Cyber Security Policy

Version	Approved by	Approval date	Effective date	Next full review
4.0	Vice Chancellor	18 November 2022	18 November 2022	November 2025

Policy Statement

Purpose	This policy sets out the principles for ensuring that UNSW Information Resources (UNSW Information Services and UNSW Information Assets) that hold UNSW Digital Information are appropriately protected. UNSW must ensure that: a) accountability and responsibility are allocated for the governance and management of cyber security. b) UNSW Information

3.5. The Chief Data and Insights Officer is accountable for Data and Information Governance within UNSW including the

4. Reporting cyber security events

4.1. Any person noticing a potential or actual cyber security incident must report it as soon as possible to the UNSW IT Service Centre or UNSW IT Cyber Security Team.

5. Non-compliance

5.1. Any non-compliance with the Cyber Security Risk Management Framework must be approved in accordance with the *Cyber Security Standard   Framework Exemption*, including a mandatory risk assessment and agreed compensating controls.

Accountabilities	
Responsible Officer	Vice-President, Finance & Operations
Contact Officer	Chief Information Officer

Supporting Information

Cyber security event	means an occurrence of an UNSW Information Resource state indicating a possible breach of security policy, failure of safeguards or a previously unknown situation that may be relevant to security.