Government of **Western Australia**
Department of **Mines, Industry Regulation and Safety**

Fraud and corruption Control Framework

April 2022

Contents

1. Introduction

The Fraud and Corruption Control Framework (the framework) has been developed to detail the Department of Mines, Industry Regulation and Safety's (the department's) approach to **Prevent**, **Detect** and **Respond** to fraud and corruption.

The department is committed to the highest standards of openness, probity and accountability in all its affairs. The department acknowledges that fraud and corruption risks exist and will work continuously and collaboratively to detect and manage these risks.

All employees share in the responsibility to identify and report suspected fraud or corruption, behave ethically and promote a culture of integrity in the workplace. Senior leaders and managers are expected to role model these behaviours to ensure this culture is embedded, and this framework is adhered to within their business areas.

The framework describes:
- What fraud, corruption and misconduct is;
- Governance and responsibilities of the executive, employees and functional areas;
- Prevention, Detection and Response controls and mechanisms aimed to create awareness, how fraud and corruption can be identified and managed; and
- How reports of fraud and corruption will be investigated and dealt with.

Suspected fraud or corruption will be managed in accordance with internal corporate policy documents (policies, procedures and guidelines) and the *Corruption, Crime and Misconduct Act 2003* (CCMA). All legal obligations to the principles of procedural fairness will be met. This framework has been developed in line with Australian Standard AS8001-2021 Fraud and Corruption Control.
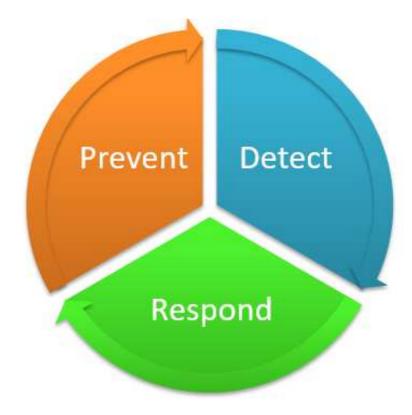

Figure 1 - The Fraud and Corruption Control System

1.1 Scope

This framework applies to:

- all employees and other workers;
- any external party involved in providing goods and services, with or without receipt of payment, to the department, such as contractors, consultants, outsourced service providers and suppliers.

While the word employee has been used throughout the framework, this should be read as also applying to others working alongside employees and/or carrying out work in any capacity for the department.

While the processes associated with some of the standards set out in the framework may result in different action being applied when not met by other workers, all employees and other workers are required to meet the standards of the framework.

1.2 Goals and Objectives

The framework exists to achieve the department's goal to minimise and prevent fraud and corruption risks with an emphasis on employee awareness, education and promoting a culture of reporting. The framework aims to clearly articulate the department's approach to fraud and corruptions risks with:

- a zero tolerance attitude towards fraud and corruption;
- commitment to integrity and accountability through the effective management of fraud and corruption risks;
- a responsibility to ensure that all necessary measures are taken to ensure employees act ethically and with integrity and are held accountable for their actions;
- a commitment to promote an integrity culture within the department; and
- a responsibility for all employees to assess the risk of fraud and corruption in their business area, identify and report suspected fraud or corruption.

1.2.1 Public Sector Commission Code of Ethics

The Public Sector Commission (PSC) Code of Ethics sets out the minimum standards of conduct and integrity for all public sector employees.

The department adheres to the Code of Ethics principles of:

Personal Integrity – we act with care and diligence and make decisions that are honest, fair, impartial, and timely, and consider all relevant information.

Relationships with others – we treat people with respect, courtesy and sensitivity and recognise their interests, rights, safety and welfare.

Accountability – we use the resources of the State in a responsible and accountable manner that ensures the efficient, effective and appropriate use of human, natural, financial and physical resources, property and information.

1.2.2 Code of Conduct

The department's Code of Conduct (the Code) outlines the standards of behaviour employees need to apply as representatives of the department which builds on the PSC Code of Ethics.

The Code, is an overarching framework, supported by corporate policy documents that establish the rules of conduct within the department. Additionally the Code outlines the responsibilities of the department and employees, providing assistance in addressing the ethical issues faced in our day-to-day business.

Employees are formally required to acknowledge the Code on commencement and complete essential Accountable and Ethical Decision Making training.

1.2.3 Values

The department's values of being **respectful**, **responsive**, **forward-thinking**, **transparent**, **fair** and **ethical**, are fundamental to the department's purpose of supporting a safe, fair and responsible future for the Western Australian community, industry and resources sector. These values reflect the qualities of our employees, ensure we lead with integrity, deliver on commitments, strive for excellence and look for better ways of doing things.

2. What is fraud, corruption and misconduct

Fraud and corruption can take many forms. Fraud and corruption may fall within the category of misconduct as defined in the CCMA. Further, many forms of fraud and corruption are offences under the *Criminal Code Compilations Act 1913*.

Definitions on these are provided below.

2.1. Fraud

Fraud is defined by Australian Standard (AS) AS8001-2021 as:

> *"Dishonest activity causing actual or potential gain or loss to any person or organisation including theft of moneys or other property by persons internal and/or external to the organisation and/or where deception is used at the time, immediately before or immediately following the activity."*

Fraud includes any practice that involves deceit or other dishonest means by which a benefit is obtained from the government. The benefits may be obtained by:

- employees (known as 'internal' or 'workplace' fraud).
- persons external to the department, either with or without assistance from departmental employees (known as 'external' or 'customer' or 'client' fraud).

