Anti-Money Laundering and Counter-Terrorism Financing Policy

Contents

1. Introduction

ABV is aware that terrorist activity requires financial support and acknowledges that one way of acquiring this support is to redirect funding intended for charitable purposes by fraudulent collection of monies or the infiltration of a charitable organisation by terrorists (without the knowledge of the staff or donors). ABV is committed to the prevention of money laundering and terrorism and acknowledges the Australian government legislation that prohibits dealing with known terrorist organisations and/or prescribed person or entities. ABV will make all reasonable efforts to ensure that no funds or other resources are misappropriated or misdirected to support or further terrorist activities.

2. Purpose

The purpose of the Anti-Money Laundering and Counter-Terrorism Financing Policy is to:

- Guide ABV's work to ensure that no funds or resources directly or indirectly support terrorist activities.
- Outline ABV's commitment to comply with all Australian laws pertaining to counter-terrorism and anti-money laundering.
- Provide for the implementation of processes to mitigate risk of money laundering or terrorism financing.

3. Scope

This policy applies to all but not limited to employees, volunteers, directors, consultants, contractors, members of the Board of ABV, members and representatives of ABV ('Applicable Persons').

4. Definitions

Prescribed Lists – are persons or organisations that have been linked to money laundering or terrorist organisations and are outlined in 5.2.

5. Policy

5.1 Policy Commitments

a. *Zero Tolerance* – ABV takes a zero-tolerance approach towards any association with terrorism or money laundering. All reasonable efforts (including due diligence and precautions) will be undertaken to ensure that resources do not assist, or otherwise support terrorist organisations, including the operatives that perform terrorist acts. ABV will be proactive in mitigating risks.
b. *Awareness and Education* – ABV will take all reasonable steps to ensure that Applicable Persons are aware of this policy and understand their obligations in relation to anti-money laundering and counter-terrorism.
c. *Prevention* – It is in ABV's best interest to know and prevent any support to known terrorist organisations.
d. *Alignment with Australian Laws* – This policy is informed by the Australian Government Counter-Terrorism Strategy and National Counter-Terrorism Plan and is guided by the Department of Home Affairs *'Safeguarding your organisation against terrorism financing: a guidance for non-profit organisations'* a copy of which is included as Attachment A to this policy.
e. *Compliance with the laws of foreign countries* – ABV will comply with the laws of any foreign countries that they operate in and respects the UN Security Council Resolution 2664 (2022) which supports the delivery of humanitarian assistance for those in need while still advancing the Security Council's mandate to maintain international peace and security.
f. *Transparency and Accountability* – ABV will ensure transparency and accountability in all financial dealings, using regulated financial institutions such as banks or building societies where possible.

5.2 Prescribed Lists

For the purposes of this policy 'Prescribed Lists' include:

a. Australian Government Consolidated List which records persons or entities subject to financial sanctions and travel restrictions by the Australian Government as updated from time to time here.
b. Australian Government Listed Terror Organisations as updated from time to time here.
c. World Bank Listing of Ineligible Firms and Individuals as updated from time to time here.

5.3 Risk Register

Anti-Money Laundering and Counter-Terrorism will be a standard inclusion on ABV's Operational Risk Register that will be monitored, reviewed and reported to ABV Board on a regular basis.

5.4 Recruitment

To ensure that no applicant has engaged in terrorist activities or with terrorist organisations, ABV will conduct background checks on all applicants to the following positions and will also ensure that they are manually checked against the Prescribed Lists. If any links are found, the applicant will not continue to be considered for any engagement with ABV.

a. Employees
b. Volunteers
c. Directors
d. Consultants
e. Contractors
f. Members of the Board of ABV
g. Members and representatives of ABV; and
h. Partners

5.5 Partnerships

a. ABV recognises the importance of managing terrorism financing and sanctions risks in its partnerships and may, where appropriate and proportionate to the level of risk, include relevant requirements in Memorandums of Understanding (MoUs), funding agreements and other partner arrangements.

b. Where funds or other resources are provided to a third party, ABV will undertake reasonable and proportionate due diligence to satisfy itself that the third party is a legitimate organisation and that the funds or resources are intended to be used for their approved purpose.

5.6 Due Diligence

When conducting due diligence on partner organisations, vendors or suppliers, ABV will apply a risk-based and proportionate approach. Depending on the nature and the level of risk of the engagement, ABV may:

a. assess the entity's governance and financial management arrangements;
b. screen relevant organisations or individuals against applicable sanctions and terrorist lists;
c. use regulated financial institutions and appropriate payment channels where practicable; and
d. undertake any additional due diligence considered necessary.

5.7 Investigation and Reporting

a. Reports of observed or suspected incidents of money laundering or terrorism financing must be reported immediately (within 24 hours) to the CEO or CFO (the person making the report should ensure that they receive an acknowledgement of receipt from the CEO or CFO). Reports may also be reported in accordance with ABV's Reporting Wrongful Disclosures or Complaints Management Policies or through the following channels:

    i. Directly to the reporter's main contact within ABV
    ii. Directly to the reporter's Line Manager
    iii. Directly to ABV's management team either verbally or in writing
    iv. Directly to an ABV Board member in writing (a request can be made to ABV's CEO for the appropriate contact details)

b. If a person receives a report in accordance with 5.7(a) (i-iv) above, they must ensure that the CEO and CFO are informed immediately (if not already). If it is considered to be a conflict of interest to notify the CEO and/or the CFO, the Chair of the Board should be notified immediately.

c. Notifications will be made to any relevant partner organisations when ABV is made aware of the following instances:

    i. Any personnel engaged with ABV is listed on a Prescribed List.
    ii. Any associated personnel or the organisation is directly or indirectly engaged in, preparing, planning, assisting in or fostering money laundering or the doing of a terrorist act.

d. Reports should include the nature of the incident, involved parties, and any relevant details.

e. The CEO/CFO should report suspicious activity to the Australian Federal Police.

f. If the matter involves an ABV staff member, the CEO follows the guidance of the Australian Federal Police in relation to internal investigation and human resource matters.

g. All Applicable Persons are required to report any observed or suspected incidents of money laundering or terrorism financing in accordance with this policy.

h. Managers/Supervisors are responsible for taking prompt action upon receiving a report and ensuring that it is managed in accordance with this policy.

