Key changes to the *IT Security Policy - Information Security Management System (ISMS)*

- The policy has been renamed as the Cyber Security Policy.
- The Chief Information Officer has been delegated authority to establish UNSW-wide Cyber Security Standards and compel work, use of equipment, or an operation, ceases due to identified or perceived cyber security risk (or a major incident).
- The Chief Information Security Officer has explicit UNSW-wide authority and accountabilities in supporting UNSW management in identification, assessment, treatment, and reporting of cyber security risks.
- Deans, Head of Schools, Heads of Research Centres, and Heads of Administrative Units are accountable to attest annually to compliance with the Cyber Security Policy Framework within their area of accountability.
- Business Owners are accountable for determining risk rating of their Information Resources, and ensuring appropriate controls are implemented.

Key changes to the current *Acceptable Use of UNSW Information Resources Policy*

- The policy has been renamed as the Acceptable Use of UNSW Information Resources Policy.
- Additional detail is provided relating to what user actions, materials or devices are not permitted.
- Misuse is defined, and its consequences are outlined.
- Approval requirements governing privacy and access to information resources have been simplified.

Key changes to the current *IT Security Standards*

- IT Security Standards have been renamed as Cyber Security Standards.
- The *Cyber Security Standard – Risk Management* has been documented to provide guidance on determining a risk rating for information resources, and mandatory controls that must be implemented to protect information resources with low, medium and high risk ratings.