



Anti Money Laundering & Counter-terrorism Policy



Otto IT Pty Ltd
ABN. 23 968 132 622
4/405 High St Northcote,
VIC 3070, Australia
1300 688 648

Policy Name:	Anti Money Laundering and Counter Terrorism Policy
Policy Date	28/08/2023
To:	Otto IT Leadership Team
From:	Integrator

Anti Money Laundering and Counter Terrorism Policy

The purpose of this policy is to identify and prevent any money laundering and counter terrorism funding. Money laundering is the process of legitimising the funds from illegal activities.

Terrorism funding is the act of providing financial support to terrorists or terrorist organisations to enable them to carry out terrorist acts.

Anti-money laundering & counter-terrorism financing (AML/CTF):

Otto IT is subject to, and complies with, applicable Australian laws including the **Anti-Money Laundering and Counter-Terrorism Financing (AML/CTF) Act 2006 (the Act)**.

Under the Act, Otto IT has adopted an AML/CTF program consisting of a set of standards which set out how it identifies, mitigates and manages money laundering and terrorism financing risk. Otto IT is required to report any suspicious activities.

Please report any incidents or suspicions to Otto IT's management.

Money Laundering

The primary goal of criminals is to make money. Often criminals use financial institutions to conceal their illegitimate funds with the aim of making 'dirty money clean' – known as money laundering.

The process of money laundering is generally completed over three stages:

1. Dirty money is 'placed' into the financial system.
2. A series of transactions provide a 'layering' effect to hide the origin of the funds.
3. Funds are 'integrated' back into the economy and appear to be lawful.

Otto IT will continue to work with AUSTRAC and the broader financial industry to curtail money laundering activity.

Terrorism Financing

The financing of terrorism is the financial support, in any form, of terrorism or of those who encourage, plan, or engage in terrorism. Those who finance terrorism transfer funds in such a way that the ultimate use, which is the support of terrorism, is concealed. The funds may be either legal or illegal in origin.

Business relationships with those who finance terrorism or other closely associated persons or entities could expose Otto IT to significant reputation, operational and legal risk.

Identification and reporting of suspicious matters:

Otto IT will identify customers or employees behaving in a suspicious way. There are number of different ways of identifying suspicious activities.

Situations that may be considered suspicious can include:

1. The unusual circumstances of an interaction with a customer;
2. The customer's transaction;
3. The business of the person involved.

All suspicious customer activities or transactions should be reported to Australian Transaction Reports and Analysis Centre (AUSTRAC).

Protecting the company:

Otto IT will endeavour to protect itself from being used for illicit activities by:

1. Conducting customer identification and verification processes to ensure our customers are who they say they are;
2. Only dealing with legitimate customers and ensuring our products and services are not being utilised by money launderers, terrorist financiers or anybody that chooses to support these types of individuals;
3. Carrying out ongoing customer due diligence;
4. Retain all records for seven years, should any investigations related to unlawful actions be conducted;

Discipline under this policy:

Management of Otto IT has the responsibility of overseeing this policy. Supervisors and managers will ensure employees are compliant with all areas of this policy, including any disciplinary action resulting from non-compliance.

Version Control

Version	Date	Author	Comment
1.0	28/08/2023	A. Kane	Policy created