

Fraud Control Policy and Management Plan

fraud

Working for a fair and equitable Australia

[Jobs Australia Member]

Insert organisation's name

Fraud Control Policy and Management Plan

About this document

All organisations have a responsibility to take steps to guard against the fraudulent use of their resources. Jobs Australia members who have government contracts to deliver employment services have an additional responsibility to ensure that government money is spent and accounted for in accordance with the terms of the contract. While this has always been the case the demands from government to demonstrate adequate fraud control measures have increased recently and we can expect this trend to continue.

Of course any fraudulent activity relating to government contracts represents a significant risk to the good name of the organisation but it also endangers the ongoing relationship with the government itself. Clearly then, well-managed organisations will want to ensure that their fraud management measures are robust, current and well-understood across all levels of their staff.

This sample Fraud Control Policy and Management Plan is designed to assist Jobs Australia members in ensuring that they have thorough, up-to-date policies and procedures in place to manage the risk of fraud occurring in their organisation.

We hope that you will find it helpful and we welcome your feedback about it and any other resources of a similar nature that we could usefully produce for you.



David Thompson AM
Chief Executive Officer
Jobs Australia
August 2006

CONTENTS

1.	Why have a Fraud Control Policy and Management Plan?	4
2.	What is fraud?	4
3.	Our organisation's policy on fraud	5
4.	What the Fraud Control Plan seeks to do	5
5.	The role of the Fraud Control Officer	5
6.	Who else has responsibilities for fraud control?	6
7.	Becoming fraud aware	6
8.	Who assesses the fraud risks in our organisation?	7
9.	The Risk Register	7
10.	Ensuring regular assessments of fraud risks	9
11.	Ongoing review of the fraud control strategies	10
12.	Detecting fraud	10
13.	How and when to report fraud	11
14.	When there's an investigation	12
15.	Making the Fraud Control Plan happen	13
16.	Examples	14
17.	Examples: Fraud involving people outside the organisation	14
18.	Examples: Fraud by employees and others using an organisation's funds	15
19.	Examples: Fraud by employees and others using an organisation's property	15
20.	Examples: Fraud by employees and others to improve personal property	16
21.	Examples: Fraud arising from staff, management, or Board of Directors or Management Committee bodies due to a failure to perform their duties	16
22.	Conclusion: More examples	16
Appendix	Jobs Australia Whistleblower Guide	19

1. Why have a Fraud Control Policy and Management Plan?

Trust is an essential component of our organisation, but sometimes trust is not enough.

Fraud does happen and often when and where it is least expected. Fraud is not only a serious breach of trust, it is also a criminal offence. When developing a fraud control policy examine all activities of your organisation, not just the areas where money is received.

Those who commit fraud:

- break the law;
- become subject to disciplinary action, including the likelihood of immediate termination of employment;
- bring our organisation into disrepute by tarnishing our reputation as sound managers of our, and the community's, resources;
- create trauma within their own family and circle of friends; and
- in extreme cases will cause our organisation to close down.

We rely on the support of government, community and business to do the things we do. The financial assistance we receive from them is dependent on many factors. Two of the most crucial are our reputation and our record for delivering our services in an ethical and accountable manner. A single instance of fraud will tarnish that good name.

The Fraud Control and Management Plan demonstrates that we are committed to achieving effective fraud control and details the practical steps we will regularly undertake to achieve this.

2. What is fraud?

Australian Standard 8001–2003 defines fraud as:

'dishonest activity causing actual or potential financial loss to any persons or entity including theft of moneys or other property by employees or persons external to the entity and whether or not deception is used at the time, immediately before or immediately following the activity. This also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or for improper use of information or position.'

Fraud can occur in a variety of ways and it is important for everyone in our organisation to have a good understanding of what constitutes fraud so that they can recognise it and take action to prevent it.

The opportunity to commit fraud requires knowledge of our organisation's systems, or those of other organisations, combined with the willingness to exploit any weakness in those systems for direct personal benefit or for the benefit of others. It uses deceit, trickery, sharp practice or sometimes simply a belief that the ends justify the means.

3. Our organisation's policy on fraud

At (name of organisation¹) we recognise that fraud is inherently wrong. It is against our values and we intend to work actively to avoid it occurring.

¹ Insert name of organisation

We aim to foster an organisational culture which will ensure that the effective prevention of fraud and corruption is an integral part of our operating activities. We will identify and promptly investigate any suspicion of fraudulent or related dishonest activities. When appropriate we will pursue legal remedies available under the law.

All our employees are accountable for, and have a role to play in, fraud and corruption control. We encourage a positive culture within our staff to disclose actual or suspected fraudulent. We will investigate all reports thoroughly. Where this is the appropriate course of action we will protect the anonymity of anyone reporting these activities. Any staff member who suspects that such activity is occurring is to follow the procedures outlined in the Whistleblower Guide.

4. What the Fraud Control Policy Plan seeks to do

The plan aims to put the following principles into practice:

- the prevention, detection and investigation of fraud;
- the prosecution of offenders, including those involving routine or minor instances of fraud where appropriate;
- the application of appropriate civil, administrative or disciplinary penalties;
- the recovery of the proceeds of fraudulent activity;
- the training of all employees in ethics, privacy and fraud awareness activities;
- the specialised training of all employees involved in fraud control activities; and
- the external scrutiny of our fraud control activities.