5.8 Breach of Policy / Retaliation

a. Violations of this policy will be met with disciplinary measures appropriate to the severity of the breach, which may include termination of employment or contractual relationships.

b. ABV prohibits any form of retaliation against individuals who report violations or participate in investigations. Retaliatory actions will be addressed with appropriate disciplinary measures.

5.9 Confidentiality

As far as is reasonably practicable, information regarding allegations and the identity of those providing the information will be kept confidential and shared only with those directly involved in the investigation process including the Australian Federal Police and other external regulators.

5.10 Monitoring and Evaluation

This policy will undergo regular monitoring and evaluation (every two years at a minimum) in the interest of continual improvement. The Compliance Officer will be responsible for monitoring and evaluation.

5.11 Anti-Money Laundering and Counter-Terrorism Checkpoints Flow Chart

A simplified flowchart of these checks and processes is included at Attachment B.

6. Related Documents

Australian Government Counter-Terrorism Strategy and National Counter-Terrorism Plan
Attachment A - Safeguarding your organisation against terrorism financing: a guidance for non-profit organisations
Attachment B - Anti-Money Laundering and Counter-Terrorism Checkpoints Flow Chart
ABV Wrongful Disclosures Policy
ABV Complaints Management Process

7. Document Information

Policy Owner:	CEO
Policy Authority:	Board
Policy Implementer:	Policy and Compliance Officer
Original approval:	14 August 2026
Last Reviewed:	14 August 2026
Last Policy Change:	14 August 2026
Next review date:	14 August 2029

Safeguarding your organisation against terrorism financing

A guidance for non-profit organisations

Non-profit organisations (NPOs) are at risk of being misused by individuals or other organisations to finance or support terrorist activity. This misuse can have serious consequences for NPOs. This can include criminal penalties.

The Australian Government has released a Guidance for NPOs which is intended to:

- build awareness of the risk of being misused for the purpose of terrorism financing
- outline **Best Practice Principles** which NPOs can adopt to help reduce this risk, and
- assist NPOs to understand and comply with legal requirements in relation to terrorism financing.

The Australian Government recognises the vital contribution that NPOs make in Australia and overseas. In minimising the risk of misuse of NPOs, the Australian Government is mindful of the need to not disrupt or discourage legitimate NPO activities. The Guidance is intended to support NPOs to continue their important work. The Guidance is not a legal document.

How do terrorist organisations misuse NPOs?

Terrorist activity requires financial support. One way of acquiring this support is to redirect funding intended for charitable purposes. There are a number of ways that this can occur, including fraudulent collection of monies and infiltration of a NPO by terrorists (without the knowledge of the staff or donors).

Complying with the Best Practice Principles

The **Best Practice Principles** are intended as a guide only to describe 'best practice'. This is not an exhaustive or comprehensive compilation. Many NPOs already have internal controls in place to promote transparency and accountability in their financial operations. Some NPOs have already implemented specific measures to reduce the risk of being misused for the purpose of terrorism financing. NPOs should not abandon proven internal controls and practices, but should review them with a view to strengthening these controls and practices to further reduce the risk of misuse for terrorism financing.

For more information

This flyer is an extract from the Australian Government publication titled *Safeguarding your organisation against terrorism financing – A guidance for non-profit organisations*. This flyer should be read in the context of the full publication. It is recommended that you obtain a copy of the full publication, which is available at **www.nationalsecurity.gov.au/npo.**

Best Practice Principles

Overarching principle

1. NPOs must make all reasonable efforts to ensure that funds are not being directed to terrorist activities.

Legal obligations

2. NPOs operating in Australia must comply with Commonwealth, State and Territory laws.
3. Australian NPOs should comply with the laws of any foreign countries that they operate in.

Risk awareness

4. NPOs should understand the level of risk that their organisation may be exposed to in relation to terrorism financing, and where risk is evident, take necessary precautions.
5. NPOs should ensure that management, staff and volunteers are aware of the level of risk that their organisation may be exposed to in relation to terrorism financing and, where risk is evident ensure that precautions are in place.

Due diligence

6. NPOs should know their beneficiaries.
7. NPOs should know the third parties they work with.
8. NPOs should regularly check that beneficiaries and third parties are not listed individuals or organisations.

Transparency and accountability

9. NPOs should conduct financial transactions where possible through regulated financial institutions, such as banks or building societies.
10. NPOs should conduct background checks of management, staff and volunteers.
11. NPOs should keep records of what assistance has been provided, who has received it, and the details of any third parties involved.
12. NPOs should conduct follow-up checks where possible to make sure that the assistance was delivered as intended.
13. NPOs should report suspicious activity to the Australian Federal Police.

Using Third Parties

Where funds are provided to a third party

14. the NPO should make all reasonable efforts to ensure the third party is aware of, and seek assurance that the third party will comply with, all applicable laws, and the NPO should make all reasonable efforts to ensure the third party is aware of, and seek assurance that the third party will comply with these Best Practice Principles.

Attachment B – Anti-Money Laundering and Counter-Terrorism Checkpoints Flow Chart