adequately	E	Maj.	Low	High	Refer to section 14 below.
A.5	Not having an AML/CTF program	E	Maj.	Low	High	Refer to section 6 above.
A.6	Failure to report suspicious matters	E	Maj.	Low	High	Refer to section 18 below.
A.7	Not submitting an AML/CTF compliance report	E	Maj.	Low	High	Refer to section 8 above.
A.8	Not having an AML/CTF Compliance Manager	E	Maj.	Low	High	Refer to section 12 below.

Source of risk: AML/CTF Business Risk (Inherent and Residual)						
A	Tyndall					
	Identification	**Assessment**		**Evaluation**		**Treatment**
	Type of ML/TF risk	Likelihood	Impact	Overall risk	Priority	Risk Mitigation and Control Procedures

A.1	Customer Types Risk (including any politically exposed persons)	E	Cat.	Low	High	Small institutional client base – easy to monitor Tyndall does not have any politically exposed persons or other companies that pose an immediately obvious ML/TF risk. The AML/CTF Compliance Manager performs KYC procedures. Refer Part B
A.2	Products or Services Risk: Types of Designated Services Provided (Refer to Sections 10.3 for a description of each Designated Service)	E	Maj.	Low	High	Tyndall does not provide designated services that have capacity to directly enable customers to launder money or finance terrorism.
	a)	E	Maj.	Low	High	Refer Section 10.2(d).
	b)	E	Maj.	Low	High	
A.3	Delivery Method Risk: Methods by which Designated Services are Delivered	E	Maj.	Low	High	Email and phone only. Arrange deals only.
A.4	Jurisdiction Risk: Foreign Jurisdictions Dealt with	E	Maj.	Low	High	Tyndall completes KYC forms and processes to review risk posed by the foreign jurisdictions being dealt with. Where risk is assessed as too great, the client is not approved.
A.5	Employees	E	Maj.	Low	High	No employee can directly handle money, only arrange deals. Refer Sections 13 and 14.

A.6 Residual Risk	E	Maj.	Low	High	Ongoing due diligence and regular monitoring of AML/CTF risk profile.

Key

Likelihood of occurrence		Impact if occurred	
A	Almost certain, is expected to occur in most circumstances	Low	Insignificant, no or very low probability that money laundering or terrorism financing will be facilitated.
B	Likely, will probably occur in most circumstances	Min.	Minor probability that money laundering or terrorism financing will be facilitated.
C	Possible, might occur in some circumstances	Mod.	Moderate probability that money laundering or terrorism financing will be facilitated.
D	Unlikely, could occur in some circumstances	Maj.	Major probability that money laundering or terrorism financing will be facilitated.
E	Rare, may occur only in exceptional circumstances	Cat.	Catastrophic, huge loss. Money laundering or terrorism financing will be facilitated.

11. APPLICATION OF PART A

11.1 Part A of the Tyndall AML/CTF Program applies to each Tyndall reporting entity in relation to all areas of its business that are involved in the provision of a designated service, including any functions carried out by a responsible third party.

11.2 The procedures in Part A apply on and from 30 September 2009.

12. AML/CTF COMPLIANCE MANAGER

12.1 The Tyndall Director (**AML/CTF Compliance Manager**):

(a) is the AML/CTF Compliance Manager for the purposes of the AML/CTF Rules; and

(b) is appointed by Tyndall as its Nominated Contact Manager for the purposes of the AML/CTF Rules.

12.2 The Tyndall AML/CTF Compliance Manager will at all times:

(a) be part of the management of Tyndall;

(b) Report directly to the Director of Tyndall; and

(c) Possess sufficient skills and experience to carry out the role of AML/CTF Compliance Manager.

12.3 The Tyndall AML/CTF Compliance Manager is responsible for implementing and over-seeing each Tyndall reporting entity's obligations under the AML/CTF Act and the AML/CTF Rules in accordance with each Tyndall reporting entity's compliance procedures.

12.4 The Tyndall AML/CTF Compliance Manager is authorised to delegate any of its responsibilities under the Tyndall AML/CTF Program, the AML/CTF Act or the AML/CTF Rules to another Tyndall employee, agent or responsible third party provided it is reasonable to do so. The AML/CTF Compliance Manager's responsibilities under to be undertaken in conjunction with an external compliance consultant.

13. EMPLOYEE DUE DILIGENCE PROGRAM

13.1 New Employees

(a) The AML/CTF Compliance Manager must be informed of all prospective new employees before they are issued with an employment contract.

(b) For all newly created roles or previously existing roles that are to be filled with a new employee, a risk assessment must be undertaken of that role to determine whether they will be in a position to facilitate the commission of a money laundering or terrorism financing offence.

(c) In respect of all prospective employees who, if employed (to fill a newly created role that is able to facilitate a ML/TF transaction, or a previously-existing role that is now able to facilitate a ML/TF transaction), may be in a position to facilitate the commission of a money laundering or terrorism financing offence in connection with the provision of an Tydall Designated Service, the AML/CTF Compliance Manager will, at its discretion:

(i) collect information about and verify the identity of the employee in accordance with Part B as if they were a new individual customer;

(ii) obtain a copy of the prospective employee's visa where the employee is not an Australian citizen; and

(iii) carry out at least two reference checks; and

(iv) obtain copies of all tertiary educational qualifications or, if none, the person's highest educational qualification; and

(v) carry out a criminal history check with the Australian Federal Police (subject to (e) below); and

(vi) carry out a credit check.

(d) Steps (i), (ii) and (iii) in (a) above will be carried out for all prospective employees regardless of their position in Tyndall.

(e) Steps (iv) and (v) will be carried out at the discretion of the AML/CTF Compliance Manager having regard to the ML/TF risk associated with the position of the prospective employee and the ability of the employee to directly deal in cash and securities.

(f) The procedures in section 13.1 will be carried out before an employment offer is made unless the AML/CTF Compliance Manager decides otherwise having regard to the reason why they cannot be completed beforehand and the ML/TF risk associated with the position of the prospective employee.

(g) If a prospective employee fails, without reasonable excuse, to comply with these procedures, then Tyndall may decide not to offer that person employment.

(h) Employment contracts issued after 19 January 2009 will include a clause stating that employment within Tyndall is conditional on passing the checks outlined in the Tyndall AML/CTF Policy.

(i) If an offer of employment has already been made, and the prospective employee does not co-operate with the above procedures or the results of the checks are not satisfactory, then Tyndall may withdraw the offer.

13.2 Existing Employees

(a) Where it is proposed that an employee will be transferred or promoted to a new role, a risk assessment must be undertaken of that role to determine whether they will be in a position to facilitate the commission of a money laundering or terrorism financing offence.

(b) Where an employee is transferred or promoted to a role that may put them in a position to facilitate the commission of a money laundering or terrorism financing offence in connection with the provision of an Tyndall Designated Service, the AML/CTF Compliance Manager will:

(i) obtain an updated copy of the employee's visa where the employee is not an Australian citizen; and

(ii) carry out any other identification, reference, criminal history checks with the Australian Federal Police or credit checks that are deemed necessary by the AML/CTF Compliance Manager.

(c) Employees who fail to comply with the procedures above will be reported to the Tyndall Director. Appropriate disciplinary action, including termination of employment, will occur where it is deemed necessary.

13.3 Copies of employee checks undertaken in accordance with this section will be kept in accordance with the Tyndall Document Retention Policy.

13.4 Managing Non-Compliance

(a) Tyndall will, on an ongoing basis, monitor its employees' compliance with the Tyndall AML/CTF Program.

(b) The compliance of employees with the Tyndall AML/CTF Program will be monitored in a number of ways and may include, subject to applicable laws, surveillance of an employee's activities in the workplace.

(c) An employee who fails to comply with the Tyndall AML/CTF Program will be reported to the Tyndall Director. Appropriate disciplinary action, including termination of employment, will occur where it is deemed necessary.

14. RISK AWARENESS TRAINING PROGRAM

14.1 The Risk Awareness Training Program is designed to ensure each employee of Tyndall receives appropriate ongoing training on the ML/TF risk that each Tyndall reporting entity may face.

14.2 The Risk Awareness Training Program is designed to enable Tyndall employees to understand:

(a) the obligations of the relevant Tyndall reporting entity under the AML/CTF Act and Rules;

(b) the consequences of non-compliance with the AML/CTF Act and Rules;

(c) the type of ML/TF risk that the relevant Tyndall reporting entity might face and the potential consequences of such risk; and

(d) those processes and procedures provided for by the Tyndall AML/CTF Program that are relevant to the work carried out by the employee.

14.3 Ongoing Compliance Training

(a) An external compliance consultant may be used to provide regular updates on compliance issues, including AML/CTF and AUSTRAC issues.

(b) These updates are made available to all employees of Tyndall.

14.4 Employee AML/CTF Seminars

(a) The AML/CTF Compliance Manager may organise AML/CTF seminars covering the AML/CTF issues faced by Tyndall. In particular, the seminars will cover issues (c) and (d) in Section 14.2 of this Policy.

(b) The AML/CTF seminars will be conducted as determined by the AML/CTF Compliance Manager. For new employees and employees on leave, a separate seminar may be conducted within a reasonable time of employment commencing if the AML/CTF Compliance Manager determines that that is necessary having regard to the ML/TF risk associated with the position of the employee or prospective employee.

(c) A record will be kept of each employee who attends an AML/CTF seminar in accordance with the Tyndall Document Retention Policy.

(d) At the discretion of the AML/CTF Compliance Manager, additional seminars will be conducted to ensure that all employees remain aware of and up to date with changes in the AML/CTF legislation and requirements.

(e) Non-attendance at an AML/CTF seminar by an employee, without reasonable excuse, will be reported to the Tyndall Director and appropriate disciplinary action will be taken at the request of the AML/CTF Compliance Manager.

(f) Some employees, depending on the nature of their role and responsibilities, may be required to undertake additional training as directed by the AML/CTF Compliance Manager from time to time.

(g) The AML/CTF Compliance Manager will make a current copy of the Tyndall AML/CTF Program available for all employees of Tyndall.

14.5 Document Retention Policy

(a) The AML/CTF Compliance Manager will require:

(i) each new employee of Tyndall to read a copy of the Tyndall Document Retention Policy within a reasonable time of their employment commencing; and

(ii) each employee of Tyndall to read a copy of the Tyndall Document Retention Policy on a regular basis as determined by the AML/CTF Compliance Manager.

(b) Employees who fail, without reasonable excuse, to read the Tyndall Document Retention Policy will be reported to the Tyndall Director and appropriate disciplinary action will be taken at the request of the AML/CTF Compliance Manager.