Fraud can take many forms, including (but not limited to):

- fraudulent use of departmental funds;
- fraudulent appropriation of assets;
- use of and disclosure of confidential information for personal gain or for another person or entity;
- theft;
- causing a loss, or avoiding or creating a liability by deception;
- providing false or misleading information to the department, or failing to provide information where there is an obligation to do so;
- making, using or possessing forged or falsified documents;
- bribery, corruption or abuse of office;
- unlawful use of departmental computers, credit cards, telephones, vehicles, and other property or services;
- failure to disclose relevant conflict of interest when making decisions, including those related to procurement, recruitment, regulation or compliance activities;
- making false claims of expenses, work hours or leave entitlements; and
- any offences of a similar nature to those listed above.

2.2. Corruption

Corruption is defined by AS8001-2021 as:

> *"Dishonest activity in which a person associated with an organisation (e.g. director, executive, manager, employee or contractor) acts contrary to the interests of the organisation and abuses their position of trust in order to achieve personal advantage or advantage for another person or organisation. This can also involve corrupt conduct by the organisation, or a person purporting to act on behalf of and in the interests of the organisation, in order to secure some form of improper advantage for the organisation either directly or indirectly".*

2.2.1 of AS8001-2021 considers bribery a subset of corruption, and is therefore defined as:

"Offering, promising, giving, accepting or soliciting of an undue advantage of any value (which could be financial or non-financial), directly or indirectly, and irrespective of location(s), in violation of applicable law, as an inducement or reward for a person acting or refraining from acting in relation to the performance of that person's duties."

Corruption is any conduct that is unlawful, improper, immoral or fraudulent and may include (but is not limited to):

- abuse of position or authority;
- conflict of interest;
- dishonestly using influence;
- nepotism and favouritism;
- inaccurate timesheets;
- inappropriate procurement and purchasing;
- inappropriate use of corporate credit cards;
- blackmail;
- failure to disclose gifts or hospitality;
- acceptance of a bribe;
- insider trading;
- misuse of internet or email; or
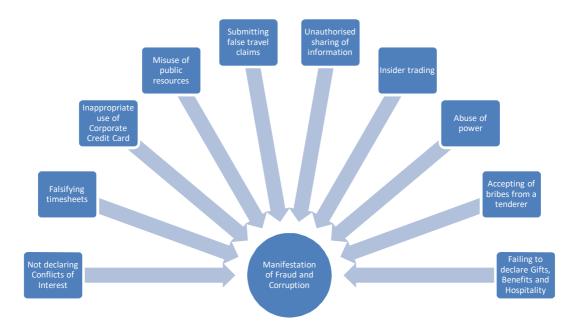- unauthorised release of confidential, private information or intellectual property.

Figure 2 - Characteristics of Fraud and Corruption

Examples of fraudulent and corrupt conduct are provided at [Appendix 1](#).

2.3. Misconduct

The CCMA defines serious and minor misconduct as follows.

Serious misconduct, defined by section 4(a), (b) or (c), occurs if a public officer:

- corruptly acts or corruptly fails to act in the performance of undertaking their duties; or
- corruptly takes advantage of their position to obtain a benefit for themselves or another person, or cause a detriment to any person; or
- in an official capacity commits an offence punishable by two or more years' imprisonment.

Minor misconduct, defined by section 4(d), occurs if a public officer engages in conduct that:

- adversely affects, or could adversely affect, directly or indirectly, the honest or impartial performance of the functions of a public authority or public officer, whether or not the public officer was acting in their public officer capacity at the time of engaging in the conduct; or
- constitutes or involves the performance of his or her functions in a manner that is not honest or impartial; or
- constitutes or involves a breach of trust placed in the public officer by reason of his or her office or employment as a public officer; or
- involves the misuse of information or material that the public officer has acquired in connection with his or her functions as a public officer, whether the misuse is for the benefit of the public officer or the benefit or detriment of another person.

Misconduct constitutes, or could constitute:

- a disciplinary offence providing reasonable grounds for termination of a person's office or employment as a public service officer under the *Public Sector Management Act 1994* (PSMA) (whether or not the public officer to whom the allegation relates is a public service officer or is a person whose office or employment could be terminated on the grounds of such conduct).

In the above reference to a public officer in the CCMA, the PSC defines a public officer as "anyone using public resources to carry out a public function under a written law."

3. Fraud and Corruption Governance and Accountabilities

3.1. Governance

The department's organisational values and culture, governance, risk management framework and controls work together to prevent, detect and respond to potential or actual fraudulent and corrupt conduct.

The PSC Code of Ethics, the department's Code of Conduct and supporting corporate policy documents outline the expected standards of behaviour to ensure accountability for fraud and corruption risks. Employees are expected to act with integrity through conducting themselves in an honest, ethical and professional manner.

The Code of Conduct and supporting policy documents emphasise employees must assist the department to:

- prevent deliberate, inadvertent or unauthorised misuse of departmental information; communication and technology;
- protect against unauthorised access, cyber-attacks and unplanned outages;
- protect against loss, misuse, insecure or omission of information;
- reduce the risk of human error;
- ensure the capture and management of corporate information;
- protect the department from legal liability; and
- protect the department's reputation.

