Fraud and Corruption Control Policy

Section 1 - Purpose

(1) The purpose of this policy is to protect the reputation and assets of Charles Sturt University (the University) from fraudulent and corrupt activities.

(2) This policy establishes a fraud and corruption control system (FCCS) consistent with the Australian Standard on Fraud and Corruption Control (AS 8001:2021). The policy provides guidance on how to prevent, detect and respond to incidents of fraud and corruption and:

a. reinforces management's commitment to, and responsibility for, identifying risk exposures to fraudulent and corrupt activities, and ensuring all staff and students are aware that the University has zero tolerance for fraud or corrupt conduct, and
b. requires staff to perform their duties with honesty and integrity in accordance with the framework of ethical conduct that underpins the expected standards of behaviour for all members of the University community.

Scope

(3) This policy applies to all staff, students, customers, contractors, business associates, partners, external service providers, volunteers and controlled entities of the University.

(4) This policy should be read in consideration of the University's Organisational Assurance Policy and the Risk Management Policy.

(5) The reporting and investigation of any allegations of fraud or corrupt conduct are dealt with under the Whistleblowing (Reporting Wrongdoing) Policy and associated processes.

(6) Research, academic and general misconduct by staff and students will be dealt with under the relevant policy instruments such as the Research Misconduct Procedure and the Student Misconduct Rule 2020.

(7) Disciplinary matters in relation to staff are dealt with in accordance with the provisions of the prevailing Charles Sturt University Enterprise Agreement.

Section 2 - Glossary

(8) For the purpose of this policy, the following additional terms have the definitions stated:

a. Certification documentation – means, as described by the Higher Education Standards Framework, a testamur, a record of results or an Australian Higher Education Graduation Statement.
b. Corrupt conduct – means the definition of corrupt conduct as set out in the Independent Commission Against Corruption Act 1988 (the ICAC Act). In summary, corrupt conduct is the dishonest or partial exercise of University functions by an official of the University. Examples include the improper use of knowledge, power or position for personal gain or the advantage of others, acting dishonestly or unfairly, or breaching public trust, or a University official being influenced by another person to use their position in a way that is dishonest, biased or

breaches public trust. Corrupt conduct is generally taken as something that is intentional, not something that occurs through mistaken action.

c. Corruption – means the definition of corruption as set out in AS 8001:2021. Corruption means dishonest activity in which a person associated with an organisation 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.
d. Fraud – means the definition of fraud as set out in AS 8001:2021. Fraud means dishonest activity causing actual or potential gain or loss to any person or organisation including theft of moneys or other property by those in scope of this policy. Fraud also includes the deliberate falsification, concealment, destruction or use of falsified documentation used or intended for use for a normal business purpose or the improper use of information or position for personal benefit.
e. Public official – means an employee of or any person otherwise engaged by or acting for or on behalf of, or in the place of, or as deputy or delegate of Charles Sturt University is a public official under the Independent Commission Against Corruption Act 1988 (NSW).
f. Relevant anti-corruption agency – means the NSW Independent Commission Against Corruption (ICAC) or equivalent state or territory agency.
g. Transaction – means an activity undertaken by an employee of the University on behalf of the University including but not limited to administration of student records, financial payments, procurement of goods or services, or administration of staff records.

Section 3 - Policy

Part A - Planning and prevention of fraud and corruption

Mandate and commitment

(9) Charles Sturt University has zero tolerance for fraud and corruption.

(10) The University Council acknowledges and accepts overall accountability for controlling the University's fraud and corruption risks.

(11) The University recognises that fraud and corruption can create reputational and financial damage to the University, undermine public confidence and damage staff and student productivity and morale. Fraud and corruption are incompatible with the values of the University and present a risk to the achievement of our objectives and provision of our services to all our stakeholders.

(12) The University recognises that the risk of fraud and corruption can arise in various contexts and will put in place measures proportionate to the risks it faces in order that staff, students and associates of the University and its controlled entities are aware and understand the relevant policies and procedures for the prevention, detection and response to fraud and corruption.

