**HUMAN RESOURCES** **UNCLASSIFIED**

# Fraud, Corruption and Misconduct Control Policy

**Effective date: 30/01/2014** **CHA/2014/918**
**Last reviewed: 03/09/2018** **Version: 2.03**

## 1. Purpose

Outlines the process for employees in preventing, and detecting fraud, corruption and other misconduct in the department. It also outlines employees' and managers'/supervisors' obligations to report and manage any wrongdoings related to this policy.

## 2. Policy

The department recognises that the management of fraud and corruption is an integral part of good governance and management practice, and is committed to:

- a zero tolerance approach towards fraud, corruption and misconduct activities.
- ethical and accountable behaviour.
- minimising the risks of fraud, corruption and misconduct associated with its operations.
- addressing any incidents of suspected fraud, corruption or misconduct by its employees.

To achieve this, the department will:

- Ensure that conduct throughout the department reflects the value statements and behaviour statements reflected in the public service values.
- Apply risk management principles to address fraud, corruption and misconduct control.
- Implement appropriate internal controls and risk treatment strategies to minimise fraud, corruption and misconduct and establish clear lines of accountability for identified treatment actions.
- Ensure effective internal fraud, corruption and misconduct reporting mechanisms are implemented and maintained and their availability is communicated to employees.
- Report on incidents of suspected fraud, corruption or misconduct to the appropriate external agency.
- Ensure protection from reprisals is given to employees who make a public interest disclosure in accordance with the *Public Interest Disclosure Act 2010*.
- Pursue available avenues to recover losses and ensure those involved in fraud, corruption or other misconduct do not benefit from such activity.
- Implement a training and awareness program to communicate the Fraud, Corruption and Misconduct Control Policy to employees.

Risk management is a requirement of the Financial and Performance Management Standard 2009 and the *Financial Accountability Act 2009*. The department's policies and procedures relevant to fraud, corruption and misconduct control include the Risk Management Framework and the Applying the Code of Conduct Supplement.

## 3. Principles

### 3.1 Code of Conduct

A strong ethical culture supports the prevention of fraud, corruption and misconduct.

The Code of Conduct provides guidance on the standard of behaviour expected of all employees. Ensuring all employees are aware and receive training in their responsibilities helps create an ethical culture and organisational integrity.

Applying the Code of Conduct Supplement provides more information on how the Code of Conduct works in the department and supports employees in making ethical decisions in their day to day work.

### 3.2 Client and community awareness

The department's external communications reinforce the high standards of integrity and probity that the public can expect in dealing with the department. A Statement of Business Ethics is published on the department's internet site outlining expectations regarding interactions with employees.

Queensland
Government

### 3.3 Risk assessments

Managing risk and perceptions is fundamental to delivering on this commitment to the community.

All department risk management processes are to consider fraud, corruption and misconduct as part of their assessment of risk and identify them in the respective risk registers. Fraud, corruption and misconduct risks and preventive controls should be monitored, tested and reviewed on a regular basis by the risk owner and escalated as required in accordance with the Integrated Risk Management Framework.

When dealing with large investments and sensitive negotiations business areas should consider the requirements for probity in its business dealings with internal and external parties and whther a need exists to engage a probity auditor as part of their risk mitigation strategy.

Internal controls and risk assessments should be tested in conjunction with major change programs to ensure that they remain relevant and effective.

Incidents must be recorded and reported as outlined below. Incidents may not be actual fraud, corruption or misconduct. There may be a system weakness identified or the identification of the absence of a control in a particular situation. Appendix A sets out some of the red flags for identifying fraud and corruption risks. Incidents will also therefore trigger a review of internal controls and risks.

### 3.4 Internal controls

Continual monitoring and reviewing of the department's internal processes is required to be part of normal management process. Further, internal controls may be required to be developed to manage fraud, corruption or misconduct risks.

### 3.5 Reporting of fraud, corruption and misconduct

The reporting and management of allegations of fraud, corruption and misconduct by an employee will be in accordance with the department's complaints management framework. It is the department's policy position that any employee can raise any concerns relating to wrongdoing, including suspicions of fraud, corruption or misconduct to the line supervisor, their manager, their business unit senior executive, the Director-General, the Director Human Resources, the Manager (Governance & Ethics), or the Crime and Corruption Commission - either in person, in writing, anonymously or by email to ethics@daf.qld.gov.au.