3.2. Roles, Responsibilities and Accountabilities

3.2.1. Director General

The Director General is accountable for the effective, responsible and economical use of the department's public resources in managing fraud and corruption risks. They are responsible for embedding integrity within the department, including governance, administration, systems, controls, culture and attitude, and accountabilities and responses, to prevent fraud, corruption and misconduct.

This accountability and responsibility is appropriately delegated to the Executive, senior managers and line managers as detailed in relevant administrative delegations and schedules.

The Director General is the authority to determine if a matter is to be dealt with through the disciplinary process.

Under the CCMA, the Director General is required to notify PSC of suspected minor misconduct, or the Corruption and Crime Commission (CCC) if serious misconduct is suspected.

3.2.2. Corporate Executive

The Corporate Executive are responsible for demonstrating leadership in the management of fraud and corruption risks for their groups. The Corporate Executive may establish sub-committees or working groups from time to time to assist it in the performance of its functions.

3.2.3. Executive Sponsor for Fraud and Corruption Prevention Control

The Executive Director Corporate Services is the department's Executive Sponsor for fraud and corruption prevention control.

The role of the Executive Sponsor is to champion fraud and corruption and prevention control within the Corporate Executive, and ensure controls are effectively integrated into the department's risks, strategic planning, corporate governance and business systems. The Executive Sponsor also oversees the education and training programs on fraud and corruption, the implementation of the framework, and advises the Director General as required on fraud and corruption matters. This position also chairs the Governance and Integrity Corporate Executive Subcommittee.

3.2.4. Audit and Risk Committee

The Audit and Risk Committee is independent and accountable only to the Director General. The Committee plays an important role in providing oversight of the department's governance, risk management and internal control practices. This oversight also provides confidence in the integrity of these practices to meet government and strategic objectives.

The committee performs its role by providing independent advice, guidance and assurance to the Director General by:

- reviewing effectiveness of governance, risk management and control;
- reviewing the financial statements and public accountability performance reporting;
- promoting improved economy, efficiency, effectiveness and ethical culture;
- reviewing reliability of management information;
- monitoring and evaluating internal audit performance;
- reviewing effectiveness of fraud control measures;
- promoting innovation and improvement; and
- monitoring compliance with laws, regulations, standards and good practice.

In discharging its responsibilities the committee has unrestricted access to employee records, data and reports. The committee is also entitled to see and receive relevant advice and explanations from management and employees as it deems necessary to discharge its responsibilities.

3.2.5. Governance and Integrity Subcommittee

The Governance and Integrity Corporate Executive sub-committee has been established in response to the department's commitment to governance, integrity and effective fraud and corruption risk management. The purpose of the sub-committee is to allow for resource and knowledge sharing; accountability in ensuring continuous improvement; support for the ongoing maintenance and promotion of DMIRS' Governance and Integrity frameworks; and to provide a co-ordinated approach to promote and embed a culture of integrity and fraud and corruption prevention across the department.

3.2.6. Leaders and managers

In addition to the delegated accountability and responsibility from the Director General, senior leaders and managers are responsible for providing strong leadership and fostering a culture

that facilitates effective adherence to the framework within their business units. In particular, they must:

- provide leadership, guidance and support to develop an ethical culture of integrity;
- have an understanding of corporate governance measures to prevent fraud and corruption;
- identify fraud and corruption risks;
- model appropriate ethical behaviours and setting and enforcing standards;
- ensure corporate policy documents are operationalised;
- engender a culture of fraud and corruption education, awareness and reporting;
- undertake fraud and corruption risk assessments, implement controls, undertake treatment plans, and review as required;
- adopt, monitor and review management controls to prevent fraud and corruption;
- report suspicions of fraud and corruption promptly, and ensure confidentiality; and
- ensure the protection of complainants who report fraud and corrupt conduct.

3.2.7. Employees

All employees have a responsibility to prevent fraud and corruption by acting ethically, complying with controls, policy documents, and reporting suspicious, fraudulent or corrupt behaviour. Therefore, employees are duty bound to report misconduct without fear of reprisal. The department will provide support and anonymity (unless required or permitted by law) to any employee who reports incidences of fraud and corruption.

Reporting is encouraged through the internal reporting framework (where possible) or alternatively, directly to the CCC or PSC. The department is obligated to support employees who have concerns about the investigation process or may be subject of detrimental behaviour towards them.

