

# Fraud and Corruption Prevention Guideline

## Section 1 - Purpose

(1) This Guideline states the University's strategy for the prevention of Fraud and Corruption.

(2) Guidance is provided on the following topics:

- a. Definition of Corruption;
- b. Definition of Fraud;
- c. Assets of the University Vulnerable to Fraud and Corruption;
- d. Perpetrators of Fraud and Corruption;
- e. Fraud and Corruption Awareness;
- f. Fraud and Corruption Detection;
- g. Fidelity Guarantee Insurance;
- h. Fraud and Corruption Risk Management:
  - i. Strategic Audit Plan;
  - ii. Internal Audit Plan;
  - iii. Fraud and Corruption Prevention and Response Strategy;
  - iv. Risk Assessment;
  - v. Integrating Fraud and Corruption Risk Assessment with Overall Risk Assessment;
  - vi. Implementation of Proposed Actions; and
  - vii. Review of Effectiveness of Strategies.

## Section 2 - Policy

(3) Refer to the [Fraud and Corruption Control Policy](#).

## Section 3 - Procedure

(4) Refer to the [Fraud and Corruption Prevention Procedure](#).

## Section 4 - Guideline

(5) The risk of fraud and corruption is ever present. The following are some of the factors that add to, or at least change, the University's risk:

- a. changes in government funding, leading to an increasing reliance on non-government funding;
- b. ventures into new markets and areas of operations;
- c. the development of commercial strategies to capitalise on the development of intellectual property and marketable products and services;

- d. convergence of the university sector and the private sector through the increase in cooperative and / or strategic partnerships;
- e. greater competition in the allocation of scarce resources;
- f. greater competition in the university sector for domestic and overseas students, staff, research funds, industry support and status;
- g. increased regulatory requirements;
- h. increased availability and extensive use of technology; and
- i. tighter timeframes and deadlines.

(6) Fraud and corruption prevention strategies demonstrate sound management practice and governance and assist the University in deterring unethical behaviour.

### **Assets of the University Vulnerable to Fraud and Corruption**

(7) The outcomes of committing fraud can be either tangible or intangible and can involve misuse of:

- a. academic records or qualifications;
- b. admittance to a program or course;
- c. consulting fees;
- d. curriculum material;
- e. examination results;
- f. funding;
- g. grants;
- h. insurance claims;
- i. internet time;
- j. motor vehicles;
- k. payroll;
- l. personal information;
- m. petty cash;
- n. property, plant and equipment;
- o. research information;
- p. rights and ownership of new inventions;
- q. supplies;
- r. telephone calls; and
- s. time.

### **Perpetrators of Fraud and Corruption**

(8) It is possible for anyone to commit fraud or corruption. It can be done alone or in collusion with others within or outside the University. Fraud or corruption could be perpetrated against the University by:

- a. a full-time, part-time or casual staff member;
- b. temporary or agency employee;
- c. a student;
- d. an agent;
- e. an external individual; or
- f. a contractor or service provider.

## **Fraud and Corruption Awareness**

(9) You need to be kept informed about the University's Fraud and Corruption Prevention and Response Strategy and what part you are expected to play in it. The University will achieve this in a number of ways, including:

- a. giving every employee a copy of the Staff Code of Conduct as part of their contract of employment;
- b. informing new staff during induction training;
- c. delivering fraud awareness training across as much of the University as possible;
- d. making the Staff Code of Conduct and key attributes of the Fraud and Corruption Prevention and Response Strategy available to all staff via the University's website;
- e. incorporating reminders to staff and students of their obligations to ethical conduct and public duties into policies, procedures, appointment letters, guidelines, training, and student and / or staff communications.

## **Fraud and Corruptions Detection**

(10) The early detection of fraud and corruption is an essential element of the University's prevention strategy.

(11) Surveys of fraud conducted in Australia regularly demonstrate that employees are the most likely to discover fraud. As a member of staff, you are therefore the key factor in detecting fraudulent or corrupt behaviour.

(12) It should be your aim to detect fraud or corruption as soon as possible after it occurs. There are a number of ways in which fraud may be detected. These may include:

- a. monitoring high risk jobs or areas;
- b. when internal controls are breached;
- c. during monthly reviews of strategic management reports such as telephone usage reports;
- d. targeted post transactional review that may indicate altered or missing documentation, falsified or altered authorisation or inadequate documentary support;
- e. departmental reviews or internal audits; or
- f. when you notice changes in behaviour patterns such as unusual behaviour or expensive lifestyles of other staff members.

## **Fidelity Guarantee Insurance**

(13) The University is covered by Industrial Special Risks insurance. The insurance is renewed on an annual basis (currently 31 October each year). This insurance covers physical loss, destruction or damage to all real and personal property of every kind and description belonging to the University or for which the University is responsible or has assumed responsibility to insure prior to the loss. There are no geographical limits on this cover.

(14) The two components relevant to this strategy include:

- a. Fidelity; and
- b. Burglary and theft.

(15) There is currently an excess on each claim.

(16) The policy covers any person acting as an agent of the University in carrying out their duties at the University.

(17) The Industrial Special Risks insurance policy is maintained by the Office of Financial Services.

