# Cybersecurity and Foreign Interference Policy

1. **Purpose**

The purpose of this Cybersecurity and Foreign Interference Policy ("policy') is to protect the Institution's community, systems, scholarship and intellectual property from cybersecurity threats and foreign interference. It ensures the integrity of teaching and the administration while complying with Australian laws and the Guidelines to Counter Foreign Interference in the Australian University Sector. The Institution is committed to identifying, managing, reporting and reducing risks through strong accountability, effective risk management, staff and student awareness, and clear governance and reporting to TEQSA and other relevant bodies. This policy supports TEQSA's requirement for providers to demonstrate how they safeguard their Institution in this context.

2. **Scope**

This policy applies to all staff, students, contractors, and affiliates of the Institution who access, manage, or use the Institution's information, data, systems, or are involved in international collaborations or activities with foreign entities.

3. **Definitions**

See *Glossary of Terms*.

4. **Policy statements**

4.1 The Institution adopts a whole-of-organisation approach to identifying, reporting and mitigating cybersecurity and foreign interference risks, complying with all relevant legislation.

4.2 Information systems and records are maintained securely and confidentially to prevent unauthorised access or fraudulent activities.

4.3 Cybersecurity and foreign interference risks are incorporated into risk management and governance frameworks and are regularly reviewed to reduce

exposure to foreign interference.

4.4 All international collaborations, partnerships, and foreign engagements undergo appropriate due diligence and risk assessments to identify cybersecurity and foreign interference threats.

4.5 Staff complete regular training on safety and security online, reporting responsibilities and secure information handling to support a culture of cybersecurity awareness.

4.6 The Institution maintains robust critical incident detection, response and recovery procedures for managing cybersecurity and foreign interference events. These are reviewed regularly to ensure they remain fit for purpose.

4.7 The Institution ensures timely reporting of foreign interference risks and incidents to the Executive Management Group (EMG) and relevant regulatory bodies (e.g. TEQSA) and external agencies (ASIO).

4.8 The Institution engages with external stakeholders, such as regulatory bodies and industry partners, to enhance the Institution's resilience against cybersecurity threats and foreign interference.

## 5. Roles and responsibilities

5.1 The Chief Information Officer (CIO) is the responsible officer for this policy and is responsible for:

- developing, implementing and monitoring cybersecurity controls;
- conducting risk assessments;
- managing incidents;
- integrating foreign interference risks into IT security and business continuity plans;
- reporting risks and interference to the EMG, Audit, Risk and Compliance Committee and Board of Directors.

5.2 The EMG ensures international collaborations comply with the policy and conduct due diligence on foreign partnerships.

5.3 Staff are required to complete awareness training, follow policy requirements, and promptly report any cybersecurity or foreign interference

incidents.

## 6. Related documents

*Business Continuity Policy*

*Business Continuity Procedures*

*Critical Incident Policy*

*Critical Incident Management Procedures*

*Risk Management Framework*

*Risk Management Policy*

## 7. Version history

| Summary of changes | Approval date | Approved by |
|---|---|---|
| New | 2 December 2025 | Board of Directors |
| | | |
| | | |
| | | |