To do this we will establish a number of measures that together will constitute our fraud control strategies. We will clearly delineate the role of the person responsible for fraud control (our Fraud Control Officer²). We will review the various policies and codes of practice we have that relate to fraud and the timelines we establish for carrying out our fraud management processes. We will undertake staff training for fraud awareness.

5. The role of the Fraud Control Officer

We have an appointed Fraud Control Officer, and this position is currently held by (Insert name of the person who holds the position³). This is the employee who has primary responsibility for overseeing the implementation and review of our Fraud Control Policy and Management Plan and for ensuring that this is well understood and actively upheld by staff at all levels of our organisation.

This appointment will be regularly rotated to avoid complacency, however the frequency will not be such that it runs the risk of losing expertise in the identification, conduct and completion of investigations. A full schedule of the Fraud Control Officer's responsibilities will be made available to staff by the responsible HR staff member.

² If you do not already have a Fraud Control Officer you will need to appoint someone or assign responsibilities to the appropriate member of staff.

³ Insert name

6. Who else has responsibilities for fraud control?

Fraud control is the responsibility of everyone in the organisation.

More specifically, the Board, CEO, the Fraud Control Officer and senior management should be aware of circumstances that may indicate the possibility of fraud. These can include:

- Discrepancies in the accounting records;
- Conflicting or missing evidence and documentation;
- Problematic or unusual relationships between the auditor and management;
- Unwillingness by management to permit the auditor to meet privately with those charged with the organisation's governance (e.g. Committee of Management, Board, Audit Committee);
- Accounting policies that appear to be at variance with industry norms;
- Frequent changes in accounting estimates that do not appear to result from changes in circumstances;
- Tolerance of violations of (the code of conduct/code of practice⁴);
- Large proportions of remuneration for senior management being dependent on bonuses and these being driven by achieving unusually successful results;
- Payments of significant bonuses and incentives as a means of increasing performance; and
- Domination by a single person or small group without compensating controls.

7. Becoming fraud aware

It is important that all employees have a general awareness of fraud and corruption and how he or she should respond if this type of activity is detected or suspected.

We will regularly communicate to you a clear definition of the types of action, particularly those that are specific to our business, that constitute fraudulent or corrupt practice, the fraud detection measures that are in place and an unequivocal statement that fraudulent and corrupt practices will not be tolerated.

An awareness of the risk of fraud control techniques and our attitude to control of fraud will be fostered by strategies that:

- ensure all employees receive training in our code of conduct at induction and throughout the period of their employment;
- ensure all employees receive regular fraud awareness training appropriate to their level of responsibility;
- ensure updates and changes to fraud-related policies, procedures and the code of conduct are effectively communicated to all employees;
- ensure all staff are aware of the alternative ways in which they can report allegations or concerns regarding fraud or unethical conduct, for instance the Jobs Australia Whistleblower Guide⁵;
- encourage staff to report any suspected incidence of fraud; and

⁴ Insert the appropriate term

⁵ See Appendix

- promote fraud awareness and standards of conduct through regular meetings, staff newsletters or other internal publications, and through the overt, ongoing commitment demonstrated by senior management in all aspects of their relationships.

8. Who assesses the fraud risks in our organisation?

The CEO has ultimate responsibility (and reports to the Board) to assess the risk of fraud occurring and implement the appropriate preventative measures. He or she does this with the direct support of the Fraud Control Officer, our auditors and all employees.

The CEO will encourage the use of a variety of techniques to assess various risk factors for fraud. These will include managing:

- **Accounting risks:** The need to assess attitudes to the application of accounting standards, and to ensure that correct procedures are followed in the case of third parties involved in the assessment of the organisation's performance e.g. auditors and government departments;
- **Personal risks:** The need to assess risks in an environment where there is an autocratic management style, unusual behaviour, expensive lifestyles, untaken holidays, poor quality staff, low morale or high staff turnover;
- **Cultural risks:** The need to be aware of the risks in a culture that requires results at any cost or has a poor commitment to internal controls and demands unquestioning obedience from staff;
- **Structural risks:** The need to understand that fraud is made easier when there are complex corporate structures and when remote locations are poorly supervised; and
- **Business risks:** The need to be alert to the risks that arise when business strategies are poor, profits exceed industry norms, the organisation has a poor corporate reputation or when it is facing liquidity problems.

9. The Risk Register

As part of our Fraud Risk Assessment (Insert name of organisation⁶) has a Risk Register. This clearly lists the identified potential fraud and corruption risks that our organisation faces.

Risk Register factors potentially affecting us are organised to cover the following areas:

- a) **misappropriation of assets**, including theft, 'temporary borrowing', control over handling of cash and recording its use;
- b) **misuse of assets**, such as unauthorised personal use of organisational assets including motor vehicle, computers, stationery;
- c) failure by staff to adhere to **delegations of authority** relating to the value of assets or contracts they can sign for;
- d) **lack of supporting documentation**;
- e) **lack of a mandatory vacation policy** (or its enforcement) for employees performing key control functions;
- f) **fraudulent financial reporting**, including intentional distortion of financial statements, capitalising revenue items, fictitious asset register items, arguments with

⁶ Insert name of organisation

auditors, calculated avoidance of auditor involvement or restrictions in access to, or availability of, staff;

