1. INTRODUCTION

The Fraud Control Policy makes a number of statements aimed at protecting the University's assets, interests and reputation. The purpose of this procedure is to outline the actions to be taken to minimise the risk to the University of incurring loss as a result of fraud or corrupt conduct.

Fraudulent activities may include but are not limited to:

- Electronic Funds Transfer (EFT) and bank file manipulation;
- Theft of inventory;
- Misappropriation of funds;
- Petty cash fraud;
- Purchases for personal use;
- Expense account fraud;
- False invoicing;
- Kickbacks/bribery;
• Conflict of interest;
• Misuse of resources;
• Cheque forgery;
• Services obtained by false documentation;
• Disclosure or breach of confidentiality;
• Information theft;
• Falsifying payroll records;
• Property or investment fraud;
• Credit card fraud;
• Data and data integrity fraud;
• Funding misrepresentation; and
• Secondary employment.

It is recognised that there are a number of factors that typically enable fraud. These factors may include but are not limited to:
• Poor internal systems/controls;
• Non-compliance with systems or controls;
• Poor supervision/management of staff;
• Lack of segregation of duties;
• Poor physical security;
• Collusion; and
• Poor background/security checks performed in recruitment processes.

Systems of internal controls are therefore needed to minimise the incidence of fraud. Such controls are integrated into a number of systems within the University that include both preventative and detection controls. This is further detailed in paragraphs 2.3.1 and 2.3.2. This procedure aims to facilitate achievement of the objectives of the Fraud Control Policy by establishing awareness, responsibilities, reporting procedures and staff training.

2. **FRAUD PROCEDURES**

The University has taken into consideration the 10-element model from the CCC to support the fraud control framework.

The CCC's 10-elements model includes:

2.1 University-wide integrated policy
2.2 Risk assessment
2.3 Internal controls
2.4 Internal reporting
2.5 External reporting
2.6 Public interest disclosures
2.7 Investigations
2.8 Code of conduct
2.9 Staff education and awareness
2.10 Client and community awareness
2.1 **University-Wide Integrated Policy**

The Policy sets out the objectives and responsibilities for controlling fraud within the University. It communicates the University's commitment to best practice and creates a framework that reduces risks of fraud and establishes an effective internal control structure.

The fraud control policy outlines the University's zero-tolerance stance on fraud.

The Finance, Resources and Risk Committee monitors the effectiveness of the fraud control procedures. The Vice President (Corporate Services) is responsible for coordinating fraud risk management and reporting to the Committee on a regular basis.

2.2 **Risk Assessment**

Fraud risks will normally be identified, evaluated and managed by responsible officers and reported in accordance with the University's decision-making processes. The University's fraud risks will be maintained in a Fraud risk register and will be updated annually with appropriate review of control strategies and actions required.

Risks will be assessed in accordance with the University's risk management framework and strategic priorities, taking account of the likelihood of the risk occurring, its potential impact and the range of implications it may have for the University.

Where an unacceptable risk is identified, relevant University staff with management responsibilities in areas that may be affected, will be informed of it, and will be required to take action, as required, to address the matter and inform staff, or other persons within their area of responsibility, about the matter.

2.3 **Internal Controls**

The Financial Accountability Act 2009 requires the Vice Chancellor (being the accountable officer) of Griffith University to establish and maintain appropriate systems of internal control as well as risk management.

The University will maintain a reliable system of internal controls to help prevent and detect fraud. Such controls will be integrated into a number of other policies and systems across the University. The responsibility for such controls will rest with the individual managers who have delegation and authority within the respective divisions. For example, controls for fraud in the finance system will rest with the Chief Financial Officer and controls aimed at protecting information systems will rest with the Chief Technology Officer. Internal controls include:

- Suitable recruitment procedures;
- Segregation of duties;
- Security (physical and information systems);
- Consideration of risk and mitigating strategies;
- Supervision and internal checks;
- Approvals within delegated authority;
- Budget controls and reconciliations;
- Clear reporting lines;
- Staff development and training;
- Asset management procedures; and
- Annual procurement related declarations from relevant staff and major suppliers (in progress).

The system of internal controls is subject to regular reviews and audits by both management and the internal auditors, including reviews of the adequacy and effectiveness of internal controls over business activities with a potential for material fraud.
2.3.1 Fraud Prevention

As fraud can occur at various levels, appropriate preventive techniques are in place. Preventive techniques encompass policies, procedures, training, and communication that stop fraud from occurring.