15. OUTSOURCING

15.1 Where Tyndall outsources any of its AML/CTF obligations, it will:

(a) have an agreement in place with the party to whom the activities are outsourced;

(b) where relevant, require the parties to whom the activities are outsourced to implement policies and procedures similar to those outlined in this AML/CTF Program;

(c) assess the ML/TF risk associated with the outsourcing of the particular activity;

(d) conduct due diligence on the activities outsourced to ensure that outsourcing these activities and services is not increasing the ML/TF risk faced by Tyndall;

(e) conduct due diligence on the parties to whom the activities are outsourced to ensure that outsourcing activities to these parties is not increasing the ML/TF risk faced by Tyndall;

(f) ensure that the parties to whom the activities and services are outsourced understand:

(i) the obligations of the relevant Tyndall reporting entity under the AML/CTF Act and Rules;

(ii) the consequences of non-compliance with the AML/CTF Act and Rules;

(iii) the type of ML/TF risk that the relevant Tyndall reporting entity might face and the potential consequences of such risk; and

(iv) those processes and procedures provided for by the Tyndall AML/CTF Program that are relevant to the work carried out by the employee.

16. PROVISION OF DESIGNATED SERVICES THROUGH PERMANENT ESTABLISHMENTS IN FOREIGN COUNTRIES

16.1 Tyndall does not provide designated services through permanent establishments in foreign countries.

16.2 If at any time Tyndall begins to provide designated services at or through permanent establishments in foreign countries, the AML/CTF Compliance Manager will determine which parts of the Tyndall AML/CTF Program will apply to the permanent establishments and will amend the Tyndall AML/CTF Program accordingly.

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

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

(a) the procedures undertaken; and

(b) information obtained in the course of carrying out the procedures; and

17.2 A copy of these records will be retained for at least seven (7) years after Tyndall ceased to provide designated services to the relevant customer.

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

18. SUSPICIOUS MATTER REPORTING

18.1 If an employee or representative of Tyndall suspects that:

(a) an existing, new or potential customer, or the agent of an existing, new or potential customer, is not who they claim to be; or

(b) information about the provision (or prospective provision) of a service to a client may be:

(i) relevant to the investigation or prosecution of a person for:

(A) an offence against a law of the Commonwealth or a State or Territory;

(B) an evasion, or an attempted evasion, of a taxation law (as defined in the *Taxation Administration Act 1953* (Cth)) or a law of a State or Territory that deals with taxation; or

(C) a money laundering or financing of terrorism offence;

(ii) of assistance in the enforcement of laws relating to proceeds of crime; or

(iii) the provision of a service to a client may be preparatory to the commission of a money laundering or a financing of terrorism offence,

the employee who forms the suspicion must **immediately** notify the AML/CTF Compliance Manager of their suspicion.

18.2 Under no circumstances should the employee or representative discuss the matter with any person other than their immediate supervisor, unless authorised by the AML/CTF Compliance Manager.

18.3 If the AML/CTF Compliance Manager receives a notification from an employee or representative under section 18.1, the AML/CTF Compliance Manager must assess the information which led the employee to form a suspicion and determine whether a suspicious matter report should be lodged.

18.4 If the AML/CTF Compliance Manager determines that a suspicious matter report must be lodged in relation to a customer, Tyndall will:

(a) apply the enhanced customer due diligence program outlined in the Tyndall AML/CTF Program; and

(b) report the suspicion to the AUSTRAC CEO:

(i) within 24 hours after the time when the AML/CTF Compliance Manager forms the relevant suspicion, if the matter relates to the financing of terrorism; or

(ii) in all other cases, within 3 business days after the time when the AML/CTF Compliance Manager forms the relevant suspicion.[1]

18.5 If the AML/CTF Compliance Manager is notified of a suspicion relating to the identity of the customer, the AML/CTF Compliance Manager must, within 14 days commencing after the day on which the AML/CTF Compliance Manager was notified of the suspicion, do one of the following for the purpose of enabling the reporting entity to be reasonably satisfied that the customer is the person that he or she claims to be:

(a) collect additional KYC information in respect of the customer;

---

1 Section 42(3)(a) AML/CTF Act

(b) re-verify, from a reliable and independent source, any KYC information that has been obtained in respect of the customer; or

(c) verify, from a reliable and independent source, any previously unverified KYC information that has been obtained in respect of the customer.[2]

18.6 If:

(a) after collecting additional KYC information from a customer in accordance with paragraph 18.5, the AML/CTF Compliance Manager is still not satisfied that the customer is who they claim to be; or

(b) the AML/CTF Compliance Manager is unable to collect any additional information from the customer,

then the AML/CTF Compliance Manager must make a suspicious matter report to AUSTRAC.

18.7 If the AML/CTF Compliance Manager makes a suspicious matter report to AUSTRAC in relation to a customer, the AML/CTF Compliance Manager must also consult with AUSTRAC and other relevant enforcement agencies to determine how best to deal with the customer.

18.8 A report to the AUSTRAC CEO of any of the matters set out at Section 18.1 must be in the approved form and sent in accordance with the requirements of the AML/CTF Act and Rules.

18.9 A representative of Tyndall must not disclose to someone other than the AUSTRAC CEO or a member of the staff of AUSTRAC:

(a) that Tyndall has reported, or is required to report, information to the AUSTRAC CEO under section 41 of the AML/CTF Act;

(b) that Tyndall has formed a suspicion, under section 41 of the AML/CTF Act, about a transaction or matter;

(c) any other information from which the person to whom the information is disclosed could reasonably be expected to infer that information has been communicated to the AUSTRAC CEO under section 41 of the AML/CTF Act or the suspicion has been formed; or

(d) that information or documentation has been given or produced under section 49 of the AML/CTF Act.

18.10 If the AML/CTF Compliance Manager, on behalf of Tyndall, forms a reasonable suspicion relating to one of the matters set out in Section 18.1 in respect of an existing customer (that is, a person who was a customer of Tyndall as at 12 December 2007), the AML/CTF Compliance Manager must, within 14 days commencing after the day on which the AML/CTF Compliance Manager formed the suspicion, carry out the applicable customer identification procedures in Part B of this AML/CTF Program unless the AML/CTF Compliance Manager determines that Tyndall has previously carried out or been deemed to have carried out that procedure or a comparable procedure.

18.11 The AML/CTF Compliance Manager must examine the background, purpose and circumstances of suspicious matters that they have detected and reported and determine whether any changes should be made to the AML/CTF Program. This should occur periodically (at least annually) and whenever a particularly unusual suspicious matter is identified.

---

2 Section 35 AML/CTF Act; Rules Part 6.2.

19. REQUEST TO OBTAIN INFORMATION FROM A CUSTOMER

19.1 Where an Tyndall reporting entity has provided or is providing a designated service to a customer and the AML/CTF Compliance Manager believes, on reasonable grounds, that a customer has information that may assist Tyndall in the identification, management and mitigation of ML/TF risk, the AML/CTF Compliance Manager may request that the customer provide Tyndall with any such information. The request must be provided in writing to the customer and notify the customer that if the customer does not comply with the request, Tyndall may do any or all of the following until the customer provides the information covered by the request:

(a) refuse to continue to provide a designated service;

(b) refuse to commence to provide a designated service; or

(c) restrict or limit the provision of the designated service to the customer.

19.2 If the customer does not comply with the request within a reasonable time then the AML/CTF Compliance Manager may determine that, until the customer provides the information covered by the request, Tyndall will:

(a) refuse to continue to provide the designated service;

(b) refuse to commence to provide the designated service; or

(c) restrict or limit the provision of the designated service to the customer.

19.3 In these circumstances, the AML/CTF Compliance Manager will determine whether the matter should be reported to AUSTRAC as a suspicious matter (see Section 18).

20. ONGOING CUSTOMER DUE DILIGENCE - OVERVIEW

20.1 Tyndall will monitor its customers with a view to identifying, mitigating and managing the risk that the provision of a designated service by a Reporting Entity at or through a permanent establishment in Australia may involve or facilitate money laundering or terrorism financing.

20.2 Tyndall will monitor its customers by implementing systems to:

(a) collect further KYC information for ongoing customer due diligence processes;

(b) update and verify KYC information for ongoing customer due diligence purposes;

(c) monitor the transactions of customers; and

(d) conduct enhanced customer due diligence in respect of high risk customers and customers about whom a suspicion has been formed.

20.3 As part of implementing systems for ongoing customer due diligence purposes, Tyndall will group its customers according to their level of risk assessed as part of the risk assessment procedures outlined in the Tyndall AML/CTF Program. The risk grouping will determine:

(a) what further KYC information needs to be collected for ongoing customer due diligence purposes in respect of a particular customer;

(b) what level of transaction monitoring needs to be conducted in relation to a customer; and

(c) whether the enhanced customer due diligence program needs to be applied.

21. ADDITIONAL KYC INFORMATION

21.1 In undertaking the risk assessment for new activities and technologies referred to in Section 10, the AML/CTF Compliance Manager will determine whether any additional KYC information should be collected from relevant customers either before any designated service is provided to the customer or during the course of the Reporting Entity's relationship with the customer. These requirements will be incorporated in the relevant customer procedures.

21.2 Based on the assessed level of ML/TF risk involved in the provision of designated services provided by Tyndall on the date that this Section of the Tyndall AML/CTF Program was adopted, Tyndall has determined that no additional KYC information needs to be collected in relation to low risk customers. The AML/CTF Compliance Manager will determine what additional KYC information will be collected in respect of medium and high risk customers prior to the provision of any designated service to assist Tyndall to undertake ongoing customer due diligence.

21.3 The additional KYC information will be collected at the same time as and in the same manner as KYC information required to be collected under Part B. Failure to provide additional KYC information will be treated in the same way as the failure to provide any other KYC information collected under Part B.

21.4 Tyndall will update and re-verify KYC information in respect of a customer where:

(a) the AML/CTF Compliance Manager considers that KYC information held in respect of a customer is likely to be incomplete or unreliable;

(b) a representative of a Reporting Entity becomes aware that KYC information held in respect of a customer has or is likely to have changed;

(c) the customer engages in a significant transaction or series of transactions with one or more Reporting Entities, where a significant transaction occurs if a transaction, or series of transactions conducted within any calendar month exceeds $100,000,000 in value; or

(d) a significant change occurs in the way the customer conducts transactions, where a significant change occurs if the number of transactions carried out by a customer increases by 100% within a 5 day period.

21.5 Where one of the above circumstances arises in respect of a customer and the applicable customer identification procedure has not previously been carried out in respect of a customer (ie. the customer is a pre-commencement customer), Tyndall will carry out the applicable customer identification procedure in accordance with Part B of the Tyndall AML/CTF Program and collect the relevant additional KYC information.

21.6 Where a change in customer information relates to:

(a) in the case of individual customers, the customer's:

(i) name;

(ii) date of birth; or

(iii) residential address;

(b) in the case of a company:

(i) the company's name; or

(ii) the company's registration number;

(c) in the case of a trust:

(i) the trustee; or

(ii) the name of the trust; and

(d) in the case of a partnership, the identity of a partner.