In order to prevent fraud and corruption all employees should:

- report suspicions of fraud and/or corruption in accordance with the department's policy documents and associated processes;
- ensure powers afforded to them in their role are exercised lawfully;
- embrace an ethical workplace culture;
- recognise the value and importance of preventing fraud and corruption;
- familiarise themselves with good work practices, management systems and controls;
- keep abreast of best practices for preventing fraud and corruption;
- decline and declare all offers of gifts and benefits;
- declare all actual, perceived or potential conflicts of interest including those of family members which may influence official responsibilities; and
- be aware of the different types of fraud and corruption that can occur in the workplace and how to detect them.
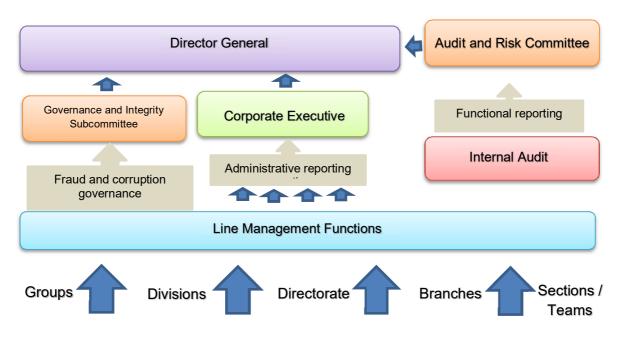
Figure 3: DMIRS Fraud and Corruption Governance Structure

3.2.8. Public Interest Disclosure officers

The *Public Interest Disclosure Act 2003* (PID Act) provides for the appointment of PID Officers who are available for employees to report wrongdoing and protects them when they do.

The PID process is a way for people to report certain types of wrongdoing of public authorities or public officers. It provides certain protections for the person making the disclosure and those who are the subject of disclosures. It provides a system for the matters disclosed to be investigated and for appropriate action to be taken.

A public interest disclosure can be made by anyone who believes on reasonable grounds their information is true. It is an offence under the PID Act to deliberately make a false or misleading disclosure. Once made, the person making the disclosure cannot withdraw it.

A disclosure must relate to a matter of public interest and show wrongdoing by a public authority, officer or contractor when performing a public function. The department has a number of PID officers who are appointed by the Director General.

3.2.9. Internal Audit Branch

The Internal Audit Branch has independent status with the department. Internal Audit provides independent, objective assurance and consulting services to add value and improve the department's integrity, performance and governance. Internal Audit helps the department accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management and internal control processes.

It also helps to enhance and protect organisational value by providing risk-based and objective assurance, advice and insight, and plays an active role in developing and maintaining a culture of accountability, integrity and adherence to high ethical standards.

Internal Audit undertakes all audits, reviews and investigations under the authority of the Director General. The scope and coverage of Internal Audit work is not limited in any way and may cover any departmental activity, operation and program.

3.2.10. Human Resources Branch

The Human Resources Branch is responsible for the development of policy documents relating to breaches of the Code of Ethics, Code of Conduct, and management of grievance and discipline processes. Its responsibilities also include the development and delivery of fraud, corruption and misconduct awareness/education programs in conjunction with Internal Audit.

3.2.11. Financial Accounting and Planning

The Financial Accounting and Financial Planning branches are responsible for the custody and control of public money and public property, procurement and general accounting and reporting requirements as per the Treasurer's Instructions under the *Financial Management Act 2006, Procurement Act 2020,* and procurement rules. The branch provides financial strategic advice, guidance and reporting to support operational groups.

3.2.12. Procurement and Contract Management

The Procurement and Contract Management Section within the Financial Accounting Branch provide an effective and efficient procurement function, including tender and contract formation, procurement strategy, advice and policy formation, compliance and client liaison. The section provides professional procurement advice to employees and the Executive and identifies, evaluates and analyses spend data. The section undertakes ad-hoc procurement and contract management reporting to assist in detection of irregularities.

3.2.13. Office of the Director General

The Office of the Director General on the advice of the Executive Sponsor for Fraud and Corruption and Prevention Control, undertakes policy document improvements, co-ordinates or implements recommendations and actions, undertakes reporting obligations to Corporate Executive and external reporting agencies, and manages the Gift Register. The General Manager Office of the Director General is the Director General's delegate scrutinising and approving gifts declared by employees, or following up on undeclared gifts brought to their attention.

3.2.14. Business Innovation Directorate

The Business Innovation Directorate manages the department's business systems and information and communication technology infrastructure, and is the custodian of digital data. The directorate ensures the security, integrity and cyber resilience of digital data through the management of information technology risks, while making sure the department's software and infrastructure are used ethically by the department's employees.

The directorate also centrally records and tracks assets, such as laptops, computers and mobile phones, and undertakes careful disposal at the expiry of their useful life.

3.2.15. Strategic Planning, Performance, Risk and Reform Branch

The Strategic Planning, Performance, Risk and Reform Branch administers risk management and compliance functions, and provides support for the department to achieve its strategic and operational objectives through planning. The branch facilitates risk workshops with Executive

leadership to identify fraud and corruption risks, and assist the business areas with operational, project and contract risk assessment.

3.2.16. Assets Branch

The Assets Branch is responsible for the department's buildings in the Perth metropolitan area and across regional Western Australia. The branch ensures the department's non-portable assets, including the information technology infrastructure, are protected through state-of-the art security – both digital and in-person during and after business hours.

3.3. Agency Partners

The Framework aligns with the oversight functions of PSC, CCC and Office of the Auditor General, and therefore, the department will seek collaboration with these agencies to educate, prevent, assess and investigate fraud, corruption and misconduct.

3.4. Environmental scans

The department continues to monitor the external environment to identify fraud and corruption risks which it may be exposed. In conducting the scan the department monitors media reports, industry presentations and circulars, and other external factors for integrity risks and vulnerabilities.