Among the University's many elements in fraud prevention are Human Resource procedures, authority limits, and transaction level procedures.

2.3.1.1 Recruitment practices

Recruitment practices include strategies to prevent fraud within the University. These strategies may include:

- Ensuring applicants are interviewed by more than one person;
- Verifying qualifications, transcripts and other certification or documentation where relevant;
- Referee checks to validate an applicant's employment history;
- Supervisors are required to be aware of potential conflicts of interest in hiring decisions; and
- Criminal history checks where this has been determined to be an inherent requirement of the role.

2.3.1.2 Performance management program

The annual performance management program will evaluate behaviour and performance as well as work related competence. Regular and robust assessment of performance with timely and constructive feedback will help prevent potential fraud and misconduct.

2.3.1.3 Exit Interviews

Exit interviews will be offered to continuing staff leaving the University as this may help the Director, Office of Human Resource Management to determine whether there are issues regarding management's integrity or information regarding conditions conducive to fraud.

2.3.1.4 Authority Limits

A staff member's level of authority will be commensurate with his or her level of responsibility to prevent fraud.

2.3.1.5 Transaction Level Procedures

As fraud schemes often involve the use of third party entities/individuals or related parties, the University will review all third-party and related-party transactions to prevent fraud. Declarations of potential conflicts of interest are made and recorded at management, executive, committee and University Council levels.

2.3.1.6 Procurement practices

Procurement practices include strategies to help prevent and possibly detect instances where fraud may occur. These strategies may include:

- Requiring appropriate staff and major suppliers to complete annual declarations relating to conflicts of interest or inducements sought/given in relation to business conducted on behalf of the University. For staff members this could include confirmation of compliance with applicable policies such as the Code of Conduct and Gifts and Benefits.
- Periodic independent review by Finance or Internal Audit of work allocated to pre-qualified suppliers to ensure that the quoting and allocation of work is transparent and equitable. Any continual preference for a particular supplier could indicate potential fraud.
• Major suppliers engaged by the University be made aware of the policies relating to conflicts of interest and gifts and benefits.

2.3.2 Fraud Detection

The University has detection controls in place. This serves as strongest deterrents to fraudulent behaviour.

Detection methods include but are not limited to anonymous reporting mechanisms (whistle blowing) and proactive fraud detection procedures specifically designed to identify fraudulent activity.

2.3.2.1 Whistle blowing

Whistle blowers can approach the Fraud Control Officer which is delegated to the Vice President (Corporate Services), or the Director, Audit, Risk and Compliance without fear of reprisals and in the full knowledge that their interests will be protected. Any claim of fraud will be handled with confidentiality as allegations of fraud, even if not proven, can cause damage to individual reputations and expose the University to legal claims for damages.

A Whistle blower hotline exists to serve as a deterrent and it is in the form of email. The email address is whistleblowing@griffith.edu.au

The Whistleblowing website also references the University’s Public Interest Disclosure Policy.

2.3.2.2 Proactive Fraud Detection Procedures

The University uses data analysis, continuous auditing techniques, and other technology tools to detect fraudulent activities as part of internal audit and external audit reviews. These are established as part of the audit plans on an annual basis.

2.4 Internal Reporting

The internal reporting system at the University will encourage a free flow of information through the normal supervisory and management channels. In addition, the General Staff Misconduct Committee Guidelines and Academic Staff Misconduct Committee Guidelines provide additional guidance in the reporting and investigation of potential fraud incidents.

The cooperation of staff is vital to the successful implementation of measures to guard against fraud. The University encourages staff to report any concerns they have, without fear of being penalised. Staff who have concerns about any improper conduct should, where appropriate, raise those concerns with their supervisor or manager.

The supervisor or manager should make use of the fraud officer email facility or document the nature of the employee's concerns and then report this to the Vice President (Corporate Services).

The Vice President (Corporate Services) will document all such reports and carry out an initial evaluation of each incident. The Vice President (Corporate Services) will commission an independent investigation of the incident, if required, and a review of internal controls relevant to the incident.

