1. **Statement**

This Guideline supports implementation of the Fraud Control Policy and Standard.

2. **Scope**

This Guideline provides information for all employees, contractors and consultants within the Department of Health divisions and commercialised business units.

3. **Requirements**

3.1 **Guideline for Fraud and Corruption Control**

3.1.1 **Commitment to fraud control**

The Department of Health (the department) has zero tolerance for corrupt conduct, fraud and maladministration. This is supported by a hierarchy of governance and controls which will continue to build an ethical organisational culture.

The department has adopted a structured governance framework and an integrated approach to the development, implementation and regular review of fraud prevention and detection, monitoring, reporting and response strategies. The framework is based on the Australian Standards Fraud and Corruption Control (AS 8001-2008). Refer to Appendix 1 for the compliance schedule.

The Department of Health Fraud Control Policy and Implementation Standard has been endorsed by the Departmental Management Team and approved by the Chief Legal Counsel for implementation. The Chief Risk Officer maintains ongoing custodianship of the Policy, Standard and Guidelines.

3.1.2 **Four major components of the Guide to Fraud and Corruption Control**

The four essential elements of fraud and corruption control are contained in Table 1.

<table>
<thead>
<tr>
<th>Table 1 Components of the Guide to Fraud and Corruption Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Ethical Culture</td>
</tr>
<tr>
<td>2. Prevention</td>
</tr>
<tr>
<td>3. Detection</td>
</tr>
<tr>
<td>4. Response</td>
</tr>
</tbody>
</table>
3.1.3 Review of the Fraud Control Guideline
This plan will be reviewed at least every two years but a review can be initiated at any time by changes in the policy environment.

3.1.4 What is fraud and corruption?
The definitions of fraud and corruption are provided in the Fraud Control Policy. For some examples of fraud and corruption, refer to Table 2 below.

<table>
<thead>
<tr>
<th>Internal</th>
<th>External</th>
<th>(Joint) Collusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>• False claims for travel, petty cash, overtime and expenses</td>
<td>• Hacking into, or interfering with a computer system (this may also occur from within the organisation) for personal gain.</td>
<td>• Certification for goods or services as being delivered when they are not</td>
</tr>
<tr>
<td>• Misuse of corporate credit cards and cab charge</td>
<td>• Charging for goods or services that are incomplete or not delivered</td>
<td>• Unlawful or unauthorised release of information</td>
</tr>
<tr>
<td>• Falsifying invoices for goods or services</td>
<td>• Fraudulently inflating invoices.</td>
<td>• Knowingly making or using forged or falsified documentation</td>
</tr>
<tr>
<td>• Dishonestly using purchase or order forms to gain a personal benefit</td>
<td></td>
<td>• Collusion with external vendors (e.g. kickbacks and providing insider information etc.)</td>
</tr>
<tr>
<td>• Dishonest use of intellectual or confidential property</td>
<td></td>
<td>• Raising fraudulent invoices and colluding with an authorising officer to approve them</td>
</tr>
<tr>
<td>• Falsifying hours on timesheet</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Working elsewhere without permission whilst on leave (e.g. sick leave)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Creating false entries in the Dangerous Drugs Register to obtain controlled drugs</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Financial statement fraud (fraudulent inflation of assets to give an inaccurate representation of profit)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Creating false bank accounts to siphon money.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• False information on CV.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

3.2 Ethical Culture
3.2.1 Fraud Control Education and training program Understanding why people commit fraud – The Fraud Diamond
The Fraud Diamond at Figure 1 describes the four key contributing elements to fraud within the department. Fraud is more likely to occur when:
• a person has an incentive or pressure to commit fraud eg gambling addiction
• weak controls provide a person with opportunities to commit fraud
• the person has the capability to recognise the opportunity to commit fraud and takes advantage of it
• the person rationalises committing the fraudulent behaviour.
Raising awareness of the above four contributing elements can support an ethical culture and assist staff in recognising early warning signs of fraudulent activity (red flags).

![The Fraud Diamond](image)

*Figure 1 – The Fraud Diamond*

Adapted from *The Fraud Diamond: Considering the Four Elements of Fraud*, David Wolfe and Dana Hermanson (2004)

3.2.2 Embedding an ethical culture

Raising awareness of ethical behaviours will assist in minimising the risk of fraud across the organisation.