- g) **high turnover** of management, legal or accounting advisors or Board members;
- h) continued employment of **ineffective accounting**, IT or internal audit staff;
- i) **hiring of friends** and relations;
- j) attitudes of and financial **pressures affecting employees** handling assets that are susceptible to misappropriation, such as:
 - **Long-term, trusted employees:** These individuals know the systems and processes in detail. This knowledge allows them to more easily circumvent controls and conceal fraud. These employees often do not take annual leave, resent questioning, and often are unable to find records or files.
 - **Life crisis of employee:** e.g. divorce, death in family, or other matters that create a need for substantial sums of money.
 - **Lifestyle changes:** e.g. employees who are living beyond their means.
 - **Rule breaker mentality:** i.e. employees who ignore rules or regulatory requirements.
 - **Unappreciated workaholic:** This includes employees who believe they are not adequately compensated for the long, hard hours they work.
- k) **inventory characteristics** such as small size and high volume;
- l) **fixed assets and plant** and equipment characteristics such as storage off-site, portability of assets;
- m) security of and access to **branch offices** including multiple keys, lack of video surveillance in danger areas;
- n) **exploitation of incentives** and bonuses in contracts with customers (e.g. government contracts);
- o) engagement of **trade contractors, subcontractors or consultants** who have inappropriately close relationships with staff; and
- p) **management characteristics** and the degree of influence management exerts.

Management characteristics and the degree of influence that management has in controlling the working environment and the organisation's activities can be subtly powerful influences that create the risk of fraud. However, the nature of the work Jobs Australia members do as nonprofit organisations means that they do not display some characteristics that represent a fraud risk in profit organisations. Where this positive situation exists it is important to guard its continuation and integrity. The following are some relevant considerations:

1. As part of the community and the nonprofit sector, Jobs Australia members are not under pressure to maintain or increase the organisation's stock/share price or earnings trend through the use of inflating or deflating cash flows. On the other hand the pressure to achieve results (e.g. renewal of contract), achieve good Star Ratings, improve ratings for key performance indicators as required in performance-based contracts such as in the Job Network do contain fraud-related risks.
2. A significant portion of management remuneration is not represented by bonuses or incentives which are dependent on the manager's division having to achieve unduly aggressive targets for operating results, financial position or cash flows.
3. There are no other third parties providing undue pressure to inflate or deflate earnings or cash flows.

4. There is no undue influence from the organisation's owners or management to pursue inappropriate tax minimisation strategies.

Desirable characteristics that will reduce the risk of fraud include the following organisational behaviour:

- The organisational structures in place provide for the effective communication of directives across the whole organisation to ensure that appropriate values and ethics are maintained;
- Known control weaknesses are addressed immediately once they become known;
- Management overtly displays and upholds respect for the law and regulatory authorities;
- Management employs effective and adequately qualified staff and utilises such external expertise as is required in the circumstances that have arisen; and
- There is no history of contravention of the Corporations Act or other securities laws.

As part of the regular audit process our auditor will undertake:

- procedural data analysis;
- visits to difference locations and surprise visits where necessary;
- an altered audit approach where necessary e.g. direct oral contact with major customers and suppliers rather than by more traditional letter/written communication;
- personal interviews where necessary;
- data mining to test the integrity of computer-based records;
- comparison of management estimates/budgets with actuals; and
- review of all payments to the Board.

In addition, our auditor is expected to report on situations involving potentially irregular items including:

- unusual transactions;
- checks on employment contracts e.g. incentives;
- examination of large and/or unusual expenses eg. expense reports/claims by senior management; and
- related party authorisations.

10. Ensuring regular assessments of fraud risks⁷

We will carry out a comprehensive Fraud Risk Assessment every two years.⁸ It will take place between (insert months of the year⁹), following which the CEO will provide the findings of the assessment to the Board at the first Board meeting after its completion and similarly to the next staff meeting.

The Fraud Risk Assessment should include a review of:

- information technology and information security;
- electronic commerce, electronic service delivery and internet transactions;
- outsourced functions;
- grants and other payments, benefits or programs;
- tendering processes, and purchasing and contract management;
- services provided to the community;
- revenue collection;
- use of credit cards;
- travel allowance and other common allowances;
- salaries; and
- property and other physical assets, including physical security.

11. Ongoing review of the fraud control strategies

We will review the effectiveness of the various fraud control strategies that make up our Fraud Control Policy and Management Plan on an ongoing basis, and we will regularly review our internal controls and any instances of fraud and corruption. We will undertake (insert timeline, e.g. yearly, biennially, and state which will be conducted internally and which will be conducted by external auditors¹⁰) reviews of our fraud control plan and make adjustments as necessary.

The Fraud Control Officer is responsible for coordinating compliance with the (yearly¹¹) strategy review and (biennial¹²) fraud risk assessment.

⁷ *Running the Risk*, Volunteering Australia's comprehensive guide to understanding risk management contains proformas for a Risk Action Plan. You can access this via their website: (www.volunteeringaustralia.org), or directly at:

http://www.volunteeringaustralia.org/html/s02_article/article_view.asp?id=129&nav_cat_id=164&nav_top_id=61&dsa=309

⁸ Insert the appropriate time period for your organisations e.g. yearly, every two years etc. Typically, an assessment of fraud and corruption risk will be carried out every two years; however the frequency will vary with the Jobs Australia member's size, diversity of business functions, geographic spread and the extent to which the organisation is monitored by other entities within the industry sector.