Tyndall will seek to verify the updated KYC information using reliable and independent documentation in accordance with Section 62.

22. TRANSACTION MONITORING PROGRAM

22.1 This Section describes the transaction-monitoring program adopted by Tyndall which includes risk-based systems and controls to monitor the transactions of customers, for the purpose of identifying any transaction that appears to be suspicious under section 41 of the AML/CTF Act (see Section 18).

22.2 The AML/CTF Compliance Manager must identify ML/TF risk factors relevant to customers of particular services and products provided by the relevant Reporting Entity which may involve the provision of a designated service and to representatives of such customers. Such risk factors include:

(a) the value of the transaction exceeds $100,000,000;

(b) the volume of transactions conducted by a customer within a 5 day period has increased by more than 100%;

(c) the transaction involves foreign countries, customers or third parties against whom sanctions have been imposed or have been included on the lists:

(i) maintained by the Department of Foreign Affairs and Trade under the *Charter of United Nations (Terrorism and Dealings with Assets) Regulations 2002* (Cth);

(ii) maintained by the Reserve Bank of Australia under the *Banking (Foreign Exchange) Regulations 1959* (Cth);

(iii) contained in the *Criminal Code Regulations 2002* (Cth); or

(d) the transaction involves a customer or third party who is a Politically Exposed Person (see Section 65).

22.3 In addition to the Risk Awareness Training required by Section 14, the AML/CTF Compliance Manager will ensure that all employees of Tyndall who have direct contact with customers or their representatives receive regular training in the identification of relevant ML/TF risk factors.

22.4 An employee of Tyndall must immediately inform the AML/CTF Compliance Manager when he or she identifies a ML/TF risk factor in relation to a customer or a customer's representative.

22.5 Where an employee of Tyndall identifies a customer or third party of a kind specified in Section 22.2(c) or 22.2(d), the AML/CTF Compliance Manager will take such action as is necessary, including seeking further information from the customer or their representative or from another source, to determine, with a reasonable degree of certainty, whether the customer or third party is that person and take appropriate action.

22.6 If it is determined, as a result of transaction monitoring, that:

(a) a customer should be placed in a higher risk grouping, Tyndall will collect additional KYC information if required by Section 21;

(b) KYC information needs to be updated or verified in respect of a customer, Tyndall will update or verify the required information in accordance with Section 21;

(c) a customer is a high risk customer, Tyndall will apply the enhanced customer due diligence program in accordance with Section 23; or

(d) a suspicious matter report needs to be lodged in respect of a customer, Tyndall will follow the procedure outlined in Section 18 of the Tyndall AML/CTF Program.

23. ENHANCED CUSTOMER DUE DILIGENCE PROGRAM 23.1

Where the AML/CTF Compliance Manager determines that:

(a) the ML/TF risk associated with a particular designated service, customer, delivery method or jurisdiction is high, including but not limited to when the customer:

(i) is engaged in business that involves a significant number of cash transactions or amounts of cash;

(ii) uses a complex business ownership structure for no apparent commercial or other legitimate reason, especially if the beneficial owners of the legal entity cannot be determined;

(iii) is based in, or conducts business through or in, a high-risk jurisdiction;

(iv) cannot provide information to verify the source of funds;

(v) requests an undue level of secrecy in relation to a designated service;

(vi) is a politically exposed person; or

(b) a suspicion has arisen for the purposes of section 41 of the AML/CTF Act (see Section 18),

The AML/CTF Compliance Manager will arrange for one or more of the following to occur:

(c) seek further information from the customer or from third party sources in order to:

(i) clarify or update the customer's KYC information in accordance with Section 21;

(ii) obtain any further KYC information in accordance with Section 21;

(iii) clarify the nature of the customer's ongoing business with the reporting entity; and

(iv) consider any suspicion that may have arisen for the purposes of section 41 of the AML/CTF Act (see Section 18);

(d) conduct more detailed analysis in respect of the customer's KYC information;

(e) verify or re-verify KYC information in accordance with the customer identification program outlined in Part B of the Tyndall AML/CTF Program;

(f) conduct more detailed analysis and monitoring in respect of the customer's activities and transactions – both past and future; or

(g) consider whether a suspicious matter report ought to be lodged in accordance with section 41 of the AML/CTF Act (see Section 18).

24. REVIEW OF THE Tyndall AML/CTF PROGRAM

Source of Section Content

Document	Sections
AUSTRAC Guidance Note: Risk management and AML/CTF programs	4.7, 8.4

24.1 The AML/CTF Compliance Manager must regularly assess Tyndall's ML/TF risk and should take steps to have the Tyndall AML/CTF Program modified appropriately:

(a) where the AML/CTF Compliance Manager identifies that there has been a significant change in the ML/TF risk relating to designated services provided by a Tyndall reporting entity;

(b) prior to Tyndall introducing a new designated service to the market;

(c) prior to Tyndall adopting a new method of delivering a designated service; and

(d) prior to Tyndall adopting a new technology or developing technology used for the provision of an existing or new designated service.

24.2 Internal

(a) Due to the small number of staff members at Tyndall, internal reviews will not be carried out unless the AML/CTF Compliance Manager considers it necessary or subject to part (b) below. However, an internal review must take place at least annually once Tyndall has sufficient scale (revenues > $100,000).

(b) Internal reviews may be carried out where required by the Tyndall Director.

(c) The internal party conducting the review should:

(i) Have unlimited access to the records, personnel and property of Tyndall within the context of Tyndall's obligations under the *Privacy Act 1988*; and

(ii) Be impartial and objective in performing their duties and should not be inappropriately influenced by management of Tyndall.

(d) The AML/CTF Compliance Manager will report the results of the internal review to the Director of Tyndall.

(e) The internal review will:

(i) assess the effectiveness of Part A of the Tyndall AML/CTF Program having regard to the ML/TF risk of each entity in the Tyndall;

(ii) assess whether Part A of the Tyndall AML/CTF Program complies with the AML/CTF Rules;

(iii) assess whether Part A of the Tyndall AML/CTF Program has been effectively implemented;

(iv) assess whether each reporting entity in Tyndall has complied with Part A of the Tyndall AML/CTF Program;

(v) assess the risk management resources available to Tyndall including, but not limited to:

(A) Funding; and

(B) Staff allocation;

(vi) identify any future needs relevant to the nature, size and complexity of Tyndall; and

(vii) assess the ongoing risk management procedures and controls in order to identify any failures.

(f) When assessing ongoing risk management procedures and controls in order to identify any failures, the internal party conducting the review may have regard to:

(i) any market information relevant to the global AML/CTF environment which may have an impact on the ML/TF risk faced by Tyndall;

(ii) failure to include all mandatory legislative components in the Tyndall AML/CTF Policy;

(iii) failure to gain approval from the Tyndall Director of the Tyndall AML/CTF Program;

(iv) insufficient or inappropriate employee due diligence;

(v) frequency and level of risk awareness training not aligned with potential exposure to AML/CTF risk(s);

(vi) changes in business functions which are not reflected in the Tyndall AML/CTF program (for example, the introduction of a new product or distribution channel);

(vii) failure to consider feedback from AUSTRAC (for example, advice regarding an emerging AML/CTF risk);

(viii) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the Tyndall AML/CTF Program;

(ix) legislation incorrectly interpreted and applied in relation to a customer identification procedure;

(x) customer identification and monitoring systems, policies and procedures that fail to:

(A) prompt, if appropriate, for further identification and/or verification to be carried out when the AML/CTF risk posed by a customer increases;

(B) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;

(C) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;

(D) take appropriate action where the identification document provided is neither an original nor a certified copy;

(E) recognise foreign identification issued by a high-risk jurisdiction;

(F) record details of identification documents, for example, the date of issue;

(G) consult appropriate resources in order to identify high-risk customers;

(H) identify when an expired or old identification document (for example, a driver's licence) has been used;

(I) collect any other name(s) by which the customer is known;

(J) be subject to regular review.

(xi) Lack of access to information sources to assist in identifying higher risk customers (and the jurisdiction in which they may reside), such as PEPs, terrorists and narcotics traffickers;

(xii) Lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:

(A) Customer identification policies, procedures and systems; and

(B) Identifying potential AML/CTF risks

(xiii) Assess the acceptance of documentation that may not be readily verifiable.

(g) If the AML/CTF Compliance Manager determines it is appropriate, the internal review may also:

(i) assess whether the risk-based procedures and processes adopted in the Tyndall AML/CTF Program have changed such that alterations need to be made to the Tyndall AML/CTF Policy;

(ii) assess whether Part B of the Tyndall AML/CTF Program is sufficient to cover the ML/TF risks posed by existing and potential customers of Tyndall; and

(iii) assess whether any additional changes need to be made to the Tyndall AML/CTF Program as a result of changes to AML/CTF regulations and legislation and the AML/CTF environment generally.

24.3 External

(a) The AML/CTF Compliance Manager will arrange for the Tyndall AML/CTF Program to be reviewed by an external party on an annual basis once Tyndall reaches sufficient scale (revenues > $100,000) or more frequently, subject to changes to the risk profile of Tyndall, legislative developments and market information regarding ML/TF risk. Additional external reviews may be carried out where the AML/CTF Compliance Manager considers it necessary.

(b) The AML/CTF Compliance Manager will report the results of the external review to the Director of Tyndall.

(c) The external review will:

(i) assess the effectiveness of Part A of the Tyndall AML/CTF Program having regard to the ML/TF risk of Tyndall;

(ii) assess whether Part A of the Tyndall AML/CTF Program complies with the AML/CTF Rules;

(iii) assess whether Part A of the Tyndall AML/CTF Program has been effectively implemented;

(iv) assess whether Tyndall has complied with Part A of the Tyndall AML/CTF Program;

(d) The AML/CTF Compliance Manager may also require the external party conducting the review to:

(i) assess the ongoing risk management procedures and controls to identify any failures including, but not limited to:

(A) failure to include all mandatory legislative components in the Tyndall AML/CTF Policy;

(B) failure to gain approval from the Tyndall Director of the Tyndall AML/CTF Program;

(C) insufficient or inappropriate employee due diligence;

(D) frequency and level of risk awareness training not aligned with potential exposure to AML/CTF risk(s);

(E) changes in business functions which are not reflected in the Tyndall AML/CTF program (for example, the introduction of a new product or distribution channel);

(F) failure to consider feedback from AUSTRAC (for example, advice regarding an emerging AML/CTF risk);

(G) failure to undertake independent review (at an appropriate level and frequency) of the content and application of the Tyndall AML/CTF Program;

(H) legislation incorrectly interpreted and applied in relation to customer identification procedures;

(I) customer identification and monitoring systems, policies and procedures that fail to:

(I) prompt, if appropriate, for further identification and/or verification to be carried out when the AML/CTF risk posed by a customer increases;

(II) detect where a customer has not been sufficiently identified and prevent the customer from receiving the designated service;

(III) take appropriate action where a customer provides insufficient or suspicious information in relation to an identification check;

(IV) take appropriate action where the identification document provided is neither an original nor a certified copy;

(V) recognise foreign identification issued by a high-risk jurisdiction;

(VI) record details of identification documents, for example, the date of issue;

(VII) consult appropriate resources in order to identify high-risk customers;

(VIII) identify when an expired or old identification document (for example, a driver's licence) has been used;

(IX) collect any other name(s) by which the customer is known;

(X) be subject to regular review.