Information on fraud, corruption and misconduct allegations is recorded by Human Resources, Governance and Ethics. In addition, Internal Audit reviews the losses register as part of its activities related to endorsing the financial statements.

The department is committed to improving how this information is collated and retained for analysis of emerging trends across the organisation. Internal Audit and Human Resources will develop an appropriate means of consolidating existing recording systems to enable effective trend reporting to the Audit and Risk Committee. Information to be reported will include allegations received, summary of actions, outcomes, recommendations for improvement and value of losses recovered.

The collection, storage, security, use and disclosure of the investigation and reporting of information will be managed as per the *Information Privacy Act 2009*. Access to the information will require a Right to Information (RTI) or application to be made to the RTI and the department's privacy unit.

Allegations of fraud committed by a party external to the department will be managed by the business unit which is the subject of the fraud. The business unit will be responsible for determining whether there is sufficient evidence to suggest fraudulent conduct. If necessary, the business unit may need to engage an external party to assist, such as a forensic accountant.

### 3.6 External reporting

Depending on the nature of the allegations, external reporting may be made to the following:

- Crime and Corruption Commission – Human Resources refers all allegations that raise a reasonable suspicion of corrupt conduct to the Crime and Corruption Commission.
- Queensland Police – Human Resources refers allegations of fraud committed by an employee to Queensland Police. If the allegations of fraud are by an external party, the affected business unit will be responsible for referring the matter to Queensland Police. A Fraud and Corruption Prevention and Response Fact Sheet is available to assist managers with this responsibility.
- Where and how allegations will be referred to the police will vary depending on the nature of the allegations and where they occurred. Employees who are requested to give evidence at trial can seek advice and guidance from the department's legal unit.

- Auditor-General – Internal Audit provides a quarterly report detailing losses incurred from offences or misconduct in accordance with section 21 of the *Financial and Performance Management Standard 2009.*

### 3.7 Public interest disclosures

A public interest disclosure (PID) may exist where the allegations refer to suspected fraud, corruption or maladministration by an employee. Further information about when a PID may exist which will require appropriate management is outlined in the Public Interest Disclosure Policy and Procedure.

### 3.8 Investigations

The CCC Liaison Officer is responsible for initiating investigations into allegations of corrupt conduct or misconduct by employees. Human Resources, Governance and Ethics are responsible for managing disciplinary processes.

The department's complaints management framework provides information on how allegations of fraud, corruption or misconduct will be handled.

Allegations, investigations and disciplinary processes will be handled confidentially.

**Employee awareness and training**

Human Resources will develop a range of training material in relation to ethical conduct including the prevention of fraud, corruption and misconduct.

This will include compulsory training in Fraud and Corruption Awareness, Code of Conduct, ethical decision making and any other required ethical topics. A range of resources is also available for employees, including the Safeguarding the Public's Money: the Importance of Internal Controls presentation, and access to CCC Corruption Prevention Advisories.

Where fraud, corruption or misconduct hot-spots have been identified, Human Resources will work with business units to provide specialised employee training in ethics.

Human Resources will develop other capacity building material including a series of notices to employees for release every six months, outlining employee responsibilities, providing links to appropriate resources and briefly outlining preventative lessons from recent prosecutions and investigations. Informing employees of preventative measures and outcomes is considered essential as it increases awareness that the agency is not immune from fraud, corruption and misconduct risks, treats such events seriously and also ensures similar occurrences elsewhere in the agency are minimised.

## 4. Recovery

The department is committed to maximising the recovery of losses incurred from fraud, corruption and misconduct activities. The department will pursue every possible avenue to recover such losses through the appropriate agencies and legal avenues. For example, employees being directed to pay monies back to the department, monetary penalties being imposed as disciplinary action, monies owed by an employee at the time of termination of employment being recovered prior to final payment being made; as a result of police charging an external party with fraud on the department, seeking restitution through the court process, or requesting repayment of monies fraudulently obtained.