# Fraud and Corruption Risk Management

## Strategic Audit Plan

(18) A Strategic Audit Plan is prepared each year by an external audit firm and signed off by the Audit and Risk Committee. This Plan outlines audit and risk management activities for the ensuing year.

(19) The Strategic Audit Plan also incorporates a University-wide risk assessment that provides the basis for refining the scope and objectives of each of the audit and risk management activities to be undertaken.

## Internal Audit Plan

(20) An Internal Audit Plan is prepared by Deloitte and plays a crucial role in the prevention of fraud and corruption within the University.

(21) The University outsources its Internal Audit on a three-year cycle. The Internal Audit function is conducted by Deloitte, which reports to the University's Audit and Risk Committee.

(22) In relation to fraud and corruption control, the University's internal audit includes ongoing reviews of controls within the University, including:

- a. reviewing the effectiveness of controls - how they are implemented in practice - via observation, interview of key personnel, review of records and sample testing;
- b. systems type testing - detailed walkthrough of significant processes; and
- c. special audits where particular areas of concern have been identified.

## Fraud and Corruption Prevention and Response Strategy

(23) The Fraud and Corruption Prevention and Response Strategy is a best practice of the [Independent Commission Against Corruption \(ICAC\)](#). It is a framework for how the University prevents and responds to fraud.

(24) Fraud and corruption control requires continuous discussion. This may include:

- a. keeping track of what other universities are doing regarding policies and procedures;
- b. ensuring reports or reviews of fraud and corruption at Australian universities are assessed for their likely impact on the University's strategy; and
- c. encouraging innovation in fraud and corruption control development, procedures and processes by staff.

(25) The fraud and corruption control and response strategy is prepared, reviewed and amended as required by the Fraud Control Officer.

## Risk Assessment

(26) The University aims to conduct fraud risk assessments at least every three (3) years. Where appropriate, the University may introduce a rolling program of risk assessments.

(27) When the University undergoes a substantial change in structure or function, or where there is a significant transfer in function (for example, as a result of outsourcing), the University may undertake further fraud risk assessment in relation to the changed functions. This fraud risk assessment may form part of a general business risk assessment exercise.

(28) Staff at all levels in the University should be involved in the fraud and corruption risk assessment process, particularly those with detailed knowledge of the University's practices and procedures, because they understand system weaknesses and whether internal controls are being adhered to. The University recognises that it is important

to ensure that the staff involved have relevant training, access to all necessary information and an understanding of the areas to be examined.

(29) The University's risk assessment must consider fraud risks from both within the University and from external factors. Risk assessments must also consider fraud risks that may emerge in the future. For example, the University needs to be aware of the changing nature of fraud arising from the greater use of external service providers and developments in information technology.

(30) Core areas that a fraud risk assessment should consider include:

- a. information technology and information security;
- b. electronic commerce, electronic service delivery and the Internet;
- c. outsourced functions;
- d. grants and other payments or benefits programs;
- e. tendering processes, purchasing and contract management;
- f. intellectual property development and commercialisation;
- g. revenue collection;
- h. use of University credit cards;
- i. travel allowances and other common allowances;
- j. payments, including salaries; and
- k. property and other physical assets, including physical security.

(31) Fraud and corruption risk assessments should be conducted in accordance with the Australian/New Zealand Standard (AS/NZS 4360:1999) - Risk Management. The University documents the risk assessment process in order to:

- a. reflect the risks across the range of functions performed by the University;
- b. measure risks in a comparable way;
- c. provide a supportable rating of the risks of fraud including both likelihood of a risk occurring and consequences for the University if the risk did occur;
- d. fine tune the process, as appropriate; and
- e. replicate the process.

(32) Fraud risk assessments provide details of the University's risk profile and vulnerability. Unauthorised access could substantially undermine the viability and effective management of the University. Therefore fraud risk assessments may be restricted in circulation, consistent with the sensitivity of the material or subject matter.

### **Integrating Fraud and Corruption Risk Assessment with Overall Risk Assessment**

(33) It is important that fraud and corruption risks are considered in the broader context of overall business risk so that fraud risk assessment takes into account University-wide strategic planning. Fraud risk should not be looked at in isolation from the general business of the University. There is considerable overlap between enterprise risk, business risk, audit risk, security risk and fraud risk. Other risk management approaches may have already highlighted changes in strategic directions that will impact on future fraud risk profiles and control frameworks.

### **Implementation of Proposed Actions**

(34) All fraud and corruption risks rated as having a High or Very High level of residual seriousness require one or more proposed actions aimed at achieving one or more of the following:

- a. alteration of existing internal control procedures;

- b. new internal control procedures;
- c. procedures aimed at detecting fraud; and
- d. fraud prevention strategies.

(35) The University may also develop proposed actions for risks assessed as being a lower residual risk. To ensure comprehensive implementation and provide a periodic check on progress, the risk assessment teams should, where possible, allocate personal responsibility for the implementation of each action item.

### **Review of Effectiveness of Strategies**

(36) It is expected that Faculties and Offices will review the results of the fraud risk assessments at least annually to ensure that strategies developed during the course of the most recent fraud risk assessment are reviewed for effectiveness and amended where necessary.