(J) Lack of access to information sources to assist in identifying higher risk customers (and the jurisdiction in which they may reside), such as PEPs, terrorists and narcotics traffickers

(K) Lack of ability to consistently and correctly train staff and/or third parties, particularly in areas with high turnover in:

(I) Customer identification policies, procedures and systems; and

(II) Identifying potential AML/CTF risks

(ii) Assess the acceptance of documentation that may not be readily verifiable.

(iii) Assess the risk management resources available to Tyndall including, but not limited to:

(I) Funding; and

(II) Staff allocation

(iv) Identify any future needs relevant to the nature, size and complexity of Tyndall.

(e) If the external reviewer determines it is appropriate, the external review may also:

(i) assess whether the risk-based procedures and processes adopted in the Tyndall AML/CTF Program have changed such that alterations need to be made to the Tyndall AML/CTF Policy;

(ii) assess whether Part B of the Tyndall AML/CTF Program is sufficient to cover the ML/TF risks posed by existing and potential customers of Tyndall; and

(iii) assess whether any additional changes need to be made to the Tyndall AML/CTF Program as a result of changes to AML/CTF regulations and legislation and the AML/CTF environment generally.

25. AUSTRAC FEEDBACK

Source of Section Content	
Document	**Sections**
AUSTRAC Guidance Note: Risk management and AML/CTF programs	8.5

25.1 Where AUSTRAC provides a Tyndall reporting entity with feedback regarding performance on the management of ML/TF risk, the AML/CTF Compliance Manager will assess AUSTRAC's feedback to determine if any changes to the Tyndall AML/CTF Program are required and implement any such changes as soon as reasonably practicable, subject to complying with the procedures in Section 26.

26. OVERSIGHT BY THE DIRECTOR / UPDATING THE PROGRAM

26.1 The Tyndall AML/CTF Program is approved by the Director of Tyndall.

26.2 The AML/CTF Compliance Manager will report to the Director of Tyndall on a regular basis in relation to:

(a) significant changes to the ML/TF risks affecting Tyndall reporting entities;

(b) compliance with the AML/CTF Program, the AML/CTF Act and the AML/CTF Rules by the Tyndall reporting entity;

(c) the results of and any report produced for any internal or external review of the Tyndall AML/CTF Program;

(d) any AUSTRAC feedback; and

(e) changes to relevant legislation.

26.3 The AML/CTF Compliance Manager will propose amendments to the Tyndall AML/CTF Program when required by the Program, by the AML/CT Act or Rules or as a result of any of the matters in paragraph 26.2. Subject to paragraph 26.4, such amendments should be considered and approved by the Director of Tyndall before they become effective.

26.4 The AML/CTF Compliance Manager can implement a change to the Tyndall AML/CTF Program immediately if the AML/CTF Compliance Manager believes that the change needs to be made before Director approval can occur. In these circumstances, the AML/CTF Compliance Manager should seek Director approval of the change as soon as reasonably practical after it is made.

PART B – CUSTOMER IDENTIFICATION

27. INTRODUCTION

27.1 **Part B** of the Tyndall AML/CTF Program sets out the customer identification procedures for Tyndall's customers.

27.2 These procedures include:

(a) prescribed processes for the collection and verification of "Know Your Customer Information" (**KYC Information**); and

(b) risk based systems and controls to determine what (if any) other information will be collected and verified in relation to a customer, having regard to the ML/TF risk relevant to the provision of Tyndall's Designated Services.

27.3 Tyndall will consider the following factors when identifying its exposure to money laundering and terrorist financing and developing its customer identification procedures:

(a) customer types

(b) the types of designated services provided;

(c) the methods by which those services are delivered; and

(d) the country in which those services are delivered.

28. APPLICATION OF PART B

Source of Section Content	
Document	**Sections**
AUSTRAC Guidance Note: Risk management and AML/CTF programs	9.1, 9.2, 9.3

28.1 Part B of the Tyndall AML/CTF Program applies to each Tyndall reporting entity, including any functions carried out by a responsible third party.

28.2 The procedures set out in Part B apply on and from 12 December 2007, except in relation to customers to whom the relevant Tyndall reporting entity has provided designated services prior to 12 December 2007 (**existing customers**).

29. KNOW YOUR CUSTOMER – CUSTOMER IDENTIFICATION AND VERIFICATION PROCEDURES

29.1 These procedures must be carried out by an Tyndall reporting entity or a responsible third party:

(a) prior to commencing to provide a designated service to a customer (other than an existing customer), unless Tyndall has already carried out the applicable customer identification procedure in respect of the customer; and

(b) by the Tyndall employee responsible for the customer (or another Tyndall employee on their behalf) unless the AML/CTF Compliance Manager authorises that they can be conducted by an external party.

29.2 The same KYC procedures will be applied across all Tyndall customers in order to ensure that additional procedures do not need to be carried out where a customer uses more than one Tyndall Designated Service.

30. KNOW YOUR CUSTOMER – CONSIDERATIONS

Source of Section Content	
Document	**Sections**
AUSTRAC Guidance Note: Risk management and AML/CTF programs	6.5

30.1 Once information relating to a customer has been collected and verified, Tyndall will re-assess the ML/TF risk posed by the customer.

30.2 In re-assessing the AML/CTF Customer Type Risk for each entity in Tyndall, the entity may consider, where appropriate and among other factors, whether:

(a) The customer is involved in a complex business ownership structure with no legitimate commercial rationale;

(b) The non-individual customer (for example, a trust, company or partnership) has a complex business structure with little commercial justification, which obscures the identity of ultimate beneficiaries of the customer;

(c) The customer is in a position which may expose them to the possibility of corruption;

(d) The customer is based in, or conducting business through or in, a high-risk jurisdiction;

(e) The customer is engaged in business which involves significant amounts of cash;

(f) There is no clear commercial rationale for the customer seeking the designated service;

(g) The customer is a PEP;

(h) An undue level of secrecy is requested regarding a designated service;

(i) The source of funds is difficult to verify;

(j) The beneficial owners of a non-individual customer are difficult to identify and/or verify;

(k) The beneficial owners of the non-individual customer are resident in a high-risk jurisdiction;

(l) There is a one-off transaction in comparison with an ongoing business relationship or series of transactions;

(m) A designated service can be used for money laundering or terrorism financing (and the extent to which it can be used)

(n) The customer makes or accepts payments (for example, electronic transfers) to or from accounts which have not been identified by the reporting entity;

(o) The customer makes or accepts payments (for example, electronic transfers) to or from offshore accounts;

(p) The customer makes withdrawal, transfer or drawdown instructions by phone or fax;

(q) The customer has access to offshore funds (for example, cash withdrawal or electronic funds transfer);

(r) The customer when migrating from one designated service to another carries a different type and level of AML/CTF risk;

(s) The customer has income which is not employment-based or from a regular known source;

(t) The customer is new rather than having a long-term and active business relationship with the reporting entity;

(u) The customer's business or provision or designated services is primarily of a money remittance service nature;

(v) The customer's business is registered in a foreign jurisdiction with no local operations or domicile;

(w) The customer's business is an unregistered charity, foundation or cultural association;

(x) The designated services provided to the customer are primarily of a private banking and/or wealth management kind;

(y) The customer is represented by another person, such as under a power of attorney.

31. INDIVIDUALS: CUSTOMER IDENTIFICATION PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	4.2

31.1 Where a new customer is an individual (other than an individual who notifies the reporting entity that he or she is a customer of Tyndall in his or her capacity as a sole trader), Tyndall must collect, at a minimum, the following information:

(a) The customer's full name;

(b) The customer's date of birth; and

(c) The customer's residential address.

31.2 Where a new customer notifies Tyndall that he or she is a customer in his or her capacity as a sole trader, Tyndall must collect, at a minimum, the following information:

(a) The customer's full name;

(b) The customer's date of birth;

(c) The full business name (if any) under which the customer carries on his or her business;

(d) The full address of the customer's principal place of business (if any) or the customer's residential address; and

(e) Any ABN issued to the customer.

31.3 Where the ML/TF risk posed by the provision of a designated service to a particular individual is assessed as medium or high under Section 30.1, the AML/CTF Compliance Manager may require the Tyndall employee responsible for the customer will collect one or more of the following pieces of information:

(a) any alias names used by the customer;

(b) the customer's occupation or business activities;

(c) the source of the customer's funds including the origin of funds;

(d) income and assets of the customer;

(e) the nature and level of the customer's intended transaction behaviour;

(f) the beneficial ownership of the funds used by the customer/the customer's account with the reporting entity; and

(g) details of the customer's employment (e.g. name of employer, length of employment, type of institution).

31.4 The information collection requirements in this section are not intended to conflict with any other obligation Tyndall has under other legislation including the *Privacy Act 1998.* Any conflicts that arise should be immediately notified to the AML/CTF Compliance Manager.

32. INDIVIDUALS: VERIFICATION – PRINCIPLES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.2

32.1 These procedures do not apply to Tyndall's customers prior to 12 December, 2007.

32.2 At a minimum, the following KYC information about a customer in section 31 must be verified:

(a) The customer's full name; and

(b) Either:

(i) The customer's date of birth; or

(ii) The customer's residential address.

32.3 Where it has been determined that the ML/TF risk posed by the provision of a designated service to an individual is medium or high under the assessment carried out under Section 30.1 and additional KYC information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC information that has been collected. The AML/CTF Compliance Manager will determine what additional KYC information will be verified in respect of that customer.

32.4 Information that is required to be verified as indicated in section 32.2 must be based on:

(a) Reliable and independent documentation;

(b) Reliable and independent electronic data; or

(c) A combination of (a) and (b) above.

33. INDIVIDUALS: VERIFICATION – PROCEDURES

Source of Section Content

33.1 The following verification procedures need to be followed for individuals:

(a) Government database verification (section 64)

(b) Politically exposed persons verification (section 65)

(c) Foreign high-risk jurisdiction verification (section 57)

(d) A document identification procedure. (A "standard customer identification procedure' outlined in sections 33.2 and 33.3 should be conducted in all cases where possible.)