The recovery of losses will limit the financial impact this may have on the department's objectives.

## 5. Authority

*Financial Accountability Act 2009*
Financial and Performance Management Standard 2009
*Information Privacy Act 2009*
*Public Interest Disclosure Act 2010*
*Right to Information Act 2009*

## 6. Scope

This policy applies to:

- All permanent, temporary and casual employees of the Department of Agriculture and Fisheries.
- Persons engaged by the department on a contract for service basis (contractor and consultants).
- Agents who have actual, implied or ostensible authority to act on behalf of the departments including members of boards and committees

## 7. Responsibilities

### 7.1 Director-General

The Director-General bears overall responsibility for the fraud, corruption and misconduct prevention efforts.

### 7.2 Board of Management (BoM) of DAF

BoM has the responsibility to:

- As the departments' risk champions, communicate and support the application of risk management practices to the prevent and control of fraud, corruption and misconduct risk in the department.
- Consider recommendations from the Audit and Risk Committee in accordance with the committee's charter.
- Consider and provide a range of treatment options for extreme and high level risks escalated from business units that are beyond their capability to address.

### 7.3 Audit and Risk Committees

As per the Audit and Risk Committee Charters.

### 7.4 Deputy Director-General, Corporate

- Approve changes to this policy to ensure it is relevant to the changing needs of the departments.

### 7.5 Executive leaders of business groups

- Implement this policy within their area of accountability.
- Be responsible for managing the risks of fraud, corruption and misconduct.
- Develop and maintain operational risk registers to ensure fraud, corruption and misconduct risk is being identified and managed within their service and program areas.

### 7.6 Internal audit unit

As per the Internal Audit Charter.

### 7.7 Director, Human Resources

- Ensure fraud, corruption and misconduct awareness related training is developed and made available to employees and managers.

### 7.8 Director, Planning & Performance

- Report and coordinate information on fraud, corruption and misconduct risks, assurance on effectiveness on controls (also see Director, Finance) and treatment strategies to BOM and the Audit and Risk Committee.
- Periodically review operational risk registers to ensure fraud, corruption and misconduct risk is being identified and managed.

### 7.9 Manager, Governance and Ethics, Human Resources

- Act as the CCC Liaison Officer for the department.
- Ensure advice is provided on issues relating to fraud, corruption and misconduct in the department.
- Ensure allegations of fraudulent or corrupt activity and misconduct by employees are appropriately managed.
- Report to Audit and Risk Committee on numbers and trends of allegations involving fraud, corruption and misconduct.
- Ensure this policy is implemented and reviewed.

### 7.10 Director, Finance unit

- Ensure action is taken in relation to losses in accordance with departmental financial procedures and delegations for losses and write-offs for losses through fraud and corruption.

### 7.11 Managers/supervisors

- Display high standards of behaviour that are consistent with and uphold the ethical values, obligations and standards in the Code of Conduct and Applying the Code of Conduct Supplement.
- Promote conduct that shows integrity, transparency in our interactions with subordinates and upholding the highest professional standards within work areas, including the documentation of decisions associated with the procurement of consultants and contractors.

- Safeguard physical and intellectual assets under their control.
- Safeguard and ensure the legitimate use of information through written confidentiality agreements or Statements of Obligations for contractors and consultants.
- Ensure the efficient use of resources.
- Promptly and appropriately manage allegations or suspicions of fraudulent or corrupt activity or misconduct.
- Inform employees of their responsibility for fraud, corruption and misconduct prevention and detection, including the process for making and managing public interest disclosures.
- Identify and evaluate areas of fraud, corruption and misconduct risk.
- Implement business unit practices to reduce the risk of fraud, corruption and misconduct
- Be aware of their obligations with respect to losses and write-offs under clause 2.24 of the Financial Management Practice Manual
- Report suspected fraud and corruption as soon as possible.
- Maintain open, honest and full communication with employees consistent with the sensitivity of matters subject to the need to maintain the confidentiality and integrity of any investigation.
- Ensure employee awareness and participation in relevant ethics, Code of Conduct and ethical decision making training, and development activities occur for employees under their control.
- Engage probity auditors for high value high risk tendering activities in accordance with the department's procurement policies.