(37) The Fraud Control Officer coordinates the compliance with the annual review of fraud mitigation strategies.

## **Section 5 - Definitions**

(38) Commonly defined terms are located in the University [Glossary](#). The following definitions apply for the purpose of this Guideline:

### **Definition of Corruption**

(39) The [Australian Standard on Fraud and Corruption Control AS8001-2003](#) defines corruption as:

- a. "Dishonest activity in which a director, executive, manager, employee or contractor of an entity acts contrary to the interests of the entity and abuses his / her position of trust in order to achieve some personal gain or advantage for him or herself or for another person or entity."

(40) The [Independent Commission Against Corruption \(ICAC\)](#) defines corrupt conduct, as it affects a public authority, as:

- a. "Corrupt conduct is also any conduct of any person (whether or not a public official) that adversely affects, or that could adversely affect, either directly or indirectly, the exercise of official functions by any public official, any group or body of public officials or any public authority and which could involve any of the following matters:
  - i. official misconduct (including breach of trust, fraud in office, nonfeasance, misfeasance, malfeasance, oppression, extortion or imposition)
  - ii. bribery
  - iii. blackmail
  - iv. obtaining or offering secret commissions
  - v. fraud
  - vi. heft
  - vii. perverting the course of justice
  - viii. embezzlement
  - ix. election bribery
  - x. election funding offences
  - xi. election fraud
  - xii. treating

- xiii. tax evasion
- xiv. revenue evasion
- xv. currency violations
- xvi. illegal drug dealings
- xvii. illegal gambling
- xviii. obtaining financial benefit by vice engaged in by others
- xix. bankruptcy and company violations
- xx. harbouring criminals
- xxi. forgery
- xxii. treason or other offences against the Sovereign
- xxiii. homicide or violence
- xxiv. (atters of the same or a similar nature to any listed above
- xxv. any conspiracy or attempt in relation to any of the above.”

(41) Examples of corrupt conduct to which the University may be subject include:

- a. payment of secret commissions (bribes) paid in money, or some other value, to a University staff member that is related to a specific action or decision of the University staff member;
- b. release of confidential information, for other than a proper business purpose, sometimes in exchange for either a financial or non-financial advantage;
- c. collusive tendering (the act of multiple tenderers for a particular contract colluding in preparation of their bids);
- d. a University staff member manipulating a tendering process to achieve a desired outcome;
- e. conflict of interest involving a University staff member acting in his or her own self-interest rather than the interests of the University;
- f. nepotism and cronyism where the appointee to a University position is inadequately qualified to perform the role to which he or she has been appointed, or not selected on merit; and
- g. receiving personal benefits in exchange for assisting a consultant to gain work at the University.

### **Definition of Fraud**

(42) Fraud is recognised as a subset of corruption.

(43) The [Australian Standard on Fraud and Corruption Control AS8001-2003](#) defines fraud as:

- a. “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 whether or not deception is used at the time, immediately before or immediately following the activity. This also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position.”

(44) Examples of fraud on the University include, but are not limited to:

- a. misappropriating University assets, including use of the University’s assets for private purposes;
- b. abuse of University property;
- c. abuse of University time;
- d. causing a loss to the University, or avoiding or creating a liability for the University by deception;
- e. claiming for travel entitlement to attend a course and then not attending the course and not reimbursing travel monies;

- f. evasion of fees due to the University;
- g. fabrication, falsification or plagiarism of research;
- h. false invoicing for goods or services never rendered;
- i. falsely misrepresenting the author of essays, assignments or research to the University;
- j. making cheques out to false persons;
- k. making, using or possessing forged or falsified documents such as Degrees or Academic Records;
- l. misapplying government grant monies;
- m. misappropriating official order forms to gain a personal benefit;
- n. obtaining an unjust advantage by misusing information gained during the course of employment with the University;
- o. providing false or misleading information to the University, or failing to provide information, where there is an obligation to do so;
- p. receiving 'kickbacks' or 'secret commissions' from a contractor;
- q. submission of exaggerated or wholly fictitious accident, harassment or injury claims;
- r. misuse of personal or sick leave;
- s. theft of cash or petty cash;
- t. theft of intellectual property;
- u. theft of plant, equipment or inventory;
- v. unauthorised transferral of University income;
- w. unlawful use of University computers, vehicles, internet, telephones and other property or services including operation of a private business using University facilities and time;
- x. using a University credit card for personal expenses and claiming them as University-related; and
- y. using taxi vouchers for private purposes.



## Status and Details

<b>Status</b>	Historic
<b>Effective Date</b>	22nd February 2021
<b>Review Date</b>	1st June 2021
<b>Approval Authority</b>	Vice-President, Finance and Resources
<b>Approval Date</b>	17th June 2011
<b>Expiry Date</b>	30th August 2021
<b>Responsible Executive</b>	Robin Payne Vice-President, Finance and Resources
<b>Responsible Officer</b>	Robin Payne Vice-President, Finance and Resources
<b>Enquiries Contact</b>	Kylie McKiernan Chief Risk Officer