33.2 **Standard domestic documentation identification procedure:** The information in section 32.2 can be verified from either an original or certified copy of a current:

(a) Australian driver's licence containing a photograph of the person; or

(b) Australian passport (it is also permissible for a passport to be issued by the Commonwealth to have expired within the preceding 2 years); or

(c) Card issued under a State or Territory law, for the purpose of proving a person's age, containing a photograph of the person in whose name the card is issued.

33.3 **Standard foreign documentation identification procedure:** The information in section 32.2 can be verified from either an original or certified copy of a current:

(a) Original or certified copy of a foreign government issued passport or similar travel document; and

(b) Where any document relied on as part of this procedure is in a language that is not English, it must be accompanied by an English translation prepared by an accredited translator.

33.4 Non-standard customer identification procedures: The procedures in sections 33.5 and 33.6 should only be conducted where:

(a) A "standard customer identification procedure in section 33.2 and 33.3 was unable to be conducted;

(b) The AML/CTF Compliance Manager forms the view that a discrepancy arose from the information collected and verified during a "standard customer identification procedure'; or

(c) Having conducted the "standard customer identification procedure', the AML/CTF Compliance Manager is not reasonably satisfied that the customer is the individual he or she claims to be.

33.5 **Acceptable 'non-standard domestic documentation identification procedure':** An acceptable "non-standard domestic documentation identification procedure' would be based on:

(a) An original or certified copy of –

(i) Australian birth certificate; or

(ii) Australian citizenship certificate; or

(iii) Both:

(A) Pension card issued by Centrelink; and

(B) An original notice issued to an individual, of a kind listed below, that contains the name of the individual and his or her residential address:

(I) Issued by the Commonwealth or a State or Territory within the preceding 12 months that records the provision of financial benefits; or

(II) Issued by the Australian Taxation Office within the preceding 12 months; or

(III) Issued by a local government body or utilities provider within the preceding 3 months that records the provision of services to that address or to that person.

33.6 **Acceptable 'non-standard foreign documentation identification procedure':** In general, Tyndall should be cautious about arranging for the provision of a product or service for a customer that presents foreign based identification that is not a passport. However, in the event the customer has not presented a passport, an example of an acceptable "non-standard foreign documentation identification procedure' would be based on either an original or certified copy of a current:

(a) National Identity Card issued by a foreign government containing a photograph of the person in whose name the card is issued; and

(b) Foreign driver's licence that contains a photograph of the person in whose name it was issued; and

(c) Where any document relied on as part of the procedure is in a language that is not English, it must be accompanied by an English translation prepared by an accredited translator.

33.7 When determining whether to accept non-standard foreign documentation, the AML/CTF Compliance Manager should have regard to the ML/TF risk posed by the provision of a designated service to a customer from that particular foreign country.

33.8 For the purposes of verification of an individual, Tyndall must have regard to the ML/TF risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Manager gives final sign-off as required in Section 66.

34. COMPANIES: CUSTOMER IDENTIFICATION PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.3

34.1 Where a new customer is a company, either domestic or foreign, it is necessary for the Tyndall employee responsible for that customer to be reasonably satisfied that:

(a) the company exists; and

(b) in respect of certain companies, the name and address of any beneficial owner of the company has been provided (see Section 35).

34.2 **Information Collection:** The following KYC Information must be collected by the Tyndall employee responsible for a customer that is a company, at a minimum in order to determine its existence:

(a) in the case of a domestic company:

(i) the full name of the company as registered by ASIC;

(ii) the full address of the company's registered office;

(iii) the full address of the company's principal place of business, if any;

(iv) the ACN/ABN issued to the company;

(v) the AFSL number issued to the company (if relevant);

(vi) whether the company is registered by ASIC as a proprietary or public company; and

(vii) if the company is registered as a proprietary company, the name of each director of the company.

(b) in the case of a registered foreign company:

(i) the full name of the company as registered by ASIC;

(ii) the full address of the company's registered office in Australia;

(iii) the full address of the company's principal place of business in Australia (if any) or the full name and address of the company's local agent in Australia, if any;

(iv) the ARBN issued to the company;

(v) the AFSL number issued to the company (if relevant);

(vi) the country in which the company was formed, incorporated or registered;

(vii) whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company or some other type of company; and

(viii) if the company is registered as a private company by the relevant foreign registration body - the name of each director of the company.

(c) in the case of an unregistered foreign company:

(i) the full name of the company;

(ii) the country in which the company was formed, incorporated or registered;

(iii) whether the company is registered by the relevant foreign registration body and if so:

A. any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;

B. the full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and

C. whether it is registered as a private or public company or some other type of company by the relevant foreign registration body;

(iv) if the company is registered as a private company by the relevant foreign registration body - the name of each director of the company; and

(v) if the company is not registered by the relevant foreign registration body, the full address of the principal place of business of the company in its country of formation or incorporation.

34.3 Where the ML/TF risk posed by the provision of a designated service to a particular company is assessed as medium or high under Section 30.1, the AML/CTF Compliance Manager may require the Tyndall employee responsible for the customer will collect one or more pieces of the following information:

(a) all business names used by the company;

(b) if the company is a public company, the name of each director of the company;

(c) the nature of the business activities conducted by the company;

(d) the source of the customer's funds including the origin of funds;

(e) the nature and level of the customer's intended transaction behaviour;

(f) the name of the company secretary;

(g) the name of the CEO or managing director (if any);

(h) in the case of a foreign company:

(i) the name of the relevant foreign registration body;

(ii) any identification number issued to the company by the relevant foreign registration body;

(i) for an unlisted public company other than an Australian regulated company, the full name and address of each beneficial owner;

(j) in the case of listed companies other than domestic listed companies and companies listed on a recognised foreign stock exchange and their majority owned subsidiaries (**approved listed companies**) and Australian regulated companies, the full name and address of the beneficial owners of the top 20 shareholdings;

(k) details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the company.

34.4 The AML/CTF Compliance Manager may also determine, where the ML/T risk posed by the company is medium or high, that the individuals referred to in Sections 34.3(f) and 34.3(g) must be screened against the lists mentioned in Section 64.1.

34.5 The verification procedures in Section 36 must also be followed, having regard to the ML/TF risk relevant to the provision of the designated service.

35. COMPANIES: CUSTOMER IDENTIFICATION PROCEDURES – BENEFICIAL OWNERS

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.3

35.1 Where a new customer is a company, either domestic or foreign, that is a proprietary or private company (other than a proprietary company that is licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company), it is necessary for the Tyndall employee responsible for the customer to:

(a) collect the information referred to in Section 34 above; and

(b) collect the name and address of each shareholder with holdings of 25% or more (if any).

35.2 The AML/CTF Compliance Manager will determine whether and to what extent any of the information referred to in Section 35.1(b) should be verified in accordance with Section 36, having regard to the ML/TF risk relevant to the provision of the designated service the new customer will be receiving.

35.3 Where a new customer is:

(a) a foreign public company;

(b) a domestic unlisted public company; or

(c) a company that is licensed and subject to the regulatory oversight of a Commonwealth, State or Territory statutory regulator in relation to its activities as a company.

it is necessary for:

(d) the Tyndall employee responsible for a customer to collect the information referred to in Section 34 above; and

(e) the AML/CTF Compliance Manager to determine whether to collect and/or verify the name and address of each beneficial owner (if any).

35.4 For the purposes of 35.3(c) above, the Tyndall employee responsible for the customer may refer to one or more of the following sources to determine whether the company is licensed and subject to regulatory oversight in Australia:

(a) Australian Securities and Investments Commission (ASIC) (www.asic.gov.au);

(b) Australian Securities Exchange (ASX) (www.asx.com.au); and

(c) Australian Prudential Regulatory Authority (APRA) (www.apra.gov.au).

35.5 For the purposes of Section 35.3(a), in determining whether to collect and/or verify the name and address of each beneficial owner (if any), the AML/CTF Compliance Manager will have regard to the ML/TF risk relevant to the provision of the designated service the new customer will be receiving. Consideration needs also to be given to the jurisdiction of incorporation of the company as well as the jurisdiction of the primary operations of the company and the location of the foreign stock or equivalent exchange (if any) and any other issues that the AML/CTF Compliance Manager deems relevant.

35.6 For the purposes of Sections 35.3(b) and 35.3(c), in determining whether to collect and/or verify the name and address of each beneficial owner (if any), the AML/CTF Compliance Manager will have regard to the ML/TF risk relevant to the provision of the designated service the new customer will be receiving. The verification procedures in Section 36 must also be followed.

36. COMPANIES: VERIFICATION – PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.3

36.1 The following verification procedures need to be followed for companies:

(a) Government database verification (section 64); and

(b) Politically exposed persons verification (section 65); and

(c) Foreign high-risk jurisdiction verification (section 57); and

(d) A document identification procedure (section 36.2).

36.2 At a minimum, the following KYC information about a customer in section 34 must be verified:

(a) In the case of a domestic company:

(i) The full name of the company as registered by ASIC;

(ii) The full address of the company's registered office;

(iii) The full address of the company's principal place of business, if any;

(iv) The ACN or ABN issued to the company;

(v) Whether the company is registered by ASIC as a proprietary or public company; and

(vi) If the company is registered as a proprietary company, the name of each director of the company;

(b) In the case of a registered foreign company:

(i) The full name of the company as registered by ASIC;

(ii) The full address of the company's registered office in Australia;

(iii) The full address of the company's principal place of business in Australia (if any) or the full name and address of the company's local agent in Australia;

(iv) The ARBN issued to the company;

(v) The country in which the company was formed, incorporated or registered;

(vi) Whether the company is registered by the relevant foreign registration body and if so whether it is registered as a private or public company or some other type of company; and

(vii) If the company is registered as a private company by the relevant foreign registration body – the name of each director of the company;

(c) In the case of an unregistered foreign company:

(i) The full name of the company;

(ii) The country in which the company was formed, incorporated or registered;

(iii) Whether the company is registered by the relevant foreign registration body and if so:

(A) Any identification number issued to the company by the relevant foreign registration body upon the company's formation, incorporation or registration;

(B) The full address of the company in its country of formation, incorporation or registration as registered by the relevant foreign registration body; and

(C) Whether it is registered as a private or public company or some other type of company by the relevant foreign registration body;

(iv) If the company is registered as a private company by the relevant foreign registration body – the name of each director of the company; and

(v) If the company is not registered by the relevant foreign registration body, the full address of the principal place of business of the company in its country of formation or incorporation.

36.3 If the company is an unregistered foreign company, the AML/CTF Compliance Manager may determine that it is necessary to seek an explanation as to why the company is not registered.

36.4 Where it has been determined under an assessment conducted under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a company is medium or high and additional KYC information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC information that has been collected. The AML/CTF Compliance Manager will determine what additional KYC information will be verified in respect of that customer.