The organisation’s expectations on ethical behaviour are outlined in the Code of Conduct which describes its commitment to creating and maintaining an environment which is professional, client responsive, safe and free of any form of unlawful or inappropriate behaviour. This commitment supports the expectations of the people of Queensland that all activities of the department are conducted with efficiency, impartiality and integrity.

3.2.3 Fraud Control Education and training program

Fraud and corruption often goes undetected because of lack of knowledge by staff in recognising the early warning signs of fraudulent activity. Staff may be unaware of how to report their suspicions or have a lack of confidence in the integrity of the complaints management processes. The department has mandatory fraud awareness training to assist in raising the awareness of fraud and how they should respond should this type of activity be suspected or detected.

Fraud awareness training is available online and through the Risk and Governance Unit, Legal and Governance Branch, System Support Services Division. Managers or executives may commission additional training specifically related to their area of business operations.

The Risk and Governance Unit will also implement targeted education and training with risk and control custodians. This will provide a bespoke extension to the standard, online training and will offer an in depth analysis of fraud risks, controls and treatments specific to the work area.

In addition, every February the department hosts ‘Fraud Awareness Month’. This is an opportunity to revisit lessons learned and promote awareness of new, emerging or changing fraud risks. During Fraud Awareness Month managers are encouraged to facilitate discussions with their work groups regarding the importance of fraud awareness and effective fraud controls. Fraud Awareness Month is coordinated by the Risk and Governance Unit.

3.2.4 Tasks for improving an ethical culture

Additional best practice tasks for improving an ethical culture include:

- fraud and corruption control responsibilities form part of the performance management framework
- ensuring all staff receive information on the Fraud Control Policy, Standard and the Code of Conduct upon induction
• ensuring updates and changes to relevant policies and procedures are effectively communicated to all staff
• confirming that all staff have participated in relevant training including Ethics, Integrity and accountability (Code of Conduct) training
• regular liaison between Executives and key branches, including Risk and Governance, Human Resources, Internal Audit, Finance, Payroll, Procurement and Conduct Advisory Services.
• regular discussion of standards of conduct or behaviours at team/unit meetings
• use of available media to disseminate fraud awareness materials, including newsletters, intranet information, emails, leaflets
• roll-out of the fraud awareness e-Learning package across the department
• measurement of staff awareness levels through an ethical culture survey
• regular liaison with Communication staff to ensure that key messages are disseminated effectively.
• annual Fraud Awareness Month to reinforce key fraud control messages.

These initiatives should be supported by effective and continuous communication and example-setting by management (tone from the top approach).

3.3 Prevention

Key aspects of a fraud prevention program include:
• ensuring managers are aware of and accountable for identified fraud risks, policies, procedures and systems within their jurisdiction
• ensuring internal controls are in place to manage potential fraud risks
• identifying control weaknesses and implementing measures to address these weaknesses
• regular fraud risk assessments to identify potential risks and control weaknesses and appropriate treatments
• proactive treatment of fraud risks and assessment of existing control effectiveness
• continuous monitoring of controls.

3.3.1 Internal controls

Internal controls are often the first line of defence against fraud. The department maintains a strong internal control system and promotes and monitors the use of effective internal controls. The Financial Management Practice Manual describes key elements of the internal control system including reporting pathways, delegations, and procedures for monitoring the performance of, and accounting for, departmental investment.

Effective internal controls are developed and maintained through the cooperation of multiple work areas within the department including the governance, internal audit and finance units.

3.3.2 Fraud and corruption risk assessment

The department adopts a formal identification, analysis and evaluation of fraud and corruption risks through a periodic assessment of risks of fraud and corruption. The following section identifies key areas which are particularly susceptible to fraud risk. It should be noted however, that regardless of the business area concerned, fraud risk is heightened when executives and managers fail to properly manage people, systems and processes. It is the responsibility of management in the department to clearly articulate to staff their roles, responsibilities and expected standards of behaviour.
Furthermore, if specific, identified fraud risks exist within a manager’s business unit or jurisdiction, it is the responsibility of that manager to monitor, control and/or treat that risk. If a change in the business environment occurs which impacts on a fraud risk, it is the responsibility of the manager or fraud risk owner to ensure the risk is updated on the fraud risk register via the QH Risk tool which is accessible via the QHEPS intranet site (see 6.3).

3.3.3 Fraud and corruption risk identification

Fraud and corruption risk identification is the process of finding, recognising and recording risks. Whilst employees are responsible for their own behaviour and actions, managers have a responsibility to ensure they provide a clear message that the types of behaviours and activities outlined in the following examples are unacceptable and will not be tolerated. Particular attention should be paid to fraud control in the following areas:

i. Correspondence and information management

All employees must ensure confidential information and personal information relating to individuals’ own privacy is securely held and only used for the purpose for which it was collected.