⁹ Insert appropriate month

¹⁰ Insert appropriate information

¹¹ Insert time period as appropriate

¹² Insert time period as appropriate

Ongoing review and improvement of fraud control strategies will come about by our organisation:

- keeping abreast of best practices, both locally and overseas;
- employing people who have experience and commitment to the continuous improvement of fraud and corruption control; and
- encouraging innovation in fraud and corruption control development, procedures and processes.

12. Detecting fraud

In the event that our fraud preventative systems fail, we will aim to detect fraud as soon as possible by:

- conducting internal reviews and branch audits on a surprise basis;
- the development of specific detection strategies for action by appropriate sectional management; and
- periodic management reviews instigated by the organisation's management team.

We will implement a fraud detection system which will include:

- a program for the strategic analysis of management accounts to identify trends that may be indicative of fraudulent conduct; and
- ongoing assessment of internal risk factors, particularly as these relate to the culture of our organisation, to the susceptibility of certain assets to misappropriation and to staff internal and external pressures; and
- a program for post-incident review.

13. How and when to report fraud

Reports of behaviour involving possible fraud should be communicated to senior management through:

- (a) the normal reporting channels including the following details¹³:
 - the name and address of the person to whom the report is directed;
 - the procedure once the report is received; and
 - when and how the reporter will be informed of the progress/action taken in light of the report e.g. to the Manager who forwards to Senior Manager/Fraud Control Officer.)
- (b) your Whistleblower Guide if appropriate¹⁴:

The Whistleblower Guide is designed to encourage and facilitate the disclosure of improper conduct, provide anonymity for staff that make those disclosures, provide protection for staff who may suffer reprisals in relation to such disclosures and for the matters disclosed to be properly investigated and dealt with. Please refer to the Whistleblower Guide for reporting details. The Jobs Australia member should ensure that all staff are aware of and can access this guide.

¹³ Jobs Australia members insert their normal reporting channel process as described.

¹⁴ Please see the Jobs Australia Whistleblower Guide that accompanies this document as an appendix.

In almost all cases the best time to report a suspected fraud or suspicious activity is immediately. Staff should be made aware of this general rule and be encouraged to have confidence that the organisation will deal with the matter in a timely manner. It is preferable to have the matter be investigated appropriately and according to standard procedures authorised by the Board. It is not desirable to simply undertake your own informal investigation.

In addition to internal reporting, the CEO will address each of the following reporting issues and where necessary enlist the support of others (generally people external to an organisation) to consider:

- protection of employees reporting suspected fraud;
- external anonymous reporting e.g. to Australian Tax Office (ATO);
- reports to the police;
- reports to external parties such as government departments;
- administrative remedies for the recovery of the proceeds of fraudulent conduct; and
- legal reporting obligations e.g. to authorities such as Australian Federal Police, state police, ATO, ASIC, or to government departments in relation to contracts held with them.

14. When there's an investigation

In the event that fraud is detected, reported or suspected an investigation will be conducted by appropriately skilled and experienced personnel who are independent of the section in which the alleged fraud has occurred.

This independent party may include:

- an external law enforcement agency;
- a manager or other senior person; or
- an external consultant operating under the direction of an independent senior person within the organisation.

The investigation should comply with all relevant legislation. Adequate records must be made of all investigations. These records are to be kept in accordance with legal, best practice and privacy management guidelines.

In conducting an investigation into allegations for fraud we will ensure that information arising from or relevant to, the investigation is not disseminated to any person not required by their position description to receive the information.

An investigation will potentially involve the following investigative activities:

- Interviewing of relevant witnesses, both internal and external, including obtaining statements where appropriate;
- Reviewing and collating of documentary evidence;
- Forensic examination of computer systems¹⁵;
- Examination of telephone records;
- Enquiries with banks and other financial institutions;
- Enquiries with other third parties;
- Data search and seizure;

¹⁵ This can include personal emails sent through an organisation's system since these are classed as a work product. In addition the organisation can be held responsible for their content.

- Expert witness and specialist testimony;
- Tracing funds, assets and or goods;
- Preparing briefs of evidence;
- Liaison with the police or other law enforcement or regulatory agencies;
- Interviewing persons suspected of involvement in fraud and corruption; and
- Report preparation.

Any investigation into improper conduct will be subject to an appropriate level of supervision having regard to the seriousness of the matter under investigation. In serious cases, it is contemplated that the Board will be the relevant supervisors.

In each instance where fraud is detected the CEO and the Fraud Control Officer should reassess the adequacy of the internal controls (particularly those directly impacting on the fraud incident and potentially allowing it to occur), and amend and improve controls where necessary.

Where improvements are required, these should be implemented as soon as possible and any amendments to internal controls should be effectively communicated to personnel appropriate to their level of responsibility and position description.

15. Making the Fraud Control Plan happen

We conduct the following activities on a daily, weekly, monthly and/or annual basis to assist in ensuring accurate financial reporting:

- Bank reconciliations are prepared and independently reviewed;
- Fixed asset registers are reconciled to the general ledger and depreciation is charged where appropriate. Physical inventories are performed against asset registers;
- At year end, accruals are left open until the latest possible moment to ensure transactions are recorded in the appropriate period;
- Provisions are generally only made to cover specific costs to be incurred;
- Bad debts, where appropriate, are written off after being approved by the CEO;
- General journals are sequentially numbered, supported by narration and proper authorisation;
- All supporting documentation is appropriately filed;
- Asset sales are recognised in the period in which the sale takes place;
- Payroll transactions are effected on (Insert DAY for weekly paid employees and/or DATE for monthly paid employees¹⁶) with resulting PAYG payments made in accordance with ATO guidelines; and
- The (Insert employee position responsible e.g. Accountant¹⁷) securely maintains information and records relating to payroll matters.

