

Prevention of Fraud and Corruption

The potential impact of fraud and corruption represents a significant risk to Deakin's assets and reputation.

To address this issue, the "Prevention and control of fraud and corruption" operational policy and procedure has been developed and approved by the Vice-Chancellor in December 2007.

Under the policy, Faculties and Other Areas within Deakin are required to establish and maintain processes for the prevention, detection and elimination of fraud and corruption and to identify and manage these risks through the risk management program.

To assist you in managing the risk, the Risk and Insurance team has prepared the following generic risk.

1. The Risk Title, Risk Category and Consequences – will be the same across all areas of the University:

Risk Title: Failure to prevent fraud or corruption across the **insert your Faculty or Area**, which may lead to:

- Damage to University reputation and culture;
- Loss of revenue and associated increased costs;
- Reduced capacity to perform core University activities;
- Litigation (from failure to meet regulatory or other obligations)

Risk Category: Financial Management risk

Consequences: Financial, University Performance, Reputation outrage and media

2. Strategic Objective, Responsibility and Ratings

These will differ across the various areas of the University.

3. Contributing Factors and Controls

The Contributing Factors and Controls have been separated into specific categories, to assist you in selecting those that are appropriate to your area.

Because of the sheer number of alternatives in these lists, we recommend that you limit your selection to the top 10 Contributing Factors applicable to your area, and the 20 of your most effective Controls.

If there is a Control that you would like to use, but you do not have it in place as yet, then you can use this wording to create an Action. This will also assist you in transferring it to a Control when the Action has been achieved.

Contributing Factors – choose up to 10 (in total) :

CONTRACTS

- Collusion or improper relationships with partners/suppliers.
- Failure to appropriately manage relationships
- Lack of adherence to tender/contract requirements
- Lack of transparency in evaluation of contracts and/or commercial activities.
- Undetected conflicts of interest in the tender evaluation process.
- Submission of false tender documentation and/or false product endorsements / claims.

FINANCE

- Fraudulent Financial Reporting.
- Fraudulent insurance claims.
- Inappropriate DFMS access provided.
- Insufficient monitoring of personal use by staff of University provided credit cards and mobile phones.
- Misuse of Corporate credit cards
- Unauthorised use of University credit cards.
- Misappropriation of cash
- Misuse of petty cash requests.
- Manipulation of procurement process
- Unethical behaviour within purchasing function.
- Duplicate payments to suppliers.
- Misuse of Purchasing system.
- Misappropriation of proceeds from asset sales
- Assets not recorded on asset register – not following fixed asset procedure
- Completing asset disposal form, when item has been lost
- Failure to protect/secure/ manage University assets
- Lack of communication between FBSD and FOA when assets are relocated or disposed of.

IT

- Failure of IT security mechanisms
- Failure to ensure data security and integrity.
- General availability of brute force password crackers
- High lap-top usage.
- Passwords stored on ITSD Servers in clear text (not encrypted)

POLICIES

- Lack of knowledge of documented policies and processes
- Lack of policy adherence, improper financial delegations.
- Infrequent use of policies and procedures.
- Insufficient communication of FBSD policies and procedures.
- Inappropriate admission and selection standards.
- Ineffective security policies
- Inadequate controls and monitoring.
- Risk management and audit processes do not detect inappropriate or unethical activity.

RESEARCH

- Staff are unaware of ethics protocols and processes.
- Scientific fraud more prevalent in laboratory work areas than in other areas.
- Fraudulent research results.
- Pressure to perform, research that by-passes normal procedures.
- Pressure to succeed in securing grant funding.

Contributing Factors – continued:

SECURITY

- Improper use of University facilities
- Physical security protocols not followed
- Responsibility for assets is placed with relevant staff in FOA.
- Security of premises
- Theft of University property.
- Unauthorised access.

STAFF

- Collusion or misconduct by staff.
- Desire for some form of financial benefit or advantage.
- Failure to comply with Academic quality assurance policies and procedures
- Inadequate training,
- Inexperienced technical staff
- Lack of consistency between on shore and off shore course delivery & assessment.
- Misuse of Travel arrangements.
- Nepotism and/or cronyism
- Non-disclosure of pecuniary interests.
- Poor academic quality assurance measures.
- Staff non-compliance with Uni Policies and Procedures.
- Staff not aware of security obligations
- Unauthorised release of confidential information
- Unethical activity.
- Manipulation of leave records
- Poor leave record keeping
- Payments to fictitious employees
- Overpayments to employees
- Misrepresentation of qualifications / skills / experience / ability to work in Australia by employees
- Reimbursement claims for non-work related activities

STUDENTS

- Academic records or personal details may be changed.
 - Exam papers may become available to some students prior to the examination.
 - Manipulation of student grades through favouritism in the assessment process (ie. "soft marking")
 - Student misconduct.
-

Controls – choose the top 20 of your most effective Controls:

Detective Controls

AUDITS

- Internal Audit Unit assesses applicable control(s) for reasonableness.
- Placed on University audit schedule.
- Internal Audit program incorporating reviews of adherence to policies & procedure
- Regular internal audit of fraud controls and reviews of fraud control procedures
- Regular internal audits of controlled entities and subsidiary companies, including balance sheets.
- Periodic internal audits of IT, security and stability of corporate applications
- Annual audit of art collection
- Audit checking on Callista
- University audit of admission, teaching, assessment and moderation
- Asset register maintenance & audit
- Regular equipment audits
- Audit of qualifications of staff
- Audits conducted by ISO9001 Quality Assurance auditor
- Regular External Security Audits are undertaken
- Stocktakes are completed on a cyclical basis
- Risk Register Review process

FINANCE

- Financial transaction reviews
- FBSD monthly financial reconciliation process.
- Regular review of purchase order system
- Corporate credit card expenditure is routinely monitored centrally within FBSD
- Insurance claims verified prior to submission to insurer
- Financial transaction reviews
- Accounts payable staff have access to all authorised signatory details and specimen signatures.
- Verification checks by accounts payable officers
- Cashier staff routinely monitor all University petty cash reimbursements.