The following are examples of inappropriate use of correspondence and information resulting in fraud and corruption:

- A former employee obtaining confidential information and providing it to a new employer to aid their dealings with Queensland Health
- An employee leaking commercial-in-confidence information obtained through the performance of their work to a member of the public.

Managers should ensure their staff are aware of their obligations and responsibilities regarding the management and control of correspondence and information.

ii. Delegations

Delegation of authority within the department establishes who is empowered to make decisions and to take action on its behalf. The department’s Delegations Policy and Implementation Standard identify requirements, roles and responsibilities in relation to delegating decisions, authority or power.

Staff may exercise their delegation through actions such as approving expenditure, requisitions or purchase orders, approving appointments or leave applications, or signing a contract that commits the department to expenditure.

The following are examples of inappropriate use of delegations resulting in fraud and corruption:

- Using delegation for fraudulent or corrupt purposes, such as awarding a contract to a contractor without proper due consideration of alternative suitable providers as per Queensland Health procurement policy and procedure.
- Exceeding delegated authority eg authorising an invoice for $15,000 where the limit is $10,000.

Employees with delegated authority are responsible for ensuring they understand their delegations and use them appropriately.

iii. Facilities and public resources

All departmental employees are accountable for resources they use or have access to in the course of performing their duties. The Code of Conduct for the Queensland Public Service Section 4.3 requires all employees to be economical, avoid waste and extravagance when
using public resources for their proper purposes and use any public resource in accordance with Queensland Government and agency policy.

The poor management and misuse of public resources can undermine the integrity and operational efficiency of the department as a Queensland Government agency thereby not providing the public with value for money.

The following are examples of misuse of resources resulting in fraud and corruption:

- Regularly taking resources, such as office supplies, stationery or equipment, home for personal use, or to sell for personal benefit
- Deliberately over-ordering resources to use the surplus for personal gain.

iv. Finance


It encompasses all requirements imposed upon the public sector such as the Code of Conduct for the Queensland Public Sector, and incorporates all legislative requirements, whole of government requirements and generally held notions of best practice.

Compliance with the FMPM is mandatory. Managers of non-finance operational units should be aware of the sections of the FMPM that affect their particular area of operation. All staff directing and undertaking financial operations should familiarise themselves with the relevant requirements of the FMPM.

The following points represent some examples of fraud and corruption as they may relate to finance functions:

- manipulating the financial system to make payments to a non-existent supplier, for personal financial gain
- approving invoices for private expenses or colluding to do so for others
- senior management inflating balance sheet values to cover up poor performance or mistakes
- failing to record purchases properly in order to disguise a fraudulent gain
- charging personal expenses to a corporate credit card
- misusing Cabcharge vouchers for personal use or profit
- allocating grant funds in contravention of departmental policy and procedure in order to obtain a financial benefit.

v. Human resource management

Human resource management in the department is governed by policies and industrial awards and directives that are issued by the Queensland Government’s Public Service Commission.

The following points represent some examples of fraud and corruption in the management of human resources:

- manipulating recruitment and selection procedures to secure the appointment of a close friend or family member
- promoting, engaging or giving an employee advantage over others for personal reasons
- unfairly disadvantaging, bullying, intimidating or discriminating against employees for personal reasons (for example, unlawful use of authority in order to derive a personal gain)
- a job candidate falsifying qualifications, employment history or references to enhance their prospects of securing a position
vi. Information management and information technology
The department maintains a range of information management and technology policies and standards regarding its information resources. Compliance with these policies and standards is mandatory for all employees.
The department is reliant on information management and information technology systems to perform its functions. It is imperative that information maintained on these systems is accurate, complete and uncorrupted. It is critical for the organisation’s efficient and productive operation that the information contained on its systems is easily accessible for legitimate purposes while being protected from any misuse.
The following points represent some examples of fraud and corruption risks:

- placing malware (for example, viruses, spyware) on departmental information technology system in an attempt to damage software or information held on the system
- using another employee’s log-in to gain network/system access
- an IT contractor providing information about the department’s information technology system to a third party who uses the information to attack the department’s systems
- an IT contractor building a ‘back door’ into information technology systems that enable unauthorised access to the department’s electronic data and records.

