Countering Foreign Interference Procedure

Section 1 - Purpose

(1) This procedure sets out the approach of Charles Sturt University (the University) to its management of risks related to foreign interference.

Scope

(2) This procedure applies to all staff, students, customers, volunteers, contractors, business associates, partners, and third party service providers of the University and its controlled entities and in relation to both formal and informal interactions.

Section 2 - Policy

(3) This procedure supports the Research Policy.

Section 3 - Procedure

Managing foreign interference risks and issues

(4) Interactions with foreign individuals, groups or entities (foreign interactions) are an important part of the University's 2030 strategy and integral to the success of its teaching, learning and research activities. These foreign interactions must be managed to limit the risk of foreign interference.

(5) Foreign interference means activities that are conducted by, or on behalf of a foreign actor, which are coercive, covert, deceptive or corrupting and are contrary to Australia’s sovereignty, values and national interests (foreign interference). Foreign interference can occur though the following:

a. Efforts to direct the University's research agenda through funding arrangements for the benefit of a foreign political, religious or social agenda.
b. Solicitation and recruitment of staff and students to further the interests of foreign actors through various forms of inducements such as collaborations, donations, gifts and payments.
c. Bullying and harassment of individuals by foreign actors resulting in a culture of self-censoring and impacting academic freedom and contrary to the values of the University.
d. Improper attempts to obtain information from staff and students whilst travelling overseas or attending seminars and conferences.
e. Unauthorised access to University information through cybersecurity attacks.

Governance and risk management framework

(6) Risks of foreign interference include the following:

a. Damage to the reputation of the University, its teaching and research teams, and individual staff and students.

b. Loss of future partnerships and collaborations or opportunities to attract talent.
c. Compromised or unauthorised access to valuable university research, sensitive or personal data.
d. Loss of intellectual property and commercialisation opportunities.
e. Breach of legal and legislative obligations.
f. Foreign governments gaining an undue commercial, technical or intellectual advantage to the disadvantage of the University.
g. Bullying and harassment of staff and students.

(7) The University manages foreign interference risks and legislative compliance obligations by ensuring foreign interference risk management is integrated into the University's governance frameworks, policies and procedures, and control environment.

(8) A key element of managing foreign interference risk is maintaining an appropriate cybersecurity and physical security posture and strategy to support continuous improvement in risk mitigation in an ever changing threat landscape.

(9) This procedure must be considered in conjunction with the following University policies and procedures:

a. University Partnerships Policy and University Partnerships Procedure
b. Admissions Procedure
c. Information Technology Policy
d. Risk Management Policy
e. Legal Policy
f. Philanthropic Donations and Gifts Received Policy
g. Compliance Management Procedure
h. Defence Trade Controls Procedure
i. Travel Policy
j. Facilities and Premises Procedure - Access, Use and Security.

Awareness and training

(10) The Office of Governance and Corporate Administration (OGCA) is responsible for building awareness and delivering training to staff and students who engage with foreign actors and are at higher risk of foreign interference.

(11) Training will support staff and students understanding of their responsibilities, the identification of foreign interference risks and the types of matters that must be escalated.

(12) The University's Legislative Compliance Guide supports staff understanding of their responsibilities and includes the key legislative and compliance requirements relevant to the University. Each legislative instrument, including those relevant to foreign interference, are assigned to an Executive Leadership Team (ELT) member and each underlying obligation is assigned to a corresponding responsible manager, to drive accountability and awareness of day-to-day ownership of compliance. The OGCA performs an annual attestation process, whereby each responsible manager confirms accountability for managing compliance and that no material breaches or impediments to compliance have been identified.

(13) The University's participation in sector-wide countering foreign interference events, including the University Foreign Interference Taskforce, supports our awareness of emerging threats and experiences of foreign interference.

Due diligence and risk assessment

(14) In line with the University Partnerships Policy and University Partnerships Procedure, the portfolio and individual

staff initiating activity with foreign actors must ensure appropriate vetting and due diligence is performed and documented, prior to entering into contractual arrangements.

(15) For partnerships involving international agreements, the Office of Global Engagement must be consulted to determine whether the proposed engagement is required to be notified to the Minister for Foreign Affairs.