CONTRACTS

- Contract management software.
- Contracts register.
- Financial diligence in tender process
- Consultant manager monitoring relationships
- Monitoring processes in relation to partnerships including Offshore Teaching Partnerships.

RESEARCH

- Monitoring of expenditure of research grants

STUDENTS

- Plagiarism detection software
- Option to independently verify prior study claims of applicants
- Ensure that Supervisors acknowledge receipt of examination papers.
- Examination Contents Summary Receipt Confirmation
- Track and Trace database for exams

Preventative Controls

CONTRACTS

- Policy on authority to sign contracts
- Spread procurement contracts
- Adequate contractual agreements
- Contractor registration through HR/Solicitors Office
- Adequate Contractor selection processes maintained.
- Vetting of contracts
- Preferred supplier system
- Supplier Contract in place
- Supplier reviews
- Contracts Assessment Sub-Committee.
- Purchasing policy and procedure
- Procurement Manual
- Independent Quantity surveyor certification of value of works complete.

FINANCE

- Procedures for use of corporate credit cards
- Corporate credit cardholders sign cardholder agreement prior to issue of card
- Credit cards subject to Financial Delegations Policy and acquittal process.
- Original receipts for corporate credit cards are required for acquittal
- Armaguard services for cash collection
- Safes within cashier workspaces
- Police checks of applicants for positions identified as potential for fraud risk
- Asset register maintained
- Finance related policies and procedures available on "The Guide"
- Workflow approval controls within purchasing system and expert review by FBSD.
- Cheque signatories per Financial Delegations Policy
- DFMS access procedures
- Travel subject to Financial Delegations Policy and acquittal process.
- DFMS account codes support differentiation between expenses and assets
- Purchase order and approval processes
- Adherence to university policy and procedures with regards to expenditure approvals
- Expense reimbursement claims require original receipts
- Receipting system
- Twice yearly completion of controlled and associated entities risk assessment.
- Report on management of University assets required by Audit Committee & by Council.

IT

- Integrity of staff and student records
- Account Lockout
- Password complexity
- Password Ageing
- IT Security Awareness program
- IT Security Officer role established
- Password complexity security policy rules

Preventative Controls

POLICIES and PROCEDURES

- Conflict of interest procedure.
- Admission and selection policy and procedures
- University Policies and procedures in relation to OHS, Academic misconduct, Financial matters
- Policies & procedures in place that promote high standards & discourage misconduct & fraud
- Senior Mgrs. Responsible for minimising risk of unethical behaviour in areas of their responsibility
- Faculty statement on assessment practices
- Faculty admissions and selection standards for HDR students
- Senior Mgrs. Responsible for compliance with uni. policies and procedures in areas of their responsibility
- Staff Induction includes Code of Good Practice in Research Policy and Procedure
- Regular reviews of procedures for access to private information
- Fixed Assets Management procedure
- Purchasing policy and procedure
- Contracts policy suite
- IT security policies, procedures and protocols
- Recruitment of staff procedure suite
- Salary advance procedure
- Travel procedure
- Ceasing employment procedure
- Fraud and corruption prevention and control policy and procedure
- Code of Conduct for staff
- Business Continuity Management framework includes Crisis Management response for fraud and corruption "incidents"
- Academic Board policies and procedures.
- Staff Code of Conduct

RESEARCH

- Code of good practice for research
- Peer review of research applications
- Code of Good Practice in Supervision of Higher Degrees by Research
- Peer review of research applications

SECURITY

- Security procedures and policies
- Wide range of Policies & Procedures covering: Selection, Assessments, Advanced Standing
- Hologram on Deakin transcripts
- Secure ordering and storage of transcript paper stocks
- Building Plan includes access control system to restrict access by swipe card only
- Alarm monitoring in most parts of the Uni
- ID tags for visitors
- Equipment loans register in place
- Master keys stored in a key safe in a secured storeroom
- Management of access cards and keys
- Video recording
- Key and card security access controls.

STAFF

- Academic Board Compliance Program.
- Reference checks
- Asset management system
- Leave requests for staff processed on-line
- Leave requests are subject to supervisor approval
- Separation of duties
- Internal Audit Unit staff with qualifications in fraud investigations

Preventative Controls

STUDENTS

- Student charter
- Student code of conduct
- Plagiarism training for staff and students
- All Exam Supervisors undertake the Supervisor On-Line Training Module
- Academics briefed on exam security requirements
- Anonymity & security of the exam storage and processing centre
- Students must show photo identification at exam venue.
- All student hardcopy files kept in secure area.
- Surveillance cameras within the exam storage and processing centre
- Student manual and unit guides explain plagiarism
- Exam paper preparation and submission requirements detailed on website
- Anti plagiarism statement signed by students for each assignment
- Course planning designed to minimise repetition of assignment material across years
- Access to student information by ID and password only
- Callista write-access and functional area of access limited to approved DSA staff
- Tax-file number algorithm checking procedure is built into Callista
- Student data stored electronically on Windows NT

Reactive Controls

- Ability to remove direct IP access at short notice
- List of non satisfactory suppliers
- Process for declaration of salary overpayments
- Salary overpayments procedure
- Directors and Officers Insurance
- Fidelity Guarantee Insurance
- Professional Indemnity
- ISR (Property) Insurance
- Public Liability insurance
- Product liability insurance
- Crime insurance

Interdependent Controls

- Asset Management Strategy
- Compliance register
- Security - building alarms & CCT