(13) To demonstrate this commitment the University, through the Vice-Chancellor and Vice-Chancellor's Leadership Team, will ensure:

a. the integration of fraud and corruption risk management into the University's values, practices and business plans,
b. that the risk of fraud and corruption is assessed and that risk assessment will be conducted:
    i. following substantive changes to the regulatory or compliance environment,

ii. following substantive changes to the mechanisms in place at the University to manage fraud and corruption risk,
iii. following detection of substantive fraud or corruption, and/or
iv. at least every two years,

c. the effectiveness of the mechanisms to control fraud and corruption risk are evaluated,
d. the investigation of suspected fraud or corruption and take appropriate disciplinary action, which may include referral to the relevant police service, of any person found to have engaged in fraud or corruption,
e. the reporting of suspected corruption, whether it involves a staff member of the University or not, to the relevant anti-corruption agency where required by law,
f. in the absence of criminal prosecution, the application of appropriate civil, administrative or disciplinary penalties against individuals who have been party to fraud or corruption,
g. the taking of reasonable legal action to recover losses that result from fraudulent or corrupt conduct,
h. cooperation with agencies including the ICAC, the NSW Ombudsman, Audit Office of NSW and NSW Police Force (or the equivalent agency/ies in another state or territory as applicable) in relation to fraud and corruption and wherever practical, the alignment of University processes to better practice advice issued by those organisations,
i. the recording of all suspected incidents of fraud and corruption to identify trends and prevent recurrence,
j. the reporting of actual and suspected fraud and corruption to the Vice-Chancellor and the Audit and Risk Committee, and
k. the due consideration of a fidelity guarantee insurance policy to protect the University against the financial consequences of fraud.

Framework of ethical conduct

(14) This policy is one element of a suite of practices in place across the University that reinforce the University's values. These values aim to guide our behaviour and way of working to help us achieve our ethos of respectfully knowing how to live well in a world worth living in.

(15) The University's framework of ethical conduct includes but is not limited to:

a. the University's statements of ethos and values,
b. Code of Conduct, Conflict of Interest Procedure, the Gifts Guidelines - Receipt by Staff and other University policies and procedures specifically intended to guide positive behaviour,
c. Student Charter,
d. the mandate and commitment to fraud and corruption control made in this policy,
e. example setting by senior management,
f. roles and responsibilities as articulated in University policies and procedures, including the Staff Generic Responsibilities Policy and the Delegations and Authorisations Policy,
g. mechanisms for reporting and managing wrongdoing and misconduct,
h. complaints management processes, and
i. mechanisms to ensure ethical standards in research and academic integrity.

(16) Supporting the University's commitment to an observable ethical culture, all staff are required to confirm in writing, annually, that they have over the previous twelve months complied with the University's Code of Conduct and this Fraud and Corruption Control Policy and that they will so comply over the ensuing twelve months.

Chief Security Officer is the fraud control officer

(17) The University recognises the Chief Security Officer as its primary fraud control officer. In relation to fraud and

corruption matters, the Chief Security Officer is responsible for:

a. developing, implementing and maintaining the University's FCCS,
b. coordinating periodic assessment of the University's fraud and corruption risks,
c. recording fraud and corruption events,
d. escalating and monitoring fraud and corruption events including coordinating internal and external reporting, and
e. conducting, coordinating or monitoring investigations into allegations of fraud and corruption.

(18) While not limiting the capacity of any person to report matters of concern to any person or agency, the Chief Security Officer is the nominated position authorised to make official reports to external agencies as a representative of the University with the exception of:

a. the Vice-Chancellor, as the principal officer of the University, who has a non-delegable duty to report to the ICAC as soon as they become aware of any matter that they suspect concerns or may concern corrupt conduct.

(19) The Chief Security Officer is to attend continuing professional development in order to maintain a sound understanding of methods for managing the risk of fraud and corruption in accordance with relevant standards and contemporary and emerging practice in the field.

(20) The Chief Security Officer is responsible for ensuring that all of the University's fraud and corruption control resources are coordinated and work together to fulfill the objectives of this policy.

Director, IT Infrastructure and Security is the information security management system officer

(21) The University recognises the Director, IT Infrastructure and Security (DIIS) as the information security management system officer. The DIIS is responsible for:

a. establishing and maintaining a sound understanding of the University's fraud and corruption exposures,
b. attending continuing professional development in technology-enabled fraud and corruption in order to maintain a sound understanding of methods for managing the risk of fraud and corruption in accordance with relevant standards and contemporary and emerging practice in the field,
c. maintaining a sound understanding of how an information security management system can effectively mitigate the risks of fraud and corruption, and
d. maintaining a sound understanding of cybercrime and methods for managing the risk of cybercrime in accordance with relevant standards and contemporary and emerging practice in the field.