Where a staff member believes that it is inappropriate to report concerns to their supervisor or manager the concern should be raised directly with the Vice President (Corporate Services). In circumstances where either a staff member or manager believes it to be inappropriate to report concerns about fraud to the Vice President (Corporate Services), the concern should be reported to the Vice Chancellor.

Staff are encouraged to raise their concerns openly as this usually assists the investigative process. However, anonymous concerns can be made in the same manner. That is, to a supervisor or manager in the first instance, or directly to the Vice President (Corporate Services). Anonymous concerns should be made in writing and should provide as much factual information as is known to the staff member.
2.5 **External Reporting**

The Crime and Corruption Act 2001 requires that agencies such as the University report any suspected corrupt conduct (including fraud). Fraud can be reported to the following independent statutory bodies:

- Queensland Audit Office (QAO);
- Queensland Police Service (QPS);
- Crime and Corruption Commission (CCC); and
- Queensland Ombudsman.

With the exception of the Crime and Corruption Commission, the internal reporting mechanisms currently in place should be exhausted prior to reporting any fraud to the external bodies. In the case of the Crime and Corruption Commission, the Vice Chancellor, as chief executive officer, has a duty to notify the Crime and Corruption Commission if he/she reasonably suspects that corrupt conduct may have occurred.

2.6 **Public Interest Disclosures**

Public Sector Ethics Act 1994, Public Interest Disclosure Act 2013 and Crime and Corruption Act 2001 are the legislations covering Public Interest Disclosures (PID). PID reporting is to follow Griffith University's internal and external reporting mechanisms, as outlined in the PID policy.

The University will take all the reasonable steps to protect and provide support to disclosers from any reprisal.

2.7 **Investigations**

It is essential that any breaches of the code of conduct or controls, regardless of where in the organisation, or by whom, they are committed, be reported and dealt with in a timely manner.

In the event that there is reasonable suspicion of fraud (based on allegations being made, audit findings or for any other reason) an investigation will be conducted. In this event, the procedures of the relevant misconduct provisions will apply.

2.8 **Code of Conduct**

The Public Sector Ethics Act 1994 requires agencies such as University to have Code of Conduct.

The University has a Code of Conduct and a Conflict of Interest policy in place. This Code provides guidance on acceptable standards of behaviour and how staff and individuals should conduct their duties while working towards achieving the University's Strategic Plan.

The University expects that all staff and individuals are placed in a position of trust and requires all to behave ethically, professionally and protect the assets of the University.

2.8.1 **Conflict of Interest**

Staff, management or contractors involved in investment, discussion, proposals and awarding major contracts are required to certify that they have no conflict of interest in the proposal/discussion.

Any staff, manager or contractor with a conflict or potential conflict of interest in any matter involving the University is required to disclose this conflict to their Group or Division manager, who will notify the Vice President (Corporate Services). The Vice President (Corporate Services) will then decide what further involvement, if any, the staff will have in the matter. As a general rule, any staff with a conflict or potential conflict of interest will be excluded from further involvement in that matter. Actual or potential conflicts of interest will be recorded by the Fraud Control Officer in a Register of Interests maintained for this purpose and may also be recorded in the staff's personnel file.

2.8.2 **Disciplinary Action**

Any staff, manager or contractor found to have committed fraud, will be subject to the actions specified in the University's misconduct or serious misconduct procedures. This may include termination of the staff member's employment.
Staff, management or a contractor who is suspected of having committed a crime may be reported to the Police.

2.9 Staff Education and Awareness

Fraud awareness will be promoted throughout the University by a range of formal and informal means. The University will ensure its staff are aware of its Fraud Control Policy by ensuring it is included in the annual reminder to staff from the Vice Chancellor about the University’s key integrity policies and by ensuring policy updates are communicated to staff.

Training will be provided to relevant staff. The University will promote fraud prevention initiatives through communication to staff and will report on how it has responded to identified fraud incidents where appropriate. Informally, managers will promote awareness of fraud risk and control strategies during group and team meetings as appropriate.

2.10 Client and Community Awareness

The University maintains public trust and confidence by behaving ethically. Issuing a code of conduct and a number of policies such as the Fraud Control Policy communicate to our clients and community that the University has zero-tolerance stance on fraud.

3. REVIEW

This procedure will be reviewed every two years by the Vice President (Corporate Services) for adequacy and effectiveness. Furthermore, it will be reviewed after any incident of fraud.