4. Fraud and Corruption Prevention

4.1. Awareness and communication

The department aims to ensure all employees have an awareness and understanding of fraud and corruption. The following strategies and activities including corporate policy documents, controls, systems, tools and training are aimed at preventing fraud and corruption risks.

4.1.1. Legislation, instruments, resources and policy documents

There are a range of legislative, instruments, internal and external resources and departmental policy documents in place to govern and support day-to-day operations and decision-making in relation to fraud, corruption and misconduct. A list of fraud and corruption prevention and detection controls, including reporting mechanisms are embedded in the policy documents and are provided at (but not limited to) Appendix 2.

4.2. Internal Controls and Management Systems

All business processes and systems, especially those identified as high risk of fraud, corruption, or misconduct are subject to a strict management system of internal controls that are documented, reviewed and updated regularly, and understood by relevant employees.

Strong internal controls and management systems are important in protecting against fraud and corruption. In many cases, where fraud, corruption and misconduct are detected, it is possible to identify a fundamental control weakness, failure, or lack of that either allowed the incident to occur or failed to detect it immediately after it occurred. In such instances, existing controls may be reviewed and enhanced to prevent fraud, corruption and misconduct in the future.

Line managers are responsible for ensuring appropriate management systems, including internal controls, are established and maintained, and undertake regular audit reviews including compliance testing.

The department's management systems include (but is not limited to):

4.2.1. Conflict of Interest

The department's Conflict of Interest policy documents that all employees with an actual, perceived or potential conflict of interest are required to submit a conflict of interest declaration and, in conjunction with their line manager, develop an action plan for the management of the conflict of interest. It is essential for all employees to undertake Conflict of Interest training.

Conflicts of interest may exist relating to the duties of the position some of which have been identified with requiring higher integrity and proactive declarations sought of private, pecuniary or non-pecuniary interests.

The Conflict of Interest declaration and its associated management plan are documented using the Conflict of Interest e-Form. By completing the form, the employee agrees to comply with the endorsed management plan for the declared conflict of interest and its subsequent review.

Depending on the nature of the declaration and management plan, the conflict of interest may require further declarations be submitted to ensure the conflict of interest is appropriately managed over the employment term.

4.2.2. Delegations Register

The Delegations Register keeps a record of the delegations, authorisations, appointments and administrative instruments currently in place within the department.

The department adheres to a rigorous and consistent framework for managing statutory delegations of decision-making power by the statutory decision-making authority to departmental officers, or to officers of other public sector agencies when appropriate.

These delegations are included in controls within business and management systems or documented and reviewed as necessary.

4.2.3. Purchasing, Incurring and Certifying Financial Delegations Framework

Consistent with the principles of sound management and the requirements of the *Financial Management Act* 2006, the Director General has approved a series of financial delegations to assist in the administration and financial management of the department.

The Financial Delegations Register details all authorised positions and their financial delegation limits including the purchasing delegation for committing the expenditure and incurring and certifying delegations for approving expenditure.

The Procurement Delegation Schedule sets out who has authority to approve various documents in procurement and contract management.

This Framework applies to all departmental employees who are required to undertake purchasing on departmental business.

4.2.4. Procurement and Contract Management System

Employees procuring products and services on behalf of the department are required to ensure that purchases are made in accordance with government and departmental policy documents. All procurement must be facilitated through the Procurement and Contract Management System or by Corporate Credit Card.

The budget owner initiating a purchase is responsible for the procurement, its operational outcomes, deliverables, and the day-to-day management of the contract. Procurement Services role is to ensure that the department's procurement processes are in accordance with best practice principles, including the WA Procurement Rules.

Procurement Services facilitates the procurement process for all contracts valued at or greater than $50,000 including GST. The department must also involve the Department of Finance in all procurements from planning activities onwards with a Total Estimated Value at $250,000 and above, with the exception of deconstruction contracts falling under the *Mining Rehabilitation Fund Act 2012*.

4.2.5. Payments

The department uses the Financial Delegations Framework as the basis to assign financial delegations (i.e. purchasing, incurring, certifying and special conditions) to senior authorising officers to enable the occupants to effectively carry out financial duties and responsibilities in relation to authorisation of payments and provide a segregation of duties to ensure no single employee is able to control all aspects of the payment authorisation process. These delegations are included in controls within finance business systems, or documented and reviewed as necessary.

Purchases over $10,000 generally require creation of a purchase order. Credit card payments where sought for payments above $10,000 are required to seek and gain proper authorisation. Additionally, a manual audit is regularly performed for inappropriate transactions.

Transactions are routinely assessed in combination with business area management to ensure expenditure is appropriate.

4.2.6. Human Resources Management Delegations

The Human Resources Management Delegations Matrix provides information on the delegated approval from the Director General to specific positions in regard to the approval of employee management across the areas of:

- Leave management;
- Allowances and salary;
- Filling a vacancy;
- Establishment; and
- Personnel management.

The department's web self-service kiosk (ESKI) is a facility utilised to record a number of processes and conditions of employment as delegated through the Human Resources Management Delegation matrix. Employees and managers should ensure accurate records of attendance are kept, absences for leave are appropriately approved and other conditions of employment that are sought are appropriately approved and current.

4.2.7. Information and Communications Technology Framework

The DMIRS ICT Governance Framework consists of the processes that ensure the effective and efficient use of IT resources, enabling the department to meet its strategic objectives as outlined in the Strategic Intent and Digital DMIRS Strategy.

