UNSW Australia - Information Security Mission Statement

Purpose

- UNSW values the use of Information Technology in supporting the University's goals and objectives, our academic services gain strength and currency from research activities, strong industry links and international presence.

- UNSW has strong engagements and partnerships with local and global communities allowing it to share knowledge, debate and research outcomes.
  - In this context; UNSW’s information, whether managed and residing on UNSW resources or held in trust and managed by third parties or business partners is considered an important asset that must be protected. Any person or organisation that uses or holds in trust these assets has a responsibility to maintain and safeguard them.

- UNSW is committed to preserving the confidentiality, integrity, and availability of information regardless of the form it takes: electronic or non-electronic. Improper use of information resources may result in harm to the University and its teaching, research and international outreach undertakings.

Aim

- This statement presents the philosophy of information security within UNSW and represents the endorsement of the UNSW Executive Team. It identifies the motivation for information security management and defines the scope of information security responsibilities throughout the University.

- UNSW aims to safeguard its local and international reputation as an academic institution by protecting its information and Information Technology assets from unauthorised disclosure, use, modification or loss.

- It is one of the UNSW’s primary objectives to develop proactive technical and