### 7.12 Employees

- Contribute to the development of improved systems and procedures that will enhance the organisations resistance to fraud, corruption and misconduct.
- Demonstrate behaviours consistent with the Code of Conduct and comply with internal control systems.
- Practice high standards of personal honesty and ethical conduct.
- Safeguard physical and intellectual assets under their control.
- Safeguard and ensure the legitimate use of information.
- Report suspected fraud, corruption, maladministration and misconduct.
- Clearly understand their obligations with respect to any losses, deficiencies and shortages.
- Ensure all personal claims are accurate and contain no deliberate omissions or falsifications.
- Complete training and awareness activities in ethics, Code of Conduct and ethical decision making

## 8. Delegations

Delegations are to be exercised in accordance with the Human Resource Delegations and Authorisations. Please confirm delegate authority levels prior to exercising any powers.

## 9. Definitions and glossary of terms

| | |
|---|---|
| *Audit and Risk Committee* | Provides independent assurance and assistance to the Director-General on the risk, control and compliance frameworks, the department's external accountability responsibilities as prescribed in the relevant legislation and standards, and the department's integrity framework |
| *CCC* | Crime and Corruption Commission. |
| *Corruption* | Dishonest activity in which an officer or contractor of an agency acts contrary to the interests of the agency and abuses his/her position of trust in order to achieve some personal gain or advantage for him or herself or for another person or legal entity or to cause a disadvantage to others. |

| | |
|---|---|
| *Corrupt conduct* | Involves wrongdoing by an employee in carrying out their official duties or exercising their powers. It must involve one of the following:<br>• dishonesty or lack of impartiality<br>• a breach of the trust put in a person by virtue of their position knowingly or recklessly<br>• a misuse of officially obtained information.<br><br>It must also be conduct engaged in for the purpose of providing a benefit or causing detriment. It must also be a criminal offence or serious enough to justify dismissal of the person from their position. For example:<br>• Accepting money or other benefits in exchange for helping someone to:<br>  o avoid prosecution<br>  o win a contract<br>  o gain government approval<br>• Stealing an employer's property or cash<br>• Detriment as including detriment to someone's property. |
| *Department* | The Department of Agriculture and Fisheries. |
| *Fraud* | Dishonest activity causing actual or potential financial loss to any person or agency including theft of moneys or other property by employees or persons external to the agency. Often, deception is used either at the time, immediately before or immediately following the activity. Fraud also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose, or the improper use of information or position to dishonestly obtain a benefit for themselves or others. |
| *Control* | An existing process, policy, procedure, system, device, task or other action that is used to modify the likelihood or the consequence of the risk event occurring. |
| *Misconduct* | Conduct, for the purpose of this policy, that is other than fraud and corruption which breaches laws, policies or the Code of Conduct. |
| *Public Interest Disclosure* | Has the meaning given to the term in the *Public Interest Disclosure Act 2010.* |

## 10. Employee complaints and appeals

If an employee is aggrieved by the decision of a delegate they may lodge a complaint. Refer to the employee complaints process on the department's intranet for further information or contact your HR network representative.

## 11. Related documents

Applying the Code of Conduct Supplement
Public Interest Disclosure Policy and Procedure
Contact with Lobbyists Policy and Procedure
Fraud and Corruption Prevention and Response Fact Sheet
Safeguarding the Public's Money: the Importance of Internal Controls
Risk Management Framework (DAF) and Risk Management Framework (DTESB)
Audit and Risk Committee Charter (DAF) and Audit and Risk Committee Charter (DTESB)
Operational Risk Register

## 12. References

Code of Conduct for the Queensland Public Service

## 13. Further information

Available on the department's intranet

- Fraud, corruption and misconduct prevention
- Complaints management
- Employee complaints
- Human Resource Delegations and Authorisations
- Financial Management Practice Manual
- Risk management
- Procurement policies and framework

External

- Crime and Corruption Commission (CCC) – Fraud and Corruption Control: best practice guide
- Crime and Corruption Commission (CCC) – prevention advisories
- Fraud Control in Australian Government Entities (Australian National Audit Office)

## 14. Review

The policy will be reviewed on an ongoing basis and following legislative changes or changes in conditions.