The Information and Communications Technology Delegations Schedule ensures appropriate approvals are in place to ensure access to processes associated with information and communications technology including applications, policy documents, budget, projects, system development and purchase of ICT goods and services.

4.2.8. Gifts, Benefits and Hospitality Delegations Schedule

The department's Gifts, Benefits and Hospitality schedule provides for approval processes associated with the approval to receive gifts, benefits and hospitality and to provide gifts and hospitality.

Where an employee or the department has been offered a gift, benefit or hospitality regardless of whether it has been declined or accepted, it must be record using the Gift, Benefits and Hospitality Declaration e-Form. The giving of gifts, benefits and/or hospitality requires advance approval by employees through the completion of the Gifts, Benefits and Hospitality Expenditure e-Form.

4.2.9. Quality Management System

An integrated Quality Management System compliant with Quality Standard AS/NZS ISO 9001-2015 (Standard) documents and maintains all processes, forms, policies and associated documents of the Application, Dealing and Compliance Processes relating to mineral and petroleum resource legislation.

The system is subject to annual audits – both internal and external – to ensure the department's mineral and petroleum resource legislation processes and business systems comply with the requirements of the Standard.

4.3. Risk Assessment

The department records its risks in a centralised online database, Cammsrisk. As part of the risk management activities, business areas must periodically identify, assess and review fraud and corruption risks in line with the department's Risk Management Policy and Framework, and develop treatment plans that specifically address the risks faced. Treatment plans are then monitored and when completed become controls that may then be assessed for their effectiveness.

Risk reports of extreme and high residual risks are submitted to the Audit and Risk Committee and Corporate Executive on a regular basis.

4.4. Training and Awareness

All employees must complete Accountable and Ethical Decision Making (AEDM) training. The training provides information to ensure employees make accountable and ethical decisions and understand the standards of conduct and integrity expected of them. The training provides information on contemporary fraud and corruption prevention practices and reporting mechanisms. The program's objectives are to:

- understand what it means to serve the public interest;
- describe public sector's accountability framework;
- explain what accountable and ethical decision making is and its importance in the workplace;
- outline the behaviour expected of DMIRS employees; and
- what, when and how to report fraudulent/corrupt behaviour and suspected breaches of the Code.

Employees must complete AEDM training within three months of commencement. AEDM Refresher online training is required to be completed every five years.

4.5. Employment Screening

The department has a number of employee screening processes which apply to approved vacancy filling practices.

A National Police Clearance is required for all advertised positions as part of the recruitment process.

Specified positions within the department have additionally been identified with enhanced integrity requirements and are subject to further conflict of interest and other identified assessment as part of the screening process.

Other requirements may include certified evidence of Australian permanent residency, evidence of qualifications, evidence of vaccination, medical clearance and/or psychometric screening.

4.6. Integrity Reporting

Integrity Reporting is a Standing Item on the Corporate Executive meeting Agenda. Items regularly reported include, but are not limited to:

- Conflicts of interest;
- Gifts, benefits and hospitality;
- Cyber security;
- Contact with lobbyists;
- Progress on remediation of matters of high risk, like Payment Card Industry Data Security Standard (PCI DSS) compliance;
- Audit findings; and
- Themed integrity trends (e.g. outcomes from disciplinary processes to reinforce key messages).

4.7. Record Keeping

The department is committed to ensuring that complete and accurate records of all business activities and decisions are created and managed in accordance with the department's Record Keeping Plan.

The department ensures that all employees are aware of their responsibilities and obligations to comply with legislative and administrative requirements, in accordance with the PSMA and the *State Records Act 2000.*

5. Fraud and Corruption Detection

5.1. Fraud and Corruption Detection Program

The department relies on a variety of strategies to prevent fraud and corruption including (but not limited to):

- procedures for reporting fraud and corruption;
- vigilance and awareness of all employees;
- internal audit activities;
- operational risk management processes; and
- analysis of controls and systems intelligence.

5.2. Internal Audit

Internal audit is an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps the department accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Audit is a core function of DMIRS which provides assurance to the Director General and the Audit and Risk Committee on:
- compliance with legislation and policy;
- efficiency and effectiveness of operations; and
- integrity of information and reporting.

Internal Audit activities assist the department through:
- identifying controls that be required to be strengthened;
- preventing similar fraud and corrupt activities in the future; and
- fraud detection considerations.

The department's Financial Management Manual is an internal control standard that is used by auditors for monitoring compliance with procedures

5.3. Compliance and Risk Management

Business areas must systematically identify and assess fraud and corruption risks in line with the department's Risk Management Framework and policy documents. The risk management policy documents provides a process structure by which risks are identified, managed, monitored and reviewed within DMIRS.

Routine risk assessment of fraud and corruption risks are to be informed by a review of critical preventative controls and analysis of information and data collected by DMIRS regarding its key risks.

This includes, but is not limited to:

- grievance and disciplinary data;
- gifts, benefits and hospitality data; and
- conflict of interest declarations.

To enable efficient reviews, all documents, resources and findings included in this framework, including but not limited to: corporate policy documents, audits, investigations, asset registers, reports, forms and declarations, must be maintained in approved recordkeeping systems.