Management uses the following methods to also minimise fraud and corruption:

- Adequate segregation of duties and use of verification procedures;
- Use of exception reports and the authorisation process with respect to the maintenance, adding to or deletion from master files such as clients, suppliers, data

¹⁶ Insert appropriate detail.

¹⁷ Insert employee position.

address changes, new advances. (All computer system update capabilities are performed in head office instead of branches);

- Establishment of a rotation plan for branch employees with respect to the deposit of cash receipts;
- Review and reinforcement of computer security measures, including requiring user-identification passwords for access to computer systems. (Routinely changing passwords will improve computer system security);
- Conduct of internal reviews and branch audits on a surprise basis; and
- Mailing of all statements from the administrative office rather than branches.

Key features of our Compliance Program include:

- Review and update of Operating Policy Manual;
- Staff empowerment through training, recognition and participation;
- Regular systems and process reviews by appropriate staff members;
- Having appropriate channels for employees to report possible non-compliance or system errors;
- Regular audit of the organisation's overall compliance effort;
- Formulation of corrective plans to address any instances of non-compliance; and
- Pre-employment screening to consider the following:
 - Verification of identity;
 - Previous criminal history;
 - Reference check with at least the two most recent employers (this will normally require telephone contact);
 - A consideration of any gaps in employment history and reasons for those gaps;
 - Verification of formal qualifications claimed; and
 - A more thorough screening process for employees applying for particularly sensitive positions.

16. Examples

There are basically two categories of fraud:

- Fraud which results in the loss of funds; and
- Fraud which results in the misuse of assets or the loss of an advantage.

Within the Jobs Australia member's working environment there are a number of areas where potential frauds could occur. We have grouped these under three headings, and have identified some examples of fraud which may be possible within organisations.

17. Examples: Fraud involving people outside the organisation

Invoices for goods and services not received:

- Invoices from the organisation's maintenance contractor for services not performed.
- Repairs to computers, or software support which are unnecessary.

Provision of goods and services by friends or family of staff:

- Tenders being awarded to people who have inside information about other bids or assessment criteria.

- Purchases being made from friends or family businesses at non-commercial prices.

Offers of incentives:

- Offers of gifts to staff in return for their directing business to the supplier.

Preferential payment terms given:

- Family and friends paid earlier than the normal commercial payment period and discounts offered not deducted.
- Unnecessary pre-payments or deposits given.
- Individuals or organisations given the opportunity to purchase assets at less than fair market value or on terms more favourable than those commercially available.

Claims by clients:

- False statements made by clients to claim benefits.

18. Examples : Fraud by employees and others using an organisation's funds

Borrowing:

- 'Borrowing funds' can be very easy if the staff member who receives cash from clients is also responsible for entering records into the cash book and for the organisation's banking.

False Receipts:

- Staff receiving cash from clients maintain two receipt books, the official organisation book and their own *unofficial* book. This enables them to use the cash for a few days, and then return the funds, at which time an official organisation receipt is written up.

False Expense Claims:

- Claims for reimbursement of out-of-pocket expenses for supplies or consumables, supposedly purchased for the organisation's use and substantiated with receipts for purchases for personal use.

False Travel Claims:

- To claim travel allowances when they are not due, or failing to return allowances for travel not undertaken. It may also be possible to claim accommodation allowances for provider-paid training or conferences.
- To purchase petrol for a personal vehicle on the organisation's account.

False Time Sheet Claims:

- Claims on time sheets for hours worked when these are not accurate.

False Claims:

- False statements made by clients to claim benefits.
- Misuse of the Job Seeker Account (JSA), such as a staff member purchasing items in the name of a jobseeker and signing as the jobseeker) when purchasing for self.

Ghosting:

- Paying by cheque for the services of non-existent casual employees. These cheques are subsequently endorsed for payment to another bank account.

Use of signed blank cheques to make payments for non-organisation purposes:

- Cheque signatories should **never under any circumstances** sign cheques which are blank and should only sign any cheque if it is accompanied by complete documentation (usually an invoice and a cheque requisition).

Personal Expenses:

- Personal expenses, such as electricity, gas and telephone accounts, are paid out of organisation funds and recorded as organisation expenses.
- The personal legal services and expenses of a senior member of staff are tacked onto the organisation's legal bill.

19. Examples: Fraud by employees and others using an organisation's property

The use of organisation facilities for personal gain:

- The use of the organisation's computers for after-hours training or tuition or the use of space and equipment for a personal business. (These actions do not incur losses for the organisation, but are an abuse of its facilities by an employee.)
- The use of the GST exemption to purchase goods or services for use by a person or an organisation for purposes other than for the lawful use of the organisation. (This action represents a serious breach of the Commonwealth tax laws. It may also incur personal liability - civil or criminal.)
- Motor vehicles, such as the use of organisation vehicles for unauthorised personal travel or by members of an employee's family.
- In an organisation with an employee bonus scheme employees can be tempted to hit the claim button before they have full documentary evidence to justify an outcome.