## 15. Approval

| | |
|---|---|
| Karenne Graham<br>Director<br>Human Resources<br>Department of Agriculture and Fisheries | Sinead McCarthy<br>Deputy Director-General,<br>Corporate<br>Department of Agriculture and Fisheries |
| Date: 02/10/2018 | Date: 02/10/2018 |

## 16. Version history

| Date | Version | Action | Description / comments |
|---|---|---|---|
| 30/01/2014 | 1.00 | Endorsed | New Policy |
| 22/04/2015 | 2.00 | Update | Changes to: department name, risk management, Crime and Corruption Commission and its jurisdiction. |
| 19/05/2016 | 2.01 | Edited | Corrected broken links and formatting. |
| 19/09/2016 | 2.02 | Edited | Change official misconduct definition to corrupt conduct definition and change CMC to CCC. Minor amendments to roles, responsibilities, terminologies and definitions for consistency across documents. |
| 25/07/2018 | 2.03 | Edited | Change to reflect policy relevant to DAF only; minor change to reflect recommendation from audit to include recovery plan. |
| 02/10/2018 | 2.03 | Approved | Changes reflected in v 2.03 approved by Director, HR |

## 17. Keywords

Fraud, corruption, misconduct, public interest disclosure, financial management, lobbyists, complaints management, prevention, risks, red flags

## 18. Appendix A - Identifying fraud and corruption related risks – Red flags

### How do I identify a fraud, corruption or misconduct risk?

- Focus on what opportunities there may be for inappropriate behaviour by employees and clients in your business.
- If in doubt, raise the issue and discuss it with peers and management through the risk management process.
- You know the nature of your business and what you are going through at the moment; do any of the red flags apply to your areas?
- Risk versus a suspected actual fraud – if you suspect actual fraud or corrupt behaviour, refer it to a delegate and/or seek advice from HR Governance and Ethics.

Some discussion points

- Emerging areas of research – do managers/supervisors understand the potential and appropriate controls or is excessive reliance placed on one employee?
- Regulatory employees in isolated areas – one-on-one contacts, limited independent overview of decisions, where are the checks and balances?
- Changing organisational structures – does everyone know to whom they report? Do all delegates know for whom they are signing and what they are signing? Are exceptions followed up? E.g. a person seeking approval from someone other than their usual supervisor.
- How do you control time-cheating?
- New relationships with new industries – are we working to the same ethical principles and obligations? Is there scope for misunderstandings about what is appropriate? I.e. gifts and benefits, contacts during contractual negotiations, expectations related to IP sharing.
- Known low-compliance areas – are there areas where you know the views related to proper procedure are seen as unnecessary overheads? Are there areas where any enquiries related to administrative matters are greeted with hostility, bluster, avoidance?
- Information and intellectual assets – how easy is it for information and intellectual assets to go missing or be misused?
- Recruitment – do you see a need for identity checks and detailed reference and experience checks? How is this done in an emergency?
- Vehicles – is there an unwillingness to record details of use?

### Red flags for fraud and corruption[1]

### Organisational

Potential red flags indicating corruption, which have been seen in organisations where corruption has subsequently been uncovered.

- Over-zealous acquisition strategies (without proper screening and due diligence, avoiding State Purchasing Policy requirements, every purchase seen as urgent)
- Autocratic management decisions regarding business relationships, such as a refusal to change a major supplier
- Not recovering costs or making profits, unexplained shifts in revenue/expenditure patterns
- Artificial barriers put up to avoid answering questions
- Excessive secrecy
- Rumours and low morale
- A complacent project leader/manager
- Overriding of budgetary controls
- Discrepancies and deviations
- Missing records or lack of detail
- Manual payments or adjustments
- Consultants given a free reign.

[1] Source – WA Department of Education and Training: Corruption Policy and Control Plan - adapted from SIRCA 01-2003 Fraud Resistance: A Practical Guide

**Individual**

Red flags in behaviour can either be objective (in that they can be measured or monitored) or subjective (in the sense of being reliant on the managers/ supervisors knowledge of the employee).