Prevention systems

(22) The University is committed to preventing fraud and corruption within the University and its controlled entities. To this end, the University will put in place appropriate mechanisms for fraud and corruption risk management, including policies and procedures, risk assessment, internal controls, investigation, reporting, education and independent auditing to reduce the incidence of fraud and corruption and regularly evaluate these for effectiveness.

(23) The University will minimise the incidence of fraud and corruption by:

a. the application of competent risk management practice,
b. making all relevant employees aware of the University's Code of Conduct, conflict of interest declaration protocols and other elements of the University's framework of ethical conduct at induction and throughout employment,

c. the establishment and implementation of processes for all students to be made aware of the University's Student Charter and other elements of the University's framework of ethical conduct at admission and throughout enrolment,
d. the establishment and implementation of management accountabilities, including:
    i. the incorporation of fraud and corruption control into the performance management system, and
    ii. allocating any losses due to fraud and corruption to the cost centre in which the loss occurred,
e. the establishment and implementation of first line assurance business practices for preventing fraud and corruption that are:
    i. developed in all relevant areas of the University where there is a risk of fraudulent or corrupt activities,
    ii. identified as required by assessment of the risk of fraud or corruption,
    iii. documented and include requirements to create records of performance of the process,
    iv. approved by a manager of sufficient skill, competence and accountability to validate the business process will be effective in the prevention of fraud and corruption, and
    v. periodically subject to informal and formal audit,
f. the inclusion of fraud and corruption control responsibilities for managers and all members of staff in the Staff Generic Responsibilities Policy,
g. the establishment and implementation of a program for the communication of awareness in relation to the risk of fraud and corruption, and
h. the establishment and implementation of processes for:
    i. employment screening and relevant employee declarations,
    ii. the vetting of business associates,
    iii. the vetting of education agents, intermediaries and partners,
    iv. vetting of student academic capability,
    v. the protection of academic and research integrity,
    vi. the protection of intellectual property,
    vii. the protection of the integrity of certification documentation, and
    viii. the protection of any personal information collected by the University.

Fraud and corruption risk assessment

(24) The Chief Security Officer will coordinate an annual program of fraud and corruption risk management activities across the University:

a. The program will be submitted to the Audit and Risk Committee for endorsement.
b. The program will be developed using a risk based approach to address the areas of greatest risk exposure first as determined through application of risk assessment methodologies identified in the Risk Management Policy and Risk Management Procedure.
c. The scope of the program will be continuously improved having regard to:
    i. risk reviews undertaken by the Risk and Compliance Unit,
    ii. the records of risk exposure in the University's risk register,
    iii. the historical incidence of fraudulent or corrupt incidents,
    iv. guidance material incorporated in AS 8001:2021, and
    v. external environment scanning including the global, national and higher education sectors generally.

(25) The Chief Security Officer will use the findings of the fraud and corruption risk assessments to develop a fraud and corruption control assurance management plan to be reported annually to the Audit and Risk Committee and monitored for effectiveness over time.

Communication and awareness of fraud and corruption

(26) The Chief Security Officer will coordinate a regular program of communication and awareness to inform all stakeholders impacted by this policy of:

a. the University's definition of behaviours that constitute fraud or corruption,
b. the University's unequivocal zero tolerance position for fraud and corruption,
c. the general incidence of fraud and corruption,
d. fraud and corruption exposures in the higher education sector,
e. the assessed fraud and corruption exposures within the University,
f. the types of fraud and corruption that have been identified at Charles Sturt University in the previous five years and how these were dealt with in terms of disciplinary action and internal control enhancements,
g. the expectations of management and staff if fraud or corruption is detected or suspected,
h. fraud and corruption reporting processes for management and staff including the University's policy for Whistleblowing (Reporting Wrongdoing),
i. an overview of the University's FCCS,
j. an overview of the resources allocated to fraud and corruption control, and
k. an overview of fraud and corruption red flag behaviours.

Employment screening and employee declarations

(27) The Executive Director, People and Culture will develop, implement and coordinate an employment screening program consistent with contemporary human resources practice, relevant legislation, codes and standards. The employment screening program should apply to appointments of:

a. senior executives, and
b. positions where the University faces an exposure to fraud and corruption above that of the level from general academic and professional/general staff.