5.4. Financial Systems Intelligence

Through the use of the department's Business Intelligence unit's ability to access multiple databases, the department seeks to provide robust meaningful financial data with the aim of reducing the opportunity of fraud and corruption by potentially rogue stakeholders.

A report has been developed which identifies expenditure per supplier across items recorded on a purchase order, non-purchase order and via credit card purchases to match against contracts. Although this report has been created manually, plans are being developed to engage business intelligence with a vision to automate the output, to allow the report to be run on a regular and ongoing basis to further reduce the department's fraud and corruption risk.

Cross checking of select payment transactions made to assess for duplication with that of an employee's back account has been introduced and will be expanded further to other payment processes.

5.5. Related Party Disclosures

The department adheres to the Australian Accounting Standards Board (AASB), Standard 124 – Related Part Disclosures which requires senior management (this incorporates Tier 1-3 employees) to disclose any business transactions which exceed $50,000 that involve close family members, including spouse and dependents, or others which could influence business decisions involving another government organisation. This extends to businesses controlled or jointly controlled by senior management and their close family members and the interaction with government.

5.6. Supplier and Customer Integrity

It is important to consider that the department may be vulnerable to externally instigated fraud or corruption. The risk of fraud and corruption will be reduced if the department knows who it is dealing with all significant commercial transactions, so the credentials, financial health and integrity of new suppliers or customers may be investigated as far as practical.

When procuring goods and/or services, employees are required to seek competitive quotes from potential suppliers. In addition to ensuring that the submitted offers meet the required specifications and represent value for money, the evaluation process is to include an assessment of the supplier and their disclosure requirements. This includes the identity of the supplier and verification of the company's ABN or ACN.

The rigour of these checks and assessments are to be commensurate with the value and/or risk presented by the procurement. When ordering from a Common Use Arrangement, suppliers on the panel have already completed a stringent assessment process undertaken by the Department of Finance.

Concerns regarding a supplier's identity or its representation are to be raised with the Manager Procurement and Contract Management.

5.7. Debarment of Supplier

The Director General may debar a supplier from supplying goods, services or works to the department because of any conduct of the supplier or of a senior officer of the supplier that may contravene Category A or B under Procurement (Debarment of Suppliers) Regulation 2021.

5.8. External complaints

The department has a mechanism for capturing feedback and complaints to service from clients, customers and members of the public. This includes the ability for complaints to be raised anonymously. Complaints are collected and referred to the relevant business area for response, or to Human Resources or Internal Audit for independent review when appropriate.

5.9. Internal reporting

The department's employees have a responsibility to report suspected fraud and corruption, including possible breaches or suspected breaches of the Code of Ethics or the Code.

Every employee is responsible for reporting suspected fraud and corruption by a public officer as soon as practicable, in line with corporate policy documents. In the first instance, internal reporting is encouraged to ensure matters are dealt with in a timely and effective manner. Suspicions of fraud and corruption can be reported internally to any of the following:

- line managers;
- other senior manager;
- Human Resources;
- Internal Audit;
- Public Interest Disclosure Officer; or
- the Director General.

5.10. External reporting

The department has primary responsibility for investigating allegations of misconduct of its own employees. However, employees can report directly to the PSC or to the CCC, which includes the option to remain anonymous. Matters can also be reported direct to the Western Australia Police Force.

The department will take all steps to ensure those who report fraud and corruption are not subject to victimisation and are able to report confidentially or anonymously.

6. Fraud and Corruption Response

6.1. Disciplinary investigation

The department will review suspected fraud and corrupt conduct through its disciplinary process to determine if misconduct has occurred. All suspected breaches of discipline will be investigated fairly and consistently and dealt with according to the department's Discipline Policy and Procedure.

Where allegations are substantiated, appropriate disciplinary action will be taken in accordance with legislative requirements, Public Sector Standards, and principles of procedural fairness.

Disciplinary action may include (but is not limited to):

- a reprimand;
- fine – not exceeding five days' remuneration;
- transfer to another public sector organisation or transfer within the existing agency;
- reduction in monetary remuneration;
- reduction in classification of the employee; and/or
- dismissal.

| Fraud and corruption misconduct reported | Assessment undertaken to determine misconduct | Notification and reporting obligations met | Investigation undertaken if required | Determination made and recommendation implemented | Prevention, lessons learned, and education |

Figure 4 - Process undertaken for reported fraudulent and corruption conduct

6.2. Reporting misconduct

As required by the CCMA, the department will record and report all reasonable suspicions of fraud and corruption to the appropriate oversight body:

- Minor misconduct – Public Sector Commission; or
- Serious misconduct – Corruption and Crime Commission.

Reports may be referred to an external agency such as the, PSC or CCC for investigation by the department, or to the Western Australia Police Force where criminal conduct has occurred.

6.3. Crisis Management

The department's Critical Incident Management Plan outlines procedures and communication protocols for both internal staff and external stakeholders in the event of a suspected case of fraud or corruption being detected – especially if senior management is implicated.

6.4. Recovery and Legal Proceedings

The department may seek to recover any money or assets lost due to incidents of fraud and corruption, and may undertake criminal or civil actions as deemed appropriate as per legal advice and after considering the cost and benefit of doing so.