20. Examples: Fraud by employees and others to improve personal property

- The use of an organisation's training programs for the improvement of personal property or the supply of services to an employee's premises.
- Individuals or organisations are given the opportunity to purchase assets at less than fair market value, or on terms more favourable than those commercially available.

21. Examples: Fraud arising from staff, management, or Board of Directors or Management Committee bodies due to a failure to perform their duties

Examples include:

- Deliberate failure to record or identify a false statement by a client where the client gains a payment or an advantage from that payment.
- Authorising or recording of data that is known not to be true so that the organisation, Board of Directors or Management Committee body or individual gains a benefit from the fraud, e.g. an employment consultant claims credit for finding a placement for the jobseeker when the jobseeker has found this him/herself (Found Own Employment: FOE).
- Providing inside or confidential information to others outside the organisation for their personal gain.
- Deliberately destroying the organisation's records.
- Manipulating or falsifying statistics to avoid criticism or a reduction in funding.
- Manipulation of data to falsely present successful organisation outcomes, such as the fraudulent reporting of Job Search Training (JST) activities e.g. to indicate completion of 100 hours when only 90 have been achieved.

- Manipulating a JSCI record of interview so that an employment consultant forges the signature of the jobseeker, or by improper use of the jobseeker's PIN to create the electronic signature.

Conclusion: More examples

The following are real-life examples that have happened to others, but which the implementation of sound fraud control policies can avoid.

1. A manager arranged for participants on a landscaping course to carry out works on a Committee member's home. The example suggests that there already exists an improper relationship between the manager and the committee member that would cause concern.
2. A cattle crush purchased for a rural skills course ended up on the manager's own farm. The same employee arranged for roadworks to be completed on his farm as part of a course. This example gives clear evidence of an employee obtaining personal gain from what the organisation does.
3. A manager in Melbourne arranged for six staff to enjoy lunch on the Gold Coast through a *Mystery Flight*. This might be well-intentioned with regard to staff, however it is inappropriate unless authorised by senior management and it will have FBT consequences.
4. A manager arranged for \$30,000 worth of work to be completed on her father's house. While there may be no 'direct' personal benefit this is totally inappropriate and is very questionable.
5. An employee regularly claimed personal grocery purchases through the organisation's petty cash system simply by presenting docketts. This is theft.
6. An employee arranged an unauthorised trip interstate supposedly to attend a work conference at the organisation's expense, but spent the time shopping. This is fraud because it misrepresents the real nature of the expense.
7. A manager arranged for his son's car to be restored through a course. Then, as soon as the course finished, the son sold the car. Even though the restoration might technically have been an approved activity the purpose was inappropriate. There has been a personal benefit, even though it was not direct.
8. An employee regularly claimed payment for overtime which he did not work. This is fraud because the employee has made false statements.
9. The chairperson of an organisation was a local computer supplier. The organisation's computer repairs were done through his firm. He replaced high quality parts in the computers with cheaper parts and used the higher quality parts in his business. Again this is a clear-cut case of fraud by the chairperson, which could have disastrous implications for the organisation's reputation.
10. A manager created phantom casual employees and arranged for payment by cash cheques. Another clear-cut case of a false statement leading to payments to which the manager is not entitled - therefore it is fraud.

APPENDIX

Jobs Australia Member Whistleblower Guide¹⁸

CONTENTS

1. Why have a Whistleblower Guide?
2. What is a whistleblower?
3. Our organisation's policy on whistleblowing
4. What the Whistleblower Guide seeks to do
5. The role of the Whistleblower Protection Officer
6. How and when does a whistleblower make a report?
7. Investigating reports
8. How can I access the Whistleblower Guide?
9. Training
10. Ongoing review of the Whistleblower Guide
11. Government Legislation Relating to Whistleblower Protection

¹⁸ Insert the name of your organisation.

1. Why have a Whistleblower Guide?

A whistleblower is a person who in good faith reports improper conduct through appropriate channels. This conduct may include dishonest, illegal, unethical conduct, a breach of Commonwealth or State legislation, and/or actual or suspected fraud. A Whistleblower Guide is therefore an important element in detecting fraudulent, illegal or other undesirable conduct.

This guide is designed to:

- encourage and facilitate disclosure of such conduct;
- provide anonymity for staff that make these disclosures;
- provide protection for staff who may fear or suffer reprisals in relation to such disclosures; and
- ensure that the matters disclosed are properly investigated and dealt with.

[JA Member] will ensure that all staff are aware of and can access this procedure through the processes outlined below.

2. What is a whistleblower?

Australian Standard 8004–2003 defines a whistleblower as:

A person being a director, manager, employee or contractor of an entity who, whether anonymously or not, makes, attempts to make or wishes to make a report in connection with reportable conduct and where the whistleblower wishes to avail themselves of protection against reprisal for having made the report. A whistleblower may or may not wish to remain anonymous.

3. Our organisation's policy on whistleblowing

At [name of organisation] we give an undertaking to all whistleblowers that we do not intend to take action against a whistleblower for reporting, and clearly state that all reports will be kept confidential and secure.

A whistleblower who reports, or seeks to make a report, will be given a guarantee of anonymity if this is desired by the whistleblower. This provision is subject to circumstances in which the law requires the disclosure of the identity of the whistleblower in legal proceedings.