(28) The program will provide for effective employment screening of relevant persons:

a. before appointment,
b. on promotion or change of employment circumstances,
c. on temporary transfer to an acting role of more than 12 weeks duration, and
d. at recurring intervals of not more than three years.

(29) The Executive Director, People and Culture will develop, implement and coordinate business processes for the declaration of outside professional activities.

(30) The Executive Director, People and Culture will develop, implement and coordinate business processes for the declaration of conflicts of interest.

Business associate vetting

(31) The Chief Financial Officer will develop, implement and coordinate a process for the vetting of business associates (suppliers):

a. The vetting process must be applied to all business associates with whom the University has an annual threshold value spend of $150,000 or more.
b. The vetting process may be applied to other business associates, subject to resource availability to undertake

the vetting.

c. The vetting process is to be repeated annually for all relevant business associates.

(32) The vetting process is to include but is not limited to the following:

a. Search of company register.
b. ABN and bank account confirmation.
c. Verification of the personal details of directors.
d. Director bankruptcy search.
e. Disqualified director search.
f. Educational qualifications claimed.
g. Assessment of credit rating.
h. Search of legal proceedings pending and judgements entered.
i. Telephone listing verification.
j. Trading address verification.
k. Media search.
l. Search of available debarment, sanction and watch-lists.
m. Search for politically exposed persons.

(33) Vetting is to be undertaken prior to the award of contracts exceeding the threshold value and at such time that the University becomes aware that expenditure with a specific supplier has exceeded the annual threshold value.

(34) Adverse outcomes in relation to vetting are to be reported to the Chief Operating Officer for consideration of the University's ongoing commercial relationship with the business associate.

Preventing technology-enabled fraud

(35) The Director, IT Infrastructure and Security (DIIS) is to implement an information security management system consistent with relevant standards and contemporary practice.

Physical security and asset management

(36) The Chief Security Officer is to maintain oversight of the University's practices for the physical security and asset management. The security of the physical environment is to be assessed in order to ensure appropriate measures are put in place for the prevention of theft of valuable tangible assets. These measures should include but are not limited to consideration of the following:

a. Perimeter security
b. Access and egress controls
c. Access code / password
d. Locks
e. Gates
f. Fences
g. Alarms
h. Video surveillance

Education agent, intermediary and partner vetting

(37) Refer to the International Education Agent Policy and the University Partnerships Policy.

Student capability vetting

(38) The University undertakes pre-admission vetting on all potential students applying for enrolment in a coursework or research course in accordance with the Admissions Policy and Admissions Procedure.

(39) Where the University outsources pre-admission vetting to a third party, the Division of Students is to ensure that vetting occurs to an equivalent or better standard to that undertaken by the University.

(40) Verification of identification occurs at point of issuing a student identification card (Charles Sturt Card) in accordance with the Enrolment Policy and Enrolment Procedure.

Protection of academic and research integrity

(41) Refer to the Academic Integrity Policy and the Research Policy which set out the requirements for the protection of academic and research integrity.

Protection of intellectual property

(42) Refer to the Intellectual Property Policy which sets out the requirements for the protection of intellectual property.

Protection of certification documentation

(43) The University Secretary will ensure the development, implementation and coordination of business practices to protect the integrity of certification documentation.

(44) These business practices must ensure all certification documentation issued by the University is:

a. unambiguously issued by Charles Sturt University,
b. readily distinguishable from other certification documents issued by the University,
c. protected against fraudulent issue, including implementing practices to:
    i. secure and account for paper stocks used in the production of certification documentation, and
    ii. ensure the storage of electronic records of certification documentation in accordance with the University's requirements for records management,
d. traceable and authenticable,
e. designed to prevent unauthorised reproduction, and
f. replaceable only through an authorised and verifiable process.

Privacy management

(45) The University Secretary will ensure the development, implementation and coordination of business practices to protect the integrity of personal information.

(46) These business practices must ensure all personal information is compliant with:

a. relevant statutory and regulatory requirements, and
b. the information protection principles (IPP) applying to NSW public sector agencies.

(47) These business practices will also have consideration of the Australian Privacy Principles and best practice in the sector.