(16) In addition to requirements from the policies and procedures outlined in clause (9) above, minimum due diligence activities to support the identification and assessment of foreign interference risks include checks on the following:

a. The citizenship of individuals and whether the corresponding country is subject to sanctions by the Australian Government.
b. Ownership structure, controlling interests, board members and directors, and management of organisations.
c. Understanding and reviewing business registration.
d. Positive regulatory and legal history.
e. Issues pertaining to intellectual property rights.
f. Cyber and information security control environment.
g. Where relevant, consideration of the potential uses of any technology and research, including dual use technologies and whether the technology/research is captured within Australia's Defence Strategic Goods List and therefore regulated for physical export or electronic supply beyond Australia.

(17) Based on due diligence performed, staff must assess the proposed activity for the risk of foreign interference. Indications where the risk of foreign interference may be heightened include the following:

a. A lack of transparency and openness from the proposed partner.
b. Foreign actors being ultimately owned or associated with an overseas jurisdiction subject to sanctions and limited democracy, freedom of speech, and respect for intellectual property rights.
c. A lack of legal recourse if the University's research or data is stolen.
d. Foreign actors have limited institutional autonomy and independent decision making from their foreign government.
e. Activity involves research associated with the Australian Government, sensitive research, dual use technologies, critical and emerging technologies, or valuable intellectual property.

(18) Where there is a heightened risk of foreign interference, the proposed activity must be escalated to the Director, Security and Resilience (CSO), National Security Compliance Committee (NSCC) and Deputy Vice-Chancellor (Research), prior to commencement.

(19) Due diligence may need to be re-performed in the event of a significant change to the activity, for example, a change in ultimate ownership of the partner or in the nature of research being undertaken. Where appropriate, an update on the significant change may be required to be submitted to the CSO, National Security Compliance Committee and Deputy Vice-Chancellor (Research).

(20) Staff and students, and the corresponding supervisors, must consider foreign interference risks when travelling on behalf of the University. In line with the University's Travel Policy, staff and students travelling internationally are required to complete a risk assessment, provided by Travel and Expense. Prior to travelling to higher risk overseas jurisdictions, a security briefing must be obtained from the University's Director, Security and Resilience (CSO).

(21) The OGCA also performs an annual risk control self-assessment (RCSA), which includes consideration of foreign interference risks and the effectiveness of mitigating controls. Where controls are assessed as ineffective or requiring improvement, corrective action plans are developed to address the gap or deficiency.

Escalation and reporting

(22) Potential or actual instances of foreign interference must be immediately reported to the University's Director, Security and Resilience (CSO) (CSO) for investigation. Examples of when staff and students must escalate potential or actual instances of foreign interference include the following:

a. Gifts, donations, preferential access to senior officials or businesspeople located in Australia or overseas, expenses-paid travel etc., designed to influence staff and students.
b. Threatening behaviour from foreign actors including bullying, harassment and exploitation of staff and students.
c. Higher risk foreign actors engaging with the University on campus locations.
d. Cybersecurity incidents, data breaches and lost information technology equipment whilst at conferences or travelling overseas.

(23) The CSO will recommend to the Deputy Vice-Chancellor (Research) whether the potential/actual foreign interference issue is reportable to external agencies, such as the Australian Security Intelligence Organisation (ASIO). In consultation with the Vice-Chancellor, the Deputy Vice-Chancellor (Research) will approve external reporting of potential/actual foreign interference to external agencies.

(24) The Vice-Chancellor, in consultation with the University Secretary, will determine if reporting of a foreign interference issue to TEQSA or other relevant government department or another regulator is required.

(25) The National Security Compliance Committee will provide regular reporting to the Audit and Risk Committee on emerging foreign interference risks and potential and/or actual identified instances of foreign interference.