Any person who reports reportable conduct as defined by this procedure must not be personally disadvantaged for having made the report by:

- dismissal,
- demotion,
- any form of harassment;
- discrimination; or
- current or future bias.

4. What the Whistleblower Guide seeks to do

The main objectives of a Whistleblower Guide are to:

- encourage the reporting of matters that may cause loss to *[JA Member]* or damage *[JA Member's]* reputation;
- to protect employees who report (anonymously or not) actual or suspected fraudulent activity; and
- assist *[JA Member]* to develop a positive internal culture to encourage disclosure by protecting the identity of reporters.

To do this we will establish a number of measures in conjunction with our fraud control strategies. These will include staff training about the Whistleblower Guide and fraud awareness, the clear delineation of the role and responsibilities of the Whistleblower Protection Officer, and how employees can access the Whistleblower Guide.

5. The role of the Whistleblower Protection Officer

We have an appointed Whistleblower Protection Officer, and this position is currently held by *[insert name of the person who holds the position]*. He/She can be contacted by *[insert relevant contact details]*.

The role of the Whistleblower Protection Officer is to safeguard the interests of the whistleblower in accordance with this guide. He/She has direct, unfettered access to independent financial, legal and operational advisers as required, and a direct line of reporting to the CEO, senior executive and Board, as may be required.

The Whistleblower Protection Officer is responsible for receiving and investigating the substance of reports. On the basis of sufficient evidence in support of matters raised in a report, the Whistleblower Protection Officer determines whether to refer reports for further action, or refute these where necessary. The Whistleblower Protection Officer is to ensure that the whistleblower is kept informed of the outcomes of the investigation of his/her report, subject to the considerations of privacy of those against whom the allegations are made.

We aim to ensure all employees are continuously aware of who our Whistleblower Protection Officer is, and the alternative ways in which employees can contact him/her.

6. How and when does a whistleblower make a report?

A whistleblower should report conduct by any person or persons connected with *[JA Member]* which, in the opinion of a whistleblower acting in good faith is:

- dishonest;
- fraudulent;
- corrupt;
- illegal (including theft, violence or threatened violence, harassment, drug use and criminal damage against property);
- in breach of Commonwealth or State legislation or local authority by-laws
- unethical;
- other serious improper conduct;
- an unsafe work practice; or
- any other conduct which may cause financial or non-financial loss to *[JA Member]* or be otherwise detrimental to the interests of *[JA Member]*.

We aim to ensure all employees remain aware at all times of the alternative reporting methods available to ensure the anonymity and confidentiality of the whistleblower.

These include: *[Choose appropriate examples or Jobs Australia member to add own]*:

- a whistleblower hotline;
- a reporting box/pigeonhole;
- a designated postal address; and
- email, subject to privacy and confidentiality protocols.

If the circumstances require, we will consider using alternative forms of reporting such as an internal or external auditor.

7. Investigating reports

All reports of the conduct outlined above will be investigated to determine whether there is sufficient evidence to substantiate or refute the allegation by a whistleblower. The investigation will be conducted by the Whistleblower Protection Officer or by direction of our Chairperson or other person decided by the Board or CEO, depending on the particular circumstances and allegations. The investigation will not be conducted by a person who may be the subject of the investigation or has inappropriate links or connections (actual or perceived) to the person(s) or practice(s) under investigation¹⁹.

All investigations should be fair, independent and in accordance with best practice. The investigation process should be accountable and open to review. An audit trail should be maintained and critical findings and decisions made during the course of investigations should be documented.

8. How can I access the Whistleblower Guide?

If you are reading this you have accessed the Whistleblower Guide! This document should be made available to all employees by: *[Choose appropriate examples or Jobs Australia member to add own]*

- on [Jobs Australia member] intranet;
- on request from Management;
- on request from the Fraud Control Officer;
- a copy will be given to all new employees; and
- an electronic copy emailed to all current employees.

9. Training

All persons commencing employment with *[Jobs Australia member]* from *[insert implementation date i.e. August 2006]* will receive training about the Whistleblower Guide at induction and throughout the period of their employment.

Current employees will be trained²⁰ about the Whistleblower Guide on *[insert implementation date.]*

¹⁹ AS8004-2003 recommends appointment of a separate Whistleblower Investigations Officer.

²⁰ For example: Jobs Australia member to organise a group session to go through the guide with staff and also advise where a copy of Fraud Control Plan is available.

10. Ongoing Review of the Whistleblower Guide

We will review the Whistleblower Guide annually to maintain and where possible increase its effectiveness.

11. Government Legislation Relating to Whistleblower Protection

Commonwealth legislation contains provisions relating to whistleblower protection which may be more applicable to your organisation than you realise. In many ways it is broader and more relevant for the non-public sector than specific state/territory whistleblower legislation which is generally limited to public officers.

NB: The protection provided to whistleblowers under the *Corporations Act* 2001 is only applicable to those Jobs Australia members who are corporations, that is a company limited by guarantee.