vii. Legal and contractual compliance
The department enters into legal contracts (for example, agreements, deeds, service contracts, memorandums of understanding,) to meet service delivery obligations.
The following points represent some examples of fraud and corruption risks:

- a contract manager fails to declare a conflict of interest but continues to deal with an associate, who is a personal friend and director of a company the department procures services from.
- solicits or accepts a bribe in order to exercise, or not exercise, their authority in a certain way
- a contract manager who fails to properly monitor the quality of the work performed by a service provider, resulting in payment of invoices for work which has not been performed.

viii. Regulatory compliance
There are two main areas of risks associated with regulatory compliance in the department. First, the department is subject to legislation and there may be risks associated with breaching the requirements of legislation (as covered in the previous sections). Second, Queensland Health acts as a regulator and as such, risks may be present regarding the appropriate or inappropriate use of power in this role as regulator.
The following points represent some examples of fraud and corruption risks:

- issuing a license to an individual or business based on factors other than objective assessment criteria (e.g. personal relationship)
- deciding or recommending not to pursue prosecution because of a personal relationship with the person or business in breach of legislation
- choosing not to audit a person or business because of a relationship with that person or business.

ix. Procurement
The department must comply with the Queensland Procurement Policy to ensure that principles, processes and procedures uphold the integrity of procurement decision making.
The following points represent some examples of fraud and corruption risks:
- Knowingly making payments on fraudulent procurement related claims
- Splitting an order to avoid obtaining competitive quotes in the tending process or to ‘work around’ delegation limits for procurement transactions.

x. Organisational Change
Fraud risk may be heightened in times of organisational change eg machinery of government changes, restructures, response to emergent situations or a migration to a new information system. Poorly managed organisational change can lead to confusion or ambiguity in reporting lines, roles and responsibilities which can create the right conditions for fraud to occur.

The following are some examples of fraud risk during times of organisational change:
- two business units merge and some staff are unsure who to submit their timesheets to due to a lack of communication. This results in failure of some staff to account for their hours of work.
- the oversight of a rarely used fund source is overlooked in the midst of a significant departmental restructure.

3.3.4 Fraud and corruption risk analysis
Analysing fraud and corruption risks is a key component for creating an effective ethical culture. The analysis phase involves developing an understanding of the risk. It provides input into risk evaluation and to decision-making on whether risks need to be treated. Subsequently, the information gathered will determine the most appropriate risk treatment options and methods.

The risk analysis process as per the Queensland Health Implementation Standard for the Use of the Risk Analysis Matrix (QH-IMP-070-2:2011) shall be used to:
- determine the possible outcome should a risk occur and the likelihood of the risk occurring using the Consequence and Likelihood tables
- determine the level of risk rating (using the Queensland Health Risk Analysis Matrix)
- determine the current and projected level of risk.

3.3.5 Fraud and corruption risk evaluation
Analysis of fraud and corruption risk against Queensland Health’s risk analysis matrix takes into account the impact of the risk on the department, and the existing, available governance controls.
A robust risk evaluation assists the department to decide on the responsible courses of action to take an integrated approach to fraud and corruption risk management and it can include the following evaluation considerations:
- whether a fraud and corruption risk needs a formal treatment plan, or appropriate additional controls
- whether resources should be dedicated towards undertaking an activity (a course of action)
- priorities for the treatment of identified risks linked to the areas of fraud and corruption.

3.3.6 Fraud and corruption risk treatment
In treating the risks, decisions are made on the most appropriate treatment (additional controls) to be pursued for each fraud or corruption risk. Consideration of treatments should include both positive and negative outcomes that may arise from implementing each fraud and corruption treatment option.

The key objective in completing risk treatments for high fraud or corruption risks is to provide specific actions to be developed, processes implemented and timeframes assigned to
appropriate departmental employees. This will assist in formally managing, monitoring, reducing or eliminating the identified risk associated with fraud and corruption.

3.3.7 Monitor and review of fraud and corruption risks
Risk registers and risk treatment become reference material during the monitor and review phase. Fraud risk owners are responsible for monitoring and reviewing their own fraud risks. Decisions undertaken for review, evaluation and treatment of risk should consider the total cost of the fraud or corruption risk under consideration, including increases or reductions in spending on controls as a result of the proposed treatment options.

3.3.8 Pre-employment screening
The Queensland Health Criminal History Checking Policy is committed to maintaining public confidence in the integrity of all staff and as such all persons to be engaged in general employment, permanently or when the period of employment is expected to exceed three months, are required to have a criminal history check.