36.5 For information that is required to be verified as indicated in Section 36.2 and, the following can be used:

(a) reliable and independent documentation (Refer Section 37);

(b) reliable and independent electronic data (Refer Section 39); or

(c) a combination of (a) and (b) above.

37. COMPANIES: SIMPLIFIED VERIFICATION PROCEDURES

37.1 The criteria in Section 36 does not have to be satisfied where Tyndall confirms that the company is:

(a) a domestic listed public company;

(b) a majority owned subsidiary of a domestic listed public company; or

(c) licensed and subject to regulatory oversight of a Commonwealth, State or Territory regulator in relation to its activities as a company,

By obtaining one or a combination of the following:

(d) a search of the relevant domestic stock exchange;

(e) a public document issued by the relevant company;

(f) a search of the relevant ASIC database; or

(g) a search of the licence or other records of the relevant regulator.

38. COMPANIES: VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.3

38.1 The following types of reliable and independent documentation are acceptable for verification of company information:

- an original and currently valid Australian financial services licence issued by ASIC;
- an original and currently valid company registration certificate issued by ASIC; or
- in relation to the beneficial ownership of a company, a disclosure certificate that verifies information about the beneficial ownership of a company (subject to Section 38.2 below).

38.2 Disclosure Certificates:

(a) For a company other than a foreign company, i.e. an Australian company, a disclosure certificate will be "reliable and independent documentation" for the purposes of 36.5(a) to verify additional information collected in respect of a company.

(b) For a foreign company where other reliable verification information is not otherwise reasonably available, a disclosure certificate verifying information about a foreign company can be relied upon by Tyndall for new customer KYC verification if given approval by the AML/CTF Compliance Manager. The AML/CTF Compliance Manager will take into consideration the ML/TF risk relevant to the provision of the designated service, including the jurisdiction of incorporation of the company as well as the jurisdiction of the primary operations of the company and the location of the foreign stock or equivalent exchange (if any), and the activities undertaken by the company and the availability of evidence about the activities and existence of the company.

39. COMPANIES: VERIFICATION - RELIABLE AND INDEPENDENT ELECTRONIC DATA

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.3

39.1 When verifying KYC Information collected from a customer by means of reliable and independent electronic data, the procedures below need to be followed.

39.2 For the purposes of verification of a company other than a foreign company, the following sources are considered to provide reliable and independent electronic data, having regard to the matters outlined in Section 40.1:

(a) Australian Securities and Investments Commission (ASIC) (www.asic.gov.au);

(b) Australian Securities Exchange (ASX) (www.asx.com.au); and

(c) Australian Prudential Regulatory Authority (APRA) (www.apra.gov.au).

39.3 For the purposes of verification of a foreign company, the following sources are considered to provide reliable and independent electronic data, having regard to the matters outlined in Section 40.1:

(a) a search of the relevant foreign stock or equivalent exchange (if any) – refer to section 39.4; and

(b) a search of the records of the relevant regulator.

39.4 A relevant foreign stock or equivalent exchange is one that is approved by ASIC for recognition, including, but not limited to the following financial markets;

(a) American Stock Exchange;

(b) Borsa Italiana;

(c) Bourse de Paris;

(d) Bursa Malaysia Main Board and Bursa Malaysia Second Board;

(e) Eurex Amsterdam;

(f) Frankfurt Stock Exchange;

(g) Hong Kong Stock Exchange;

(h) JSE Securities Exchange;

(i) London Stock Exchange;

(j) NASDAQ National Market;

(k) New York Stock Exchange;

(l) New Zealand Stock Exchange;

(m) Stock Exchange of Singapore;

(n) SWX Swiss Exchange;

(o) Tokyo Stock Exchange; and

(p) Toronto Stock Exchange.

39.5 For the purposes of verification of a foreign listed public company, Tyndall must have regard to the ML/TF risk relevant to the provision of the designated services being provided (or potentially provided), including the location of the foreign stock or equivalent exchange (if any). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Manager gives final sign-off as required in Section 66.

40. COMPANIES: VERIFICATION - ALTERNATIVE DATA

40.1 Where the data in Sections 37 and 39 above cannot be obtained or is not sufficient to verify the required data listed in Sections 34.2 and 35, in consultation with the AML/CTF Compliance Manager, the Tyndall employee responsible for the customer will determine whether alternative sources of data can be obtained. This alternative data must be reliable and independent such that it can be accepted into the verification process. In making this determination, the following factors need to be taken into account:

(a) the accuracy of the data;

(b) how secure the data is;

(c) how the data is kept up-to-date;

(d) how comprehensive the data is (for example, by reference to the range of persons included in the data and the period over which the data has been collected);

(e) whether the data has been verified from a reliable and independent source;

(f) whether the data is maintained by a government body or pursuant to legislation; and

(g) whether the electronic data can be additionally authenticated.

41. COMPANIES: VERIFICATION – INDEPENDENT CONTACT

41.1 To verify KYC Information collected from a customer, the Tyndall employee responsible for the customer will independently initiate contact with the company. This contact will be made using information contained in public resources such as:

(a) White Pages Directory;

(b) Yellow Pages Directory;

(c) ASIC Database;

(d) internet searches; and

(e) APRA database.

41.2 Any of the electronic data in Sections 39.2 or 39.3 can also be used for the purposes of this Section.

42. TRUSTEES - CUSTOMER IDENTIFICATION PRINCIPLES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.4

42.1 Where a new customer acts in the capacity of a trustee of a trust, it is necessary for the Tyndall employee responsible for that customer to be reasonably satisfied that:

(a) The trust exists; and

(b) The name of each trustee and beneficiary, or a description of each class of beneficiary, of the trust has been provided (section 45).

43. TRUSTEES – PART 1: CUSTOMER IDENTIFICATION PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.4

43.1 In accordance with section 42.1(a), the following KYC information must be collected from a customer:

(i) the full name of the trust;

(ii) the full business name (if any) of the trustee in respect of the trust;

(iii) the type of the trust;

(iv) the country in which the trust was established;

(v) if any of the trustees is an individual, then in respect of one of those individuals – the information required to be collected from an individual under sections 31 to 33;

(vi) if any of the trustees is a company, then in respect of one of those companies – the information required to be collected from a company under sections 34 to 41;

(vii) if the trustees comprise individuals and companies then in respect of either an individual or a company – the information required to be collected from the individual or company (as the case may be) under the applicable customer identification procedures in sections 31 to 33.

43.2 Where it is determined under an assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a trustee of a trust is medium or high, the AML/CTF Compliance Manager may require the Tyndall employee responsible for the customer will collect one or more pieces of the following information:

(a) All business names used by the trusts and any other name under which the trust operates;

(b) The nature of the business activities conducted by the trust;

(c) The source of the customer's funds including the origin of funds;

(d) The jurisdiction in which the trust was established;

(e) Details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the trust;

(f) The nature and level of the customer's intended transaction behaviour;

(g) The income and assets (including location) of the trust;

(h) Details of any parties with which the trust owns property, is in partnership or undertakes a joint venture.

44. TRUSTEES: PART 1 VERIFICATION – PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.4

44.1 The following verification procedures need to be followed for trusts:

(a) Government database verification (section 64); and

(b) Politically exposed persons verification (section 65); and

(c) Foreign high-risk jurisdiction verification (section 57); and

(d) A document identification procedure (section 44.2).

44.2 At a minimum, the following KYC information about a customer in section 42 must be verified:

(a) The full name of the trust from a trust deed, certified copy or certified extract of the trust deed, reliable and independent documents relating to the trust or reliable and independent electronic data;

(b) If any of the trustees is an individual, then in respect of one of those individuals – information about the individual in accordance with the customer identification procedures in sections 31 to 33;

(c) If any of the trustees is a company, then in respect of one of those companies – information about the company in accordance with the procedures in sections 34 to 41; and

(d) If the trustees comprise individuals and companies then in respect of either an individual or a company – the information about the individual or company (as the case may be) in accordance with the applicable procedures in sections 31 to 33.

44.3 Where it has been determined under an assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a trustee of a trust is medium or high and additional KYC information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC information that has been collected. The AML/CTF Compliance Manager will determine what additional KYC information will be verified in respect of that customer.

45. TRUSTEES: PART 2: CUSTOMER IDENTIFICATION PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.4

45.1 In accordance with section 42.1(b), the following KYC information must be collected from a customer:

(i) the full name and address of each trustee in respect of the trust; and

(ii) either:

(A) the full name of each beneficiary of the trust; or

(B) if the terms of the trust identify the beneficiaries by reference to membership of a class – details of the class.

46. TRUSTEES: PART 2 VERIFICATION – PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.4

46.1 The information collected under section 45 must be verified by:

(a) A trust deed, certified copy or certified extract of a trust deed;

(b) Reliable and independent documents relating to the trust;

(c) Reliable and independent electronic data; or

(d) A combination of (1) to (3) above.

46.2 For the purposes of sections 46.1(b) and 46.1(c), "reliable and independent documents relating to the trust" includes a disclosure certificate that verifies information about a trust where:

(a) The verification is being conducted as a result of a risk-based assessment in section determining that additional information is required about the trustee; and

(b) The information to be verified is not otherwise reasonably available from the sources in section 46.1.

46.3 For the purposes of verification of a trustee, Tyndall must have regard to the ML/TF risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Manager gives final sign-off as required in Section 66.

47. TRUSTEES: SIMPLIFIED VERIFICATION – PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.4

47.1 The criteria in sections 44 and 45 will not need to be satisfied where it can be verified that a trustee falls into one of the following categories:

(a) A managed investment scheme registered by ASIC;

(b) A managed investment scheme that is not registered by ASIC and that:

(i) Only has wholesale clients; and

(ii) Does not make small scale offerings to which section 1012E of the *Corporations Act 2001* applies;

(c) Registered and subject to the regulatory oversight of a Commonwealth statutory regulator in relation to its activities as a trust; or

(d) A government superannuation fund established by legislation.

48. PARTNERS: CUSTOMER IDENTIFICATION PRINCIPLES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.5

48.1 Where a new customer acts in the capacity of a partner in a partnership, it is necessary for the Tyndall employee responsible for that customer to be reasonably satisfied that:

(a) The partnership exists; and

(b) The name of each of the partners in the partnership has been provided in accordance with section 49.1(e).

49. PARTNERS: CUSTOMER IDENTIFICATION PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.5

49.1 The following KYC information and documentation, at a minimum, must be collected from a customer:

(a) the full name of the partnership;

(b) the full business name and registration number (if any) of the partnership as registered under any State or Territory business names legislation;

(c) the country in which the partnership was established;

(d) in respect of one of the partners – the information required to be collected from an individual under sections 31 to 33;

(e) the full name and residential address of each partner in the partnership except where the regulated status of the partnership is confirmed through reference to the current membership directory of the relevant professional association.