Commonwealth Legislation	Relevant Issues
<p><i>Corporations Act</i> 2001</p>	<p>If an officer or employee of a company, person contracted for the supply of goods or services or employee of a person contracted for the supply of goods or services to a company, in good faith makes a disclosure to ASIC or specified persons (such as a senior manager, auditor or director of the company (s1317AA(b)) which relates to a contravention of the <i>Corporations Act</i> 2001 (s1317AA) ("the Act"), the person who made the disclosure in compliance with the Act is not subject to any civil or criminal liability for making the disclosure (s1317AB(1)(a)).</p> <p>Also, no contractual or other remedy may be enforced and no contractual or other right may be exercised against the person on the basis of disclosure (s1317AB(1)(b)) and if a court is satisfied an employer purports to terminate a contract of employment on the basis of a disclosure, it may order the employee be reinstated (s1317AB(3)):</p> <p>http://www.austlii.edu.au/au/legis/cth/consol_act/ca2001172/</p>
<p><i>Workplace Relations Act</i> 1996</p>	<p>If an officer, employee or member of an organisation or of a branch of an organisation on reasonable grounds makes a disclosure to a specified person (such as the Employment Advocate, a Registrar or authorised officer (s337A(b)) relating to contravention of the <i>Workplace Relations Act</i> 1996 ("the Act") or Schedule 1A of the Act, (s337A of <i>Workplace Relations Amendment (Codifying Contempt Offences) Act</i> 2004 which amends the <i>Workplace Relations Act</i> 1996), the person who made the disclosure in compliance with the Act is not subject to any civil or criminal liability for making the disclosure (s337B(1)(a)).</p> <p>Also, no contractual or other remedy may be enforced and no contractual or other right may be exercised against the person on the basis of disclosure (s337B(1)(b)). Victimisation (including threats or conduct which caused detriment) due to making a disclosure is prohibited (s337C) and a person who</p>

	<p>suffers damage due to someone contravening this prohibition may be compensated in damages by them (s337D):</p> <p>http://www.austlii.edu.au/au/legis/cth/consol_act/wra1996220/</p> <p>http://www.workplace.gov.au/workplace/Category/Legislation/WRAct/WorkplaceRelationsAmendmentCodifyingContemptOffencesAct2004.htm</p>
--	---

Who Does State/Territory Whistleblower Protection Legislation Relate To?

Jurisdiction & Legislation	Includes
VIC <i>Whistleblowers Protection Act 2001</i>	Disclosures of improper conduct by public officers and public bodies only (s1(a)): http://www.austlii.edu.au/au/legis/vic/consol_act/wpa2001322/
NSW <i>Protected Disclosures Act 1994</i>	Disclosures about corrupt conduct, maladministration, and serious and substantial waste in the public sector (s3) by public officials only (s8): http://www.austlii.edu.au/au/legis/nsw/consol_act/pda1994251/
QLD <i>Whistleblowers Protection Act 1994</i>	Disclosures about unlawful, negligent or improper public sector conduct or danger to public health or safety or the environment (s7(1)): http://www.austlii.edu.au/au/legis/qld/consol_act/wpa1994322/
TAS <i>Public Interest Disclosures Act 2002</i>	Disclosures made by public officers only (s6): http://www.austlii.edu.au/au/legis/tas/consol_act/pida2002313/
SA <i>Whistleblowers Protection Act 1993</i>	Maladministration and waste in the public sector and of corrupt or illegal conduct generally (s3): http://www.austlii.edu.au/au/legis/sa/consol_act/wpa1993322/
WA <i>Public Interest</i>	Disclosure relating to performance of a public function, a public authority, a public officer, or a public sector

<i>Disclosure Act 2003</i>	contractor (s3): http://www.austlii.edu.au/au/legis/wa/consol_act/pida2003295/
ACT <i>Public Interest Disclosure Act 1994</i>	Disclosure of conduct of a person (whether or not a public official) that adversely affects, or could adversely affect, either directly or indirectly, the honest or impartial performance of official functions by a public official or government agency (s4): http://www.austlii.edu.au/au/legis/act/consol_act/pida1994295/

Whistleblower Protection Legislation includes the following features:

Jurisdiction & Legislation	Provides for (in some form or another and with some conditions)
VIC <i>Whistleblowers Protection Act 2001</i>	<ul style="list-style-type: none"> • Confidentiality for whistleblowers identity • Prohibition/Protection against reprisals • Absolute privilege against defamation • Anonymous disclosures
NSW <i>Protected Disclosures Act 1994</i>	<ul style="list-style-type: none"> • Confidentiality for whistleblowers identity • Protection against reprisals • Absolute privilege against defamation • Anonymous disclosures
QLD <i>Whistleblowers Protection Act 1994</i>	<ul style="list-style-type: none"> • Confidentiality for whistleblowers identity • Prohibition/Protection against reprisals • Injunctions against reprisals under the Act • Absolute privilege against defamation • Anonymous disclosures
TAS <i>Public Interest Disclosures Act 2002</i>	<ul style="list-style-type: none"> • Confidentiality for whistleblowers identity • Prohibition/Protection against reprisals • Absolute privilege against defamation • Anonymous disclosures
SA	<ul style="list-style-type: none"> • Confidentiality for whistleblowers identity

<i>Whistleblowers Protection Act</i> 1993	<ul style="list-style-type: none"> • Prohibition/Protection against reprisals
WA <i>Public Interest Disclosure Act</i> 2003	<ul style="list-style-type: none"> • Confidentiality for whistleblowers identity • Prohibition/Protection against reprisals
ACT <i>Public Interest Disclosure Act</i> 1994	<ul style="list-style-type: none"> • Confidentiality for whistleblowers identity • Prohibition/Protection against reprisals • Absolute privilege against defamation

NB: A bill is pending in the Northern Territory.