Pre-employment screening is one effective means of preventing fraud. For example, pre-employment screening may detect falsified qualifications or employment history. Criminal history checking may identify previous criminal convictions for offences within Australia or New Zealand. Selection panels, delegates for appointments, recruitment units and human resources managers shall ensure employees, prospective employees and other persons have the requisite criminal history check prior to appointment.

At the manager’s discretion, current employees may be required to undertake a criminal history check when their employment circumstances change (e.g. secondment, higher duties, promotion, transfer, deployment etc).

Upon appointing a new staff member, the department should undertake the following as a minimum:

- Verification of identity
- Verification of right to work in Australia
- Police criminal history check / blue card
- Reference check

3.3.9 Information Sharing
Information pertaining to fraud related events (internal or external to the department), trends and analysis of data will be shared with relevant stakeholders. This will be coordinated by the Risk and Governance Unit in cooperation with CAS and as necessary, Queensland Audit Office (QAO) and the Crime and Corruption Commission (CCC).

3.3.10 Contractor and supplier due diligence
The department will perform effective due diligence on contractors and suppliers which may include the following:

- Search on company register
- ABN confirmation
- Verification of persons/positions authorised to commit the contract/supplier to a contract
- Assessment of financial viability
- Trading address verification
- Media search such as Google etc.

The department will consider ongoing commercial relationships and reassess a future working relationship if it is found that there is a real or perceived increased risk of fraud or corruption.
3.3.11 Tasks for fraud prevention
Additional best practice tasks for fraud prevention include the following:

- the Director-General and/or the Chief Risk Officer in conjunction with the Fraud and Corruption Working Group may request audits/reviews of specific areas of concern.
- monitoring of actions taken following recommendations made by the Crime and Corruption Commission as a result of proactive reviews and investigations.
- clear and consistent communication by executives/managers regarding adherence to relevant internal controls, policies, procedures, systems and expected standards of conduct.
- routinely identifying possible conflicts of interest particularly in high risk areas such as finance, procurement and human resource management.

3.4 DETECTION
Despite prevention activities, fraud and corruption may still occur. Therefore it is important specific strategies are in place to detect and report fraud as soon as possible after it has occurred.

3.4.1 Reporting instances of fraud
As per the Standard and HR Policy E9 (Requirements for Reporting Corrupt Conduct) all departmental staff who become aware of suspected fraudulent or corrupt conduct have an obligation to report the matter and must do so immediately.

It is recommended that suspected fraud be reported through line management in the first instance, who will arrange for the matter to be referred to Conduct Advisory Services (CAS). However, for instances where this is not appropriate, a staff member may report the matter directly to CAS (CO_Complaints@health.qld.gov.au) or the Crime and Corruption Commission (http://www.ccc.qld.gov.au/corruption/report-corruption/how-to-report-corruption).

Staff reporting allegations of fraud or corruption must maintain confidentiality i.e information regarding the alleged fraud or corruption must only be shared with persons directly involved in receiving, assessing or managing the complaint. Once a report is made, take no further action until advised by CAS.

The department will ensure complaints and disclosures are managed impartially and in accordance with the Public Interest Disclosure Act 2010 and HR Policy I5 Public Interest Disclosures.

3.4.2 Protection for persons making a public interest disclosure
The Public Interest Disclosure Act 2010 supports the disclosure of improper conduct or wrongdoing. One of the primary objectives of the act is to provide protections for persons who, in good faith, report wrongdoing. For a complaint to be considered a public interest disclosure it must be assessed against strict criteria. In the Department of Health this assessment is conducted by CAS.

3.4.3 Identification of early warning signs (red flags)
Identifying and acting on possible warning signs (red flags) can play an important role in the early detection of fraud. Fraud awareness training promotes understanding of red flags amongst staff.

Red flags do not indicate guilt or innocence, but they may provide warning signs of possible fraud. Red flags are often categorised as either behavioural or transactional. Transactional red flags refer to unusual or out of the ordinary business or financial transactions. Behavioural red flags refer to unusual behaviours or traits exhibited by a person. Some examples are provided
in the table below. It should be noted that a person engaging in fraud will often exhibit a combination of warning signs such as those listed in table 3. It is therefore important to consider the context and the bigger picture.