6.5. Confidentiality and Integrity

Confidentiality of the process will be maintained and observed by all persons reporting, managing, administering or the subject of any fraud or corruption. This includes preserving the original condition of any evidence including potential digital evidence.

6.6. Internal Control Review

Where fraud or corruption is detected, the Executive Sponsor for Fraud and Corruption Control may request line management to reassess the adequacy of internal control systems, particularly those directly relating to the fraud or corruption incident, and recommend improvements if required.

6.7. Fraud, Corruption and Misconduct Register

Every reported incident of fraud and corruption, whether substantiated or not, will be maintained by the General Manager Human Resources or General Manager Internal Audit for the Director General in a confidential electronic file to which only the Director General, or persons authorised by the Director General, may have access.

Information contained within the register may be used in effective measurement and management of fraud and corruption against or by the department.

7. Review and continuous improvement

The Framework will be continuously improved through:

- review every two years or following significant changes to operations or structures of the department;
- review of effectiveness of fraud and corruption risk assessment, management and oversight;
- review of effectiveness of management measures, controls, processes, procedures and lessons learned following fraud and corruption incidents; or
- changes to the applicable laws, regulations, standards and best practice guidelines.

Authority

Primary Contact: Executive Director, Corporate Services
Policy Owner: Director General, Department of Mines, Industry Regulation
                         and Safety

Appendix 1 – Examples of fraudulent and corrupt conduct

• Failing to declare and appropriately manage conflicts of interest.
• Using information obtained through the course of their duties for their personal benefit or another person's benefit (i.e insider trading).
• Using statutory powers or employment status to place undue pressure or influence for personal benefit.
• Submitting a record of attendance (a timesheet) containing false information or times not worked.
• Failure to submit accurate leave records.
• A manager signing off on fraudulent overtime claims.
• Misuse of public resources (ICT equipment, phones, vehicles and equipment) for private use.
• Unauthorised use of a departmental motor vehicle.
• Corporate credit card misuse, such as payment for personal expenses.
• Disclosing personal, sensitive or restricted information outside of the department without authority.
• Regularly taking resources, such as office supplies, stationery or DMIRS equipment, home for personal use or to sell for personal benefit.
• Approving invoices for private expenses or colluding to do so for others.
• Submitting a false travel or reimbursement claim and receiving a benefit to which they are not entitled.
• Knowingly making or using forged or falsified documentation.
• Manipulating recruitment and selection procedures to secure the appointment of a close friend or family member or associate.
• Management promoting, engaging or giving an employee advantage over others for personal reasons.
• Submitting false salary packaging claim and receiving a benefit not entitled.
• Accepting or soliciting a bribe or secret commission from a tenderer to give partial consideration to them.
• Providing commercial-in-confidence information to a tenderer resulting in them obtaining an unfair advantage over other tenderers in the tender process.
• Colluding with a supplier of goods or services to the department for personal gain.
• Facilitation payments i.e. obtaining kickbacks for organising preferential treatment.
• Soliciting or accepting gifts or benefits for personal gain or preferential treatment for clients.

Appendix 2 – Legislation and other instruments

Legislation

Relevant legislation includes (but is not limited to):

- *Corruption, Crime and Misconduct Act 2003*
- *Criminal Code Act Compilation Act 1913*
- *Financial Management Act 2006*
- *Mining Rehabilitation Fund Act 2012*
- *Procurement Act 2020*
- *Procurement (Debarment of Suppliers) Regulations 2021*
- *Public Interest Disclosure Act 2003*
- *Public Sector Management Act 1994*
- *State Records Act 2000*

External information

- Integrity in the Western Australian government sector
- Integrity Strategy for WA Public Authorities 2020-2023
- Corruption and Crime Commission
- Public Sector Commission
- Commissioner's Instruction No. 7: Code of Ethics

Internal resources

- Integrity matters

Delegations Framework, Schedules and Registers

- Delegations Register
- Gifts, Benefits and Hospitality Schedule of Delegations
- Human Resources Management Delegations
- ICT Schedule of Delegations
- Purchasing, Incurring and Certifying Financial Delegations Framework
- Procurement Delegations Schedule

Fraud and corruption related corporate policy documents

- Code of Conduct;
- Annual and Long Service Leave Management Procedure
- Conflict of Interest Policy, Procedure and Guideline
- Contact with Lobbyists Guideline and Form
- Corporate Credit Card Policy and Procedure
- Corporate Record Keeping and Information Management Policy and Manual
- Critical Incident Management Plan

- Debtor Management Policy, and Procedure
- Discipline Policy and Procedure
- Employee Personal Files Access Procedure
- Filling a Vacancy Policy, and Procedure
- Flexible Work Policy
- Financial Management Manual
- Gifts, Benefits and Hospitality Procedure
- Grievance Resolution Policy and Procedure
- Managing Inappropriate and Unreasonable Workplace Behaviours Policy and Guideline
- Procurement Policy
- Procurement and Contract Management Guideline
- Public Interest Disclosure Policy, Procedure and Form
- Risk Management Policy, Guidelines and Framework
- Secondary Employment Procedure
- Travel Policy, and Procedure
- Work at Home Procedure and Form

The department's corporate policies and procedures are available on the Quality Management System.