49.2 Where it is determined under an assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a partner of a partnership is medium or high, the AML/CTF Compliance Manager may require the Tyndall employee responsible for the customer will collect one or more pieces of the following information:

(a) all business names used by the partnership;

(b) In the case of partnerships other than regulated partnerships:

(i) the nature of the business activities conducted by the partnership;

(ii) the source of the customer's funds including the origin of funds;

(iii) the jurisdiction in which the partnership was established;

(iv) in the case of any individual partners – the information required to be collected with respect to medium risk individuals;

(v) in the case of any corporate partners – the information required to be collected with respect to medium risk companies;

(c) details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the partnership; and

(d) the nature and level of the customer's intended transaction behaviour.

50. PARTNERS: VERIFICATION – PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.5

50.1 The following verification procedures need to be followed for partnerships:

(a) Government database verification (section 64); and

(b) Politically exposed persons verification (section 65); and

(c) Foreign high-risk jurisdiction verification (section 57); and

(d) A document identification procedure (section 50.2).

50.2 At a minimum, the following KYC information about a customer in section 42 must be verified:

(a) The full name of the partnership from the partnership agreement, certified copy or certified extract of the partnership agreement, reliable and independent documents relating to the partnership or reliable and independent electronic data; and

(b) Information about one of the partners in accordance with the applicable customer identification procedure with respect to individuals set out in sections 31 to 33.

50.3 Where it has been determined under an assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a partner of a partnership is medium or high and additional KYC information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC information that has been collected. The AML/CTF Compliance Manager will determine what additional KYC information will be verified in respect of that customer.

50.4 The verification in section 50.2 and 50.3 must be based on:

(a) A partnership agreement, certified copy or certified extract of a partnership agreement;

(b) A certified copy or certified extract of minutes of a partnership meeting;

(c) Reliable and independent documents relating to the partnership;

(d) Reliable and independent electronic data; or

(e) A combination of (a) to (d) above.

50.5 For the purposes of sections 50.4(c) and 50.4(d), "reliable and independent documents relating to the partnership' includes a disclosure certificate that verifies information about a partnership where:

(a) The verification is being conducted as a result of a risk-based assessment in section determining that additional information is required about the partnership; and

(b) The information to be verified is not otherwise reasonably available from the sources in section 50.4.

50.6 For the purposes of verification of a partnership, Tyndall must have regard to the ML/TF risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Manager gives final sign-off as required in Section 66.

51. ASSOCIATIONS: CUSTOMER IDENTIFICATION PRINCIPLES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.6

51.1 Where a new customer notifies Tyndall that it is an incorporated or unincorporated association, it is necessary for the Tyndall employee responsible for that customer to be reasonably satisfied that:

(a) The association exists; and

(b) The name of any members of the governing committee (howsoever described) of the association have been provided.

52. ASSOCIATIONS: CUSTOMER IDENTIFICATION PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.6

52.1 The following KYC information and documentation, at a minimum, must be collected from an incorporated or unincorporated association:

(a) If the customer notifies Tyndall that it is an incorporated association:

(i) the full name of the association;

(ii) the full address of the association's principal place of administration or registered office (if any) or the residential address of the association's public officer or (if there is no such person) the association's president, secretary or treasurer;

(iii) any unique identifying number issued to the association upon its incorporation by the State, Territory or overseas body responsible for the incorporation of the association; and

(iv) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association; and

(b) if the person notifies the reporting entity that he or she is a customer in his or her capacity as a member of an unincorporated association:

(i) the full name of the association;

(ii) the full address of the association's principal place of administration (if any);

(iii) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association; and

(iv) in respect of the member – the information required to be collected from an individual under sections 31 to 33;

52.2 Where it is determined under a risk assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to an association is medium or high, the AML/CTF Compliance Manager may require the Tyndall employee responsible for the customer will collect one or more pieces of the following information:

(a) date of formation of the association;

(b) all names under which the association operates;

(c) the name of each member of the governing body(ies) of the association;

(d) the objects and activities of the association;

(e) the source of the customer's funds including the origin of funds;

(f) the name of the CEO, managing director or general manager (if any);

(g) in the case of a foreign incorporated association, the name of the relevant foreign registration body;

(h) in the case of an unincorporated association, the jurisdiction in which it was formed;

(i) the total number of members;

(j) other products of the reporting entity or a related entity held currently or within a specified period by the customer;

(k) details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the association;

(l) the nature and level of the customer's intended transaction behaviour;

(m) the beneficial ownership of the funds used by the customer/the customer's account with the reporting entity;

(n) details of any overseas activities of the association;

(o) the income and assets (including location) of the association; and

(p) details of any parties with which the association owns property, is in partnership or undertakes a joint venture.

53. ASSOCIATIONS: VERIFICATION – PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.6

53.1 The following verification procedures need to be followed for associations:

(a) Government database verification (section 64); and

(b) Politically exposed persons verification (section 65); and

(c) Foreign high-risk jurisdiction verification (section 57); and

(d) A document identification procedure (section 50.2).

53.2 At a minimum, the following KYC information about a customer in section 52:

(i) If the customer notifies Tyndall that it is an incorporated association – verify from information provided by ASIC or by the State, Territory or overseas body responsible for the incorporation of the association or from the rules or constitution of the association or from a certified copy or certified extract of the rules or constitution of the association or from reliable and independent documents relating to the association or from reliable and independent electronic data:

(A) the full name of the incorporated association;

(B) any unique identifying number issued to the association upon its incorporation; and

(C) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the association; and

(ii) if the person notifies the reporting entity that he or she is a customer in his or her capacity as a member of an unincorporated association verify:

(A) the full name (if any) of the association from the rules or constitution of the association or from a certified copy or certified extract of the rules or constitution of the association or from reliable and independent documents relating to the association or from reliable and independent electronic data; and

(B) information about the member in accordance with the applicable customer identification procedure with respect to individuals in sections 31 to 33;

53.3 Where it has been determined under an assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to an association is medium or high and additional KYC information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC information that has been collected. The AML/CTF Compliance Manager will determine what additional KYC information will be verified in respect of that customer.

53.4 The verification in section 53.2 and 53.3 must be based on:

(a) The constitution or rules of the association or a certified copy or certified extract of the constitution or rules of the association;

(b) The minutes of meeting of the association or a certified copy or certified extract of minutes of meeting of the association;

(c) In the case of an incorporated association, information provided by ASIC or by the State, Territory or overseas body responsible for the incorporation of the association;

(d) Reliable and independent documents relating to the association;

(e) Reliable and independent electronic data; or

(f) A combination of (a) to (e) above.

53.5 For the purposes of sections 53.4(d) and 53.4(e), "reliable and independent documents relating to the partnership" includes a disclosure certificate that verifies information about an association where:

(a) The verification is being conducted as a result of a risk-based assessment in section 46.2 determining that additional information is required about the association; and

(b) The information to be verified is not otherwise reasonably available from the sources in section 53.4.

53.6 For the purposes of verification of an association, Tyndall must have regard to the ML/TF risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Manager gives final sign-off as required in Section 66.

54. REGISTERED CO-OPERATIVES: CUSTOMER IDENTIFICATION PRINCIPLES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.7

54.1 Where a new customer notifies Tyndall that it is a registered co-operative, it is necessary for the Tyndall employee responsible for that customer to be reasonably satisfied that:

(a) The co-operative exists; and

(b) The names of the chairman, secretary or equivalent officer in each case of the co-operative have been provided.

55. REGISTERED CO-OPERATIVES: CUSTOMER IDENTIFICATION PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.7

55.1 The following KYC information and documentation, at a minimum, must be collected from a registered co-operative:

(i) the full name of the co-operative;

(ii) the full address of the co-operative's registered office or principal place of operations (if any) or the residential address of the co-operative's secretary or (if there is no such person) the co-operative's president or treasurer;

(iii) any unique identifying number issued to the co-operative upon its incorporation by the State, Territory or overseas body responsible for the registration of the co-operative; and

(iv) the full name of the chairman, secretary and treasurer or equivalent officer in each case of the co-operative.

55.2 Where it is determined under a risk assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a registered co-operative is medium or high, the AML/CTF Compliance Manager may require the Tyndall employee responsible for the customer will collect one or more pieces of the following information:

(a) date of formation of the co-operative;

(b) all names under which the co-operative operates;

(c) the name of each member of the governing body(ies) of the co-operative;

(d) the objects and activities of the co-operative;

(e) the source of the customer's funds including the origin of funds;

(f) the name of the CEO, managing director or general manager (if any);

(g) the jurisdiction in which it was formed;

(h) the total number of members;

(i) details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the co-operative;

(j) the nature and level of the customer's intended transaction behaviour;

(k) the beneficial ownership of the funds used by the customer/the customer's account with the reporting entity;

(l) details of any overseas activities of the co-operative;

(m) the income and assets (including location) of the co-operative; and

(n) details of any parties with which the co-operative owns property, is in partnership or undertakes a joint venture.

56. REGISTERED CO-OPERATIVES: VERIFICATION – PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.7

56.1 The following verification procedures need to be followed for registered co-operatives:

(a) Government database verification (section 64); and

(b) Politically exposed persons verification (section 65); and

(c) Foreign high-risk jurisdiction verification (section 57); and

(d) A document identification procedure (section 50.2).

56.2 At a minimum, the following KYC information about a customer in section 55 must be verified from information provided by ASIC or by the State, Territory or overseas body responsible for the registration of the co-operative or from any register maintained by the co-operative or a certified copy or certified extract of any register maintained by the co-operative or from reliable and independent documents relating to the co-operative or from reliable and independent electronic data:

(a) the full name of the co-operative; and

(b) any unique identifying number issued to the association upon its incorporation.

56.3 Where it has been determined under an assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a registered co-operative is medium or high and additional KYC information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC information that has been collected. The AML/CTF Compliance Manager will determine what additional KYC information will be verified in respect of that customer.

56.4 The verification in section 56.2 and 56.3 must be based on:

(a) Any register maintained by the co-operative or a certified copy or certified extract of any register maintained by the co-operative;

(b) Any minutes of meeting of the co-operative or a certified copy or certified extract of any minutes of meeting of the co-operative;

(c) Information provided by the State, Territory or overseas body responsible for the registration of the co-operative;

(d) Reliable and independent documents relating to the co-operative;

(e) Reliable and independent electronic data; or

(f) A combination of (a) to (e) above.

56.5 For the purposes of sections 56.4(d) and 56.4(e), "reliable and independent documents relating to the partnership" includes a disclosure certificate that verifies information about a registered cooperative where:

(a) The verification is being conducted as a result of a risk-based assessment in section 49.2 determining that additional information is required about the association; and

(b) The information to be verified is not otherwise reasonably available from the sources in section 56.4.

56.6 For the purposes of verification of a registered co-operative, Tyndall must have regard to the ML/TF risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Manager gives final sign-off as required in Section 66.