### Transactional Red Flags
- Transaction occurring at an unusual time (e.g., a cab charge receipt for a taxi fare on a Saturday evening)
- Frequency of the transaction is unusual (e.g., the transaction may be a one-off, or an unusual transaction consistently processed at a certain time by the same person)
- Place of transaction is unusual (e.g., corporate card transaction from a casino or clothing store)
- Amount of the transaction is unusual (e.g., amount of transaction just under the delegated authority of a person, an invoice split into two halves in order to appear within delegation limits)
- Unusual relationships between persons (related parties, over personalised relationship between parties, management performing clerical functions which could easily be delegated to subordinate staff).

### Behavioural Red Flags
- Gambling addiction, substance abuse/addiction problems
- Creditors or collectors appearing/contacting the workplace
- Overly familiar, non-professional relationships with contractors/suppliers.
- Refusing vacations, sick leave or promotions
- Lack of a strong code of personal ethics
- Deliberate disregard for internal controls
- Prior criminal history (charges and/or convictions)
- Unnecessary retention/control of records or business functions
- Insisting on working unusual or non-standard business hours
- Avoiding or delaying provision of documentation when requested by Auditors.
- Giving gifts to peers, supervisors or colleagues in positions of influence
- Lack of transparency, vagueness or dismissiveness to questions regarding roles, functions or projects.

### 3.4.4 Data analysis program
Data analysis is a powerful means of detecting fraud and other improper behaviour. It is a process of uncovering patterns and relationships in datasets that appear unrelated and it can also highlight discrepancies which may indicate fraud and irregular behaviour.

The Director, Internal Audit is responsible for ensuring that the data analysis program focuses on key risk areas including key fraud risks. The data analysis program is aimed at strategic use of computer systems in the identification of fraud indicators. Using data analytic techniques, trends can be examined and investigated which may be indicative of fraudulent conduct. In addition, continuous monitoring by key control owners such as finance and payroll also supports good practice.

### 3.4.5 Post-incident review
The department, through the Fraud and Corruption Working Group, will ensure an effective review process following an incidence of significant fraud. This includes a broader assessment of the issue/s and putting into practice the feedback from lessons learned.
3.4.6 The role of internal audit
Internal audit supports efforts to establish a culture that embraces ethics, honesty, and integrity. Internal audit assist with the evaluation of internal controls used to detect or mitigate fraud, and may be involved in fraud investigations.
Internal audit is the last line of defence for assessing the effectiveness of internal controls. The Internal Audit unit may receive directives from management, the Fraud and Corruption Working Group or the Audit and Risk Committee. Therefore, the Internal Audit unit may play a variety of consulting, assurance, advisory, and investigative roles in the department's fraud management process.
Internal Audit has regular, direct access to the department’s executive via representation on the Audit and Risk Committee.

3.4.7 External audit
The department will take a proactive approach and will liaise with the Queensland Audit Office to facilitate the exchange of information in relation to the prevention and detection of fraud, and will respond quickly to concerns identified during the course of external audit work.

3.4.8 Fraud Control Officers
There are three Fraud Control Officers with specialist skills, qualifications and experience who work together to lead fraud and corruption control policy, planning and programs within Queensland Health: Chief Risk Officer, Director Governance and Principal Prevention Officer. For example:
- Director Governance works together with the Chief Risk Officer and Principal Prevention Officer to develop and maintain departmental policies and standards
- The Principal Prevention Officer ensures current best practice in fraud control is integrated into training and development programs, works with the Chief Risk Officer to develop and maintain departmental policies and standards, and works with the relevant risk owners to manage the department’s exposure to fraud risk.

Whilst the Chief Finance Officer (CFO) is not one of the designated ‘Fraud Control Officers’, the CFO is accountable for the financial control framework.

3.4.9 Tasks for fraud detection
Where appropriate, fraud detection measures should be communicated and promoted to all staff. Awareness of detection measures often acts as a deterrent and therefore, a preventative measure. Additional best practice tasks for fraud detection include the following:
- The Director-General and/or Chief Risk Officer may request audits/reviews of specific areas of concern.
- Reinforcing to staff their obligations to report wrongdoing.
- Fraud awareness training.

3.5 RESPONSE, OUTCOMES AND RECOVERY

3.5.1 Assessing and managing complaints of suspected fraud
The Manager, Conduct Advisory Service shall respond to reports of suspected fraud or corruption by:
- Assessing each matter to determine whether or not it meets the thresholds for corrupt conduct or a public interest disclosure.
- If the matter could amount to corrupt conduct, making appropriate referrals to the Crime and Corruption Commission.
- If the matter is assessed as a public interest disclosure, making appropriate referrals to the Queensland Ombudsman’s Office.
- Where appropriate, referring serious allegations of fraud or corruption to the Queensland Police Service on behalf of the department.
- Overseeing and coordinating investigations in accordance with the Crime and Corruption Commission guidelines as outlined in their publication ‘Corruption in Focus’.
- Reporting on system weaknesses to relevant internal and external stakeholders e.g. Risk and Governance Unit, Queensland Audit Office, Audit and Risk Committee.