Roles and responsibilities

Office or body	Authorities and responsibilities
Deputy Vice-Chancellor (Research)	1. Overall executive leadership responsibility for managing foreign interference risk to the University. 2. Ensure key foreign interference risks and compliance issues are reported to the Executive Leadership Team (ELT) and Audit and Risk Committee in a timely manner. 3. In consultation with the Vice-Chancellor, approve external reporting of potential or confirmed instances of foreign interference to external agencies.
Office of Governance and Corporate Administration	1. Develop and implement staff foreign interference awareness training. 2. Maintain currency of the legislative compliance guide and Charles Sturt University obligations with regards to foreign interactions. 3. Ensure key foreign interference risks and mitigating strategies are identified and included in the University's Risk Control Self-Assessment (RCSA) risk registers. 4. Provide guidance on third party risk management, including due diligence requirements on third parties subject to increased risks of foreign interference. 5. Ensure assurance activities on the management of foreign interference risks are included in the University's enterprise assurance plan.
Director, Security and Resilience (CSO)	1. Investigate potential and actual instances of foreign interference. 2. Record, escalate and make recommendations to the Deputy Vice-Chancellor (Research) on risks, compliance issues, and required reporting to external agencies such as the Australian Security Intelligence Organisation (ASIO). 3. Undertake recording and external reporting of potential and actual instances of foreign interference subsequent to approval from the Deputy Vice-Chancellor (Research). 4. Support the risk assessment and due diligence process on activities considered at higher risk of foreign interference. 5. Maintain a register of higher risk overseas jurisdictions, as determined by the Australian Government, where there is increased risk to staff and students from foreign actors and increased likelihood of foreign interference occurring. 6. Provide regular reporting to the National Security Compliance Committee to support ongoing reporting to the Audit and Risk Committee.

Division of Information Technology	1. Ensure the University's information and cyber security framework, governance reporting, and operational controls supports the management of foreign interference risks. 2. Escalate and report information and cyber security risks and incidents to the Executive Leadership Team and Audit and Risk Committee on a timely basis.
National Security Compliance Committee	1. Consider security and foreign interference risks and issues associated with Australian government and sensitive research, dual use technologies, or valuable intellectual property. 2. Maintain record of all Australian Government, sensitive, and dual use technologies, and valuable intellectual property. 3. Provide governance reporting through to the Audit and Risk Committee on foreign interference risks, issues, and mitigating strategies where relevant.
Office of Global Engagement	1. In line with the University Partnerships Procedure, the Office of Global Engagement determine whether proposed foreign arrangements are required to be notified to the Minister for Foreign Affairs, via the online portal.
All staff	1. Any staff engaging in any activity or partnership on behalf of or with a foreign actor as part of their University business must evaluate the proposed activity or partnership for the risk of foreign interference, foreign influence and/or statutory reporting or regulatory obligations. 2. Engage Legal Services prior to entering into any contractual arrangements. 3. In accordance with the University's Conflict of Interest Procedure, declare any actual, potential or perceived conflict of interests associated with foreign actors. 4. Promptly escalate risks and potential and/or actual instances of foreign interference to their manager and the Director, Security and Resilience (CSO). 5. Notify the Division of Information Technology immediately whenever cybersecurity threats are identified or suspected. 6. Comply with required processes regarding travel briefings and debriefings in line with the University's Travel Policy. International travel must comply with the University's Travel Policy and travel to higher risk overseas jurisdictions must be subject to prior consultation with the Director, Security and Resilience (CSO) and the University's global assistance provider.

Section 4 - Guidelines

(26) Nil.

Section 5 - Glossary

(27) For the purpose of this procedure, the following terms have the definitions stated:

a. Dual use technologies – means technologies that may be used for both civilian and military purposes.
b. Foreign actor – means a foreign national, a foreign country, a foreign university without institutional autonomy, a foreign government, a department, agency or entity of a foreign government.
c. Foreign arrangement – means proposed or existing written arrangements, agreements, contracts, understandings, proposals or undertakings between Australian entities (including public universities) and foreign entities (including their government, agencies, departments and universities, unless autonomous). They may be legally-binding or not legally-binding.
d. Foreign influence – means activities of foreign governments to influence deliberations on issues of importance to them, and which, when conducted in an open and transparent manner, are a normal aspect of international relations and diplomacy and can contribute to the public debate.
e. Foreign interactions – means collectively foreign influence, foreign arrangements and foreign interference.
f. Foreign national – means a person from a foreign entity, including an embassy or foreign government official, or a trade or business representative.

Status and Details

Status	Historic
Effective Date	21st March 2023
Review Date	21st March 2026
Approval Authority	Deputy Vice-Chancellor (Research)
Approval Date	21st March 2023
Expiry Date	28th January 2025
Unit Head	Neena Mitter Deputy Vice-Chancellor (Research)
Author	Dugald Hope Director, Risk and Compliance
Enquiries Contact	Office of the Deputy Vice-Chancellor and Vice-President (Research) +61 2 6933 4237