57. GOVERNMENT BODIES: CUSTOMER IDENTIFICATION PRINCIPLES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.8

57.1 Where a new customer notifies Tyndall that it is a Government body, it is necessary for the Tyndall employee responsible for that customer to be reasonably satisfied that:

(a) The Government body exists; and

(b) In the case of certain kinds of Government bodies – information about the beneficial ownership of the Government body has been provided, where sought by the reporting entity.

58. GOVERNMENT BODIES: CUSTOMER IDENTIFICATION PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.8

58.1 The following KYC information and documentation, at a minimum, must be collected from a Government body:

(a) the full name of the Government body;

(b) the full address of the Government body's principal place of operations;

(c) whether the Government body is an entity or emanation, or is established under legislation, of the Commonwealth; and

(d) whether the Government body is an entity or emanation, or is established under legislation of a State, Territory, or a foreign country and the name of that State, Territory or country.

58.2 Where it is determined under a risk assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a government body is medium or high and additional KYC information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC information that has been collected. The AML/CTF Compliance Manager will determine what additional KYC information will be verified in respect of that customer.

(a) for government bodies of countries which are not FATF members:[3]

(i) date of establishment of the body;

(ii) the functions and activities of the body;

(iii) the source of the customer's funds including the origin of funds;

(iv) the name of any legislation governing the operations of the body;

(v) the countries where the body has offices;

(b) details of any current or recent prosecutions and inquiries related to money laundering, terrorist links, tax offences and corruption in respect of the body; and

3 Consideration should be given to the appropriateness of this distinction. Note that the Russian Federation is a member.

(c) other products of the reporting entity or a related entity held currently or within a specified period by the customer.

59. GOVERNMENT BODIES: VERIFICATION – PROCEDURES

Source of Section Content	
Document	**Sections**
Anti-Money Laundering and Counter-Terrorism Financing Rules Instrument 2007 (No. 1)	Part 4.8

59.1 The identity of government bodies which are classified as low risk by the AML/CTF Compliance Manager will not be verified. Where it has been determined under an assessment carried out under Section 30.1 that the ML/TF risk posed by the provision of a designated service to a government body is medium or high and additional KYC information has been collected in respect of that customer, it may be necessary to verify some or all of the additional KYC information that has been collected. The AML/CTF Compliance Manager will determine what additional KYC information will be verified in respect of that customer.

59.2 The following verification procedures need to be followed for government bodies:

(a) Government database verification (section 64); and

(b) Politically exposed persons verification (section 65); and

(c) Foreign high-risk jurisdiction verification (section 57); and

(d) A document identification procedure (section 50.2).

59.3 The verification in section 59.1 must be based on:

(a) Reliable and independent documents;

(b) Reliable and independent electronic data; or

(c) A combination of both.

59.4 For the purposes of verification of a government body, Tyndall must have regard to the ML/TF risk relevant to the provision of the designated services being provided (or potentially provided). These factors will be deemed to have been sufficiently considered when the AML/CTF Compliance Manager gives final sign-off as required in Section 66.

60. AGENTS: IDENTIFICATION PROCEDURES

60.1 Where an agent requests the provision of a designated service on behalf of a customer, Tyndall must collect, at a minimum the following:

(a) the full name of the person who purports to act on behalf of the customer; and

(b) evidence of the customer's authorisation of the person to act on its behalf.

60.2 Where an agent requests the provision of a designated service on behalf of a customer, Tyndall will carry out the relevant customer identification procedure outlined in Part B, in respect of that customer.

61. AGENTS: VERIFICATION PRINCIPLES

61.1 Tyndall will not verify the identity of the agent where the ML/TF risk associated with the provision of the designated service is classified as low by the AML/CTF Compliance Manager. Where it is determined that the ML/TF risk associated with the provision of the designated service to the particular customer is medium or high, Tyndall will verify the information specified in Section 60.1 in accordance with the requirements of Section 32.4.

61.2 Tyndall will verify the identity of the customer in accordance with its customer identification procedures set out in Part B.

62. VERIFICATION – RELIABLE AND INDEPENDENT DOCUMENTATION

62.1 It is assumed that any document used to verify KYC information will be sufficiently contemporaneous unless otherwise specified in the AML/CTF Rules or in this AML/CTF Program. For the purposes of this AML/CTF Program, a document will be sufficiently contemporaneous if it has not expired or, where it does not have an expiry date, is no more than three months old.

62.2 If a customer is unable to provide an original copy of a document for the purposes of verifying KYC information, the AML/CTF Compliance Manager will need to determine, having regard to the ML/TF risk associated with the provision of a designated service to that customer, whether it is appropriate to rely on a certified copy of the document.

62.3 The AML/CTF Compliance Manager will take steps to determine whether any document produced by a customer has been forged, tampered with, cancelled or stolen.

63. VERIFICATION – FOREIGN JURISDICTIONS

Source of Section Content	
Document	**Sections**
AUSTRAC Guidance Note: Risk management and AML/CTF programs	6.11

63.1 Where Tyndall has the prospect to acquire a new customer from a foreign jurisdiction, an assessment must be made as to whether it is a high-risk jurisdiction. The factors that should be considered in this assessment include, but are not limited to:

(a) Whether the customer is based in a country that is a FATF member and any FATF reports about that country;

(b) The legal framework and standard AML/CTF controls of the foreign jurisdiction; and

(c) The economic climate of the foreign jurisdiction.

63.2 The assessment should take into account information from legitimate, respected domestic and/or international bodies.

63.3 Where an assessment is made that the customer is from a high-risk jurisdiction, the matter must be referred to the AML/CTF Compliance Manager who will make a decision as to whether Tyndall should continue dealing with the customer.

64. VERIFICATION – GOVERNMENT DATABASES

64.1 Where Tyndall is likely to provide designated services to a new customer, the following procedures must be carried out in addition to the KYC procedures discussed elsewhere in the Tyndall AML/CTF Program by the Tyndall employee responsible for the customer:

(a) DFAT Consolidated List

(i) The name of a prospective customer must be checked against the DFAT Consolidated List available at http://www.dfat.gov.au/icat/freezing terrorist assets.html.

(ii) The DFAT Consolidated List must be accessed directly from the DFAT website every time a prospective customer is checked – a copy of this spreadsheet should not be saved on an employee's computer in order to ensure that the most recent version of the Consolidated List is used.

(iii) Alternatively, the DFAT 'LinkMatch Lite' software may be used to check the names of a prospective customer – prior to a prospective customer being checked, the most recent version of the 'LinkMatch Lite' software must be downloaded from http://www.dfat.gov.au/divs/ild/download lms.html.

(iv) Where there is a match it must be **immediately** referred to the AML/CTF Compliance Manager who will carry out the "What if I do find a match?" procedures published at http://www.dfat.gov.au/icat/freezing terrorist assets.html

(v) Where a match is found on the DFAT Consolidated List, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Manager.

(b) Australian National Security (ANS)

(i) The name of the new customer must be checked against the ANS Listing of Terrorist Organisations available at http://www.nationalsecurity.gov.au/agd/www/nationalsecurity.nsf/AllDocs/95FB057CA3DECF30CA256FAB001F7FBD?OpenDocument

(ii) The ANS Listing of Terrorist Organisations must be accessed directly from the ANS website listed in subsection (i) above every time a prospective customer is being checked – a copy of this list should not be saved on an employee's computer in order to ensure that the most recent version is used.

(iii) Where there is a match it must be **immediately** referred to the AML/CTF Compliance Manager.

(iv) Where there is a match with the ANS Listing of Terrorist Organisations, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Manager.

(c) Reserve Bank of Australia (RBA) Sanctions List

(i) The name of the new customer must be checked against the RBA Sanctions List available at: http://www.rba.gov.au/MarketOperations/International/FinancialSanctionsCashReporting/sanctions.html.

(ii) The RBA Sanctions List must be accessed directly from the RBA website listed in subsection (i) above every time a prospective customer is being checked – a copy of this list should not be saved on an employee's computer in order to ensure that the most recent version is used.

(iii) Where there is a match it must be **immediately** referred to the AML/CTF Compliance Manager.

(iv) Where there is a match with the RBA Sanctions List, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Manager.

(d) Criminal Code List

(i) The name of a new customer must be checked against the list contained in the *Criminal Code Regulations 2002* available at: http://www.comlaw.gov.au/

(ii) Where there is a match it must be **immediately** referred to the AML/CTF Compliance Manager.

(iii) Where there is a match with the Criminal Code List, there must not be any further dealings with the customer until permitted by the AML/CTF Compliance Manager.

65. VERIFICATION – POLITICALLY EXPOSED PERSONS

Source of Section Content	
Document	**Sections**
AUSTRAC Guidance Note: Risk management and AML/CTF programs	6.6, 6.8

65.1 Where Tyndall has the prospect to acquire a new customer, the following procedures must be carried out in addition to the KYC procedures discussed elsewhere in the Tyndall AML/CTF Policy

the individual must be assessed as to whether they may satisfy the definition of a politically exposed person (PEP).

65.2 If it is determined that a customer is a PEP, Tyndall will:

(a) obtain approval from the AML/CTF Compliance Manager before providing a designated service to the customer;

(b) collect information regarding the source of wealth and source of funds used by the customer;

(c) apply the enhanced customer due diligence program outlined in Section 23 of the Tyndall AML/CTF Program.

65.3 All foreign customers of Tyndall must undergo the PEP verification process.

65.4 Domestic customers of Tyndall will only need to undergo the PEP verification process where it is warranted by the AML/CTF risk(s) faced by Tyndall.

65.5 It is the responsibility of all Tyndall staff to be aware of the risk associated with PEPs and to report any information or suspicions immediately to the AML/CTF Compliance Manager.

66. NOTIFICATION OF ALL NEW CUSTOMERS TO THE AML/CTF COMPLIANCE MANAGER

66.1 The AML/CTF Compliance Manager must be notified of all new customers.

66.2 Sign-off for each new customer should be obtained from the AML/CTF Compliance Manager certifying that no additional KYC Information relating to the customer's existence needs to be verified.

67. TOLERANCE OF DISCREPANCIES AND ERRORS

67.1 **Tolerance of discrepancies:** Where, during the KYC Information collection and verification process, a director, officer or employee of Tyndall discovers any discrepancies in the KYC Information provided by the new customer, the matter should be immediately notified to the AML/CTF Compliance Manager. The discrepancy must not be raised with the new customer without first consulting the AML/CTF Compliance Manager.

67.2 **Pre-defined tolerance levels for matches and errors:** Tyndall will allow for obvious typographical errors in customer information other than name, company registration or identification number, or date of birth. Where the error elates to name, company registration or identification number, or date of birth, the AML/CTF Compliance Manager should be notified and independent contact should be initiated with the customer to clarify the information.