3.5.2 External investigation procedures

In Queensland’s public sector there are a number of independent agencies which are responsible for promoting governance, accountability, integrity and to provide law enforcement:

- The Crime and Corruption Commission
- The Queensland Audit Office
- The Queensland Ombudsman
- The Queensland Police Service.

The Director-General, Department of Health has a duty to notify the Crime and Corruption Commission of corrupt conduct as per Section 38 of the Crime and Misconduct Act 2001. The Director-General delegates this function to the Manager, Conduct Advisory Services.

If assessed as corrupt conduct, the Crime and Corruption Commission will advise the appropriate action which may include:

- Assuming responsibility to investigate the matter.
- Jointly manage an investigation with the department.
- Refer the matter back to the department to deal with as it sees fit, subject to potential audit by the Crime and Corruption Commission.
- Refer the matter back to CAS for investigation. If so, CAS may recommend the appointment of an external independent investigator.

The department will ensure that investigators are appropriately appointed, experienced and accredited.

In all cases of suspected corrupt conduct, including alleged fraud, the Queensland Police Service will inform the initial assessment process by advising the department whether or not it is in the public interest for the Queensland Police Service to involve themselves in the matter.

3.5.3 Reviewing systems and procedures post, audit, investigation or inquiry

Risk and Governance Unit, Internal Audit and/or CAS will work with relevant stakeholders to reassess the adequacy of the internal control environment and actively plan and implement improvements where required. Reviews of systems and procedures may arise from investigations into an alleged fraud, an audit (internal or external) or a system review of a specific function or area. For example, if an investigation into an alleged fraud recommends changes to policies, procedures or controls, CAS will notify the relevant recommendation owner and stakeholders who will coordinate implementation, monitoring and oversight of the matter.

3.5.4 Provision of information to external agencies

The department shares relevant information with external agencies (e.g. the Crime and Corruption Commission, Queensland Police Service, Queensland Audit Office) as identified in the Standard.
3.5.5 Disciplinary action
Action taken in response to allegations of fraud and corruption will be in accordance with relevant legislation, policies and the principles of natural justice.

The management of discipline in the department is contained in the Discipline HR Policy E10. The department will consider reasonable management and/or disciplinary action against staff resulting from substantiated allegations of fraud or corruption. Action may include, but is not limited to: reprimand, reduction of the level of remuneration, transfer or redeployment or termination of employment.

The department may undertake disciplinary action against an employee regardless of, or before the outcome of any related criminal or civil proceedings.

3.5.6 Recovery of losses
The department is committed to maximising the recovery of losses incurred from fraud and corruption activities and will pursue every possible avenue in doing so through the appropriate agencies and legal avenues. The recovery of losses will limit the financial impact this may have on the department’s objectives.

4. Legislation
- Workplace Conduct and Ethics HR Policy E1 (QH-POL-113)
- Control Framework for Expenditure (2014)
- Criminal History Checking HR Policy B40 (QH-POL-122)
- Discipline HR Policy E10 (QH-POL-124)
- Corruption in Focus (Crime and Corruption Commission)
- Financial Management Practice Manual (FMPM)
- Risk Management Policy (QH-POL-070)
- Queensland Procurement Policy
- Public Interest Disclosures HR Policy I5 (QH-POL-202)
- Recruitment and Selection Policy HR Policy B1 (QH-POL-212)
- Requirements for Reporting Corrupt Conduct HR Policy E9 (QH-POL-218)