Internal audit

(48) Internal audit supports the prevention of fraud and corruption by:

a. evaluating the effectiveness of internal controls in mitigating the risk of fraud and corruption,
b. developing a risk-based internal audit program that considers the risk of fraud and corruption in line with the Internal Audit Charter, and
c. periodically reviewing the effectiveness of the University's fraud and corruption prevention framework, including this policy.

Part B - Detection of fraud and corruption

Detection systems

(49) In the event that the mechanisms in place at the University fail to prevent fraud and corruption, the University is committed to the establishment of robust systems of detection. The Chief Security Officer, as the University's primary fraud control officer, has the responsibility to ensure and validate the development of systems to detect and investigate fraud and corruption. As a minimum, these processes will include post transactional review, data mining and analysis of management accounting reports.

Post-transactional reviews

(50) A random selection of transactions will be reviewed, after processing, by personnel unconnected with the business unit making the transaction. Transactions to be reviewed include any action where a fraudulent or corrupt gain or loss is possible and includes:

a. financial transactions,
b. student administration transactions,
c. transactions related to the production of certification documentation,
d. staff administration transactions,
e. recruitment and selection transactions,
f. tender selection and procurement transactions, and/or
g. any other area of transaction at the reasonable discretion of the Chief Security Officer.

(51) The transaction reviews will look to ensure:

a. relevant documentation relating to the transactions is available and complete, and
b. transaction authorisations are properly made and recorded.

Data analytics

(52) Processes for data analysis will be developed to consider the relevant indicators of the University's fraud and corruption exposures. Data analysis is to be used to identify suspect transactions with particular consideration of false or fictitious invoicing.

Analysis of accounting reports

(53) Processes for the analysis of accounting reports will be developed to identify trends that may be indicative of fraud or corrupt conduct. Such analysis may include:

a. monthly actual/budget comparison reports at account code level,
b. reports comparing expenditure against industry benchmarks, or
c. reports highlighting unusual trends in bad or doubtful debts.

Student related fraud and corruption detection systems

(54) Refer to relevant policies such as Admissions Policy, Enrolment Policy, Student Misconduct Rule, Academic Integrity Policy, Research Misconduct Procedure, Assessment Policy, Credit Policy, or Research Policy.

External audit

(55) The University will have the Audit Office of NSW validate the annual financial statements.

(56) The University will participate in audits by the Audit Office of NSW annually and as otherwise required.

Part C - Response to fraud and corruption

Reporting fraud and corruption

(57) Fraud and corruption, and other wrongdoing, can be reported as set out in the Whistleblowing (Reporting Wrongdoing) Policy. The University encourages all members of the University community to report reasonable suspicions of wrongdoing in relation to the University.

Complaint management

(58) The University's complaints management processes are to ensure that relevant staff receiving complaints, including frontline and communications staff, are trained in recognising complaints about fraud and corruption and the subsequent internal and external reporting processes that are available.

Exit interviews

(59) The University's exit interview process is to seek to identify any knowledge or reasonable suspicion the exiting employee has of potentially fraudulent or corrupt conduct. The scope of the enquiry is to include the conduct of:

a. the exiting employee themself,
b. other persons internal to the University, and
c. persons internal to the University's business associates.

Investigation of fraud and corruption

(60) Where a report of wrongdoing is made to an authorised disclosure officer as set out in the Whistleblowing (Reporting Wrongdoing) Policy, the report will be managed and investigated as stated in the Whistleblowing (Reporting Wrongdoing) Procedure.

Responses to privacy concerns

(61) Where a person expresses a concern regarding their personal information held by the University, these concerns will be responded to in accordance with the University's Privacy Management Plan.

Breach of policy

(62) The University may commence applicable disciplinary procedures if a person to whom this policy applies breaches this policy (or any related procedures), which may include referral to the police. A breach of this policy may also be a breach of other University policies, such as the Code of Conduct.

(63) The University may consider breaches of this policy serious misconduct and grounds for termination of employment, in accordance with the relevant enterprise agreement and/or employment contract.

Section 4 - Procedures

(64) Nil.

Section 5 - Guidelines

(65) Nil.

Status and Details

Status	Current
Effective Date	15th September 2021
Review Date	15th September 2023
Approval Authority	University Council
Approval Date	15th September 2021
Expiry Date	Not Applicable
Unit Head	Kim Broadley Director, Risk and Compliance 34988
Author	Elizabeth Harangozo Risk Adviser +19356
Enquiries Contact	Elizabeth Harangozo Risk Adviser +19356