Objective red flags are reasonably positive indicators that something is wrong, and can usually be monitored in order to establish the cause of the change in behaviour. Objective red flags can include:

- Signs of excessive wealth or spending, increasing debts and lack of wealth, changes in personal circumstances
- Long absences from work, poor timekeeping
- Failure to take leave
- Changes to work patterns, long hours after normal business hours
- Manager override of normal controls
- Excessive use of facilities (i.e. telephone, computer or internet) outside normal work areas
- Obvious unethical or immoral behaviour
- The finding of a false background
- Running another business while at work
- Managers bypassing subordinates
- Subordinates bypassing managers
- Review of potential conflicts of interest reveals undeclared personal, business or family relationship with another employee;
- Placing undated/post-dated cheques in petty cash
- Excessive employee turnover
- Unexplained employee absences
- Personal creditors appearing at or contacting workplace
- Using government facilities while on leave (e.g. car, corporate card)

Subjective red flags are more difficult to rely on — they should always be linked to other red flags in the process or systems to which an individual has access.

Subjective red flags include:

- Abnormal social behaviour
- Problems with gambling, drug or alcohol abuse
- Excessive mood swings, aggression, marked changes in behaviour
- Discovered to be a liar, cheat or lawbreaker
- Overeager to assume other people’s duties or to provide help
- Refusal to relinquish duties
- Excessive, undeclared use of corporate hospitality
- Resistance to audit and questions
- Answering questions and deflecting attention — arrogant and aggressive
- Providing misleading or ambiguous explanations to questions
- Gambling (including playing the share market) while at work
- Borrowing money from fellow employees while at work
- Secretiveness
- Refusal, evasion or delay in producing files, minutes or other records
- Marked character changes
- Excessive or apparent total lack of ambition
- Excessive control of records by one officer
- Covering up inefficiencies

### Process

Red flags in a process arise from anomalies on documents or transactions. For example, red flags on payment instructions being processed include;
Even though accounting and payment employees perform a routine activity with hundreds of transactions per day, they can sometimes spot these anomalies very quickly.

- Unusual delivery instruction (e.g. a purchase order made out to a place other than a department office) with an urgent processing request
- Photocopied document or attachment
- Unnecessary words or explanations on the instruction to try and make it seem more plausible
- Appearance or style not consistent with normal transactions
- Beneficiary name spelt incorrectly — mismatch with account number, vendor name/number
- Payment not consistent with the normal business of the vendor or business group
- Missing expenditure vouchers and unavailable official records
- Crisis management coupled with a pressured work environment
- Excessive variations to budgets or contracts
- Lack of executive or management oversight
- Reconciliations are not maintained or can’t be balanced
- Excessive journals
- Petty cash advances are not used
- Unauthorised changes to systems or work practices
- Lowest tenders or quotes passed over with minimal or no explanation recorded
- Lost or missing assets
- Absence of controls and audit trails
- Lack of clear financial delegation

### IT based

Systems red flags arise from monitoring routines built into computer and communication systems. They are a powerful means of detecting illicit behaviour. For example:

- Someone logs on to a system using the user identification and password of an employee who is on leave; or attempts to sign on if the password is disabled while the employee is on leave
- A higher than average number of failed logins
- Sign-on from areas outside normal work area
- Signing on at unusual times of the day
- Unusual network traffic
- Controls or audit logs turned off

## 19. Appendix B - Fraud, Corruption and Misconduct Control Plan

| | | | |
|---|---|---|---|
| **Date reviewed** | | **Endorsed by** | |

| Risk | Proposed actions | Responsible officer | Timeframe | Performance measures | Reporting and monitoring |
|---|---|---|---|---|---|
| Describe high or extreme risk from risk assessment process | Change or introduce new controls | Name of officer esponsible | When to be completed | | From who and when reports are to be completed |
| Example | | | | | |
| Staff inappropriately accessing, using or releasing politically sensitive information relating to policy /business programs | • Staff training in Code of Conduct and information security<br>• Facilities are available to lock sensitive information<br>• Shredders and security bins are available to all staff<br>• Implement WOG Information Classification Scheme<br>• Increased vigilance by line managers | | | Audits show no improper claims | Report to HMU/BOM every month until completed |
| | | | | | |
| | | | | | |