5. Supporting documents
- Ambulance Service Act 1991
- Crime and Corruption Act 2001
- Criminal Code Act 1899
- Criminal Proceeds Confiscation Act 2002
- Financial Accountability Act 2009
- Financial and Performance Management Standard 2009
- Hospital and Health Boards Act 2011
- Public Interest Disclosure Act 2010
- Public Sector Ethics Act 1994
- Public Service Act 2008
- Australian Standard Fraud and Corruption Control AS 8001-2008
- Code of Conduct for the Queensland Public Service 2011
- Queensland Ombudsman : Public Interest Disclosure Standard No.1 2013
6. Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Collusion</td>
<td>Secret or illegal cooperation or conspiracy in order to deceive others; Law collusion between ostensible opponents in a lawsuit</td>
</tr>
<tr>
<td>Confidential Information</td>
<td>Pursuant to s139 of the <em>Hospital and Health Boards Act 2011</em> confidential information means information, acquired by a person in the person’s capacity as a designated person, from which a person who is receiving or has received a public sector health service could be identified.</td>
</tr>
</tbody>
</table>
| Corrupt Conduct       | Corrupt conduct is the conduct of a person, regardless of whether the person holds or held an appointment, that -  
                          1. adversely affects, or could adversely affect, directly or indirectly, the performance of functions or the exercise of powers of a unit of administration or a person holding an appointment; and  
                          2. is not honest or impartial; or involves a breach of trust (knowingly or recklessly); or involves a misuse of information; and  
                          3. provides a benefit to the person or another person or causes a detriment to another person; and  
                          4. would, if proved, be a criminal offence or a disciplinary breach providing reasonable grounds for termination of the person’s services.  
                          For the full definition, please refer to the *Crime and Corruption Act 2001*. |
| Formal Investigation  | Pursuant to s190 of the *Hospital and Health Boards Act 2011*, a ‘formal’ investigation process involves the appointment or engagement of an investigator by the Director-General, or delegate.  
                          The investigation is a focused and detailed examination or inquiry, for which an investigator(s) is appointed to uncover facts and determine the truth of an allegation. This may include collecting, processing, analysing, storing, and evaluating evidence and providing findings and recommendations.  
                          The final product of a formal investigation is an investigation report. After considering the report, the Director-General, or delegate, may take the action he or she considers appropriate in relation to the matters identified in the report. |
<p>| Fraud                 | A Criminal Offence defined in the <em>Criminal Code Act 1899</em> |</p>
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Fraud (cont)          | Dishonest activity causing actual or potential financial loss to any person or entity including theft of moneys or other property by employees or persons external to the entity and where 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 the improper use of information or position for personal financial benefit.  
**For example:** false claims on a CV, using a cab voucher for personal travel, falsely making a claim on a timesheet, false invoicing, unauthorised use of credit cards, theft of intellectual property or other confidential information, falsifying time-sheets to claim overtime not worked. |
| Fraud Risk           | The effect of possible fraud on the objectives of the department, division and/or business unit.                                                                                                |
| Maladministration    | An administrative action that—  
(a) was taken contrary to law; or  
(b) was unreasonable, unjust, oppressive, or improperly discriminatory; or  
(c) was in accordance with a rule of law or a provision of an Act or a practice that is or may be unreasonable, unjust, oppressive, or improperly discriminatory in the particular circumstances; or  
(d) was taken—  
(i) for an improper purpose; or  
(ii) on irrelevant grounds; or  
(iii) having regard to irrelevant considerations; or  
(e) was an action for which reasons should have been given, but were not given; or  
(f) was based wholly or partly on a mistake of law or fact; or  
(g) was wrong |
| Misconduct           | Inappropriate or improper conduct in an official capacity; or in a private capacity that reflects seriously and adversely on the public service.                                                                  |
| Natural Justice      | Natural justice is an administrative law principle that provides for fairness in decision-making. It is concerned with ensuring that an objective decision maker reaches a procedurally fair decision.  
Natural justice has two rules:  
- Rule against bias: decision-makers are to be objective, free of bias, and have no personal interest in the matter being decided.  
- Hearing rule: an individual is to be informed of the substance of an allegation/s against them and have the opportunity to present their case prior to a decision being made. |
<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public interest disclosure (PID)</td>
<td>A public interest disclosure is a disclosure under Chapter 11 of the <em>Public Interest Disclosure Act</em> and includes all information and help given by the discloser to a proper authority for the disclosure.</td>
</tr>
<tr>
<td>Staff/Employees (including contractors and consultants)</td>
<td>For the purposes of this policy the term ‘staff’ refers to all Department of Health employees, and all individuals acting as its agents.</td>
</tr>
</tbody>
</table>
| Stealing / Theft                                                    | Theft is dealt with under Sections 391 of the Criminal Code  
*For example: an employee steals a laptop belonging to Department of Health without consent and with the intention of not returning the laptop.* |

### Version Control

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 1.1</td>
<td>March 2015</td>
<td>Scheduled review by Risk and Governance Unit</td>
</tr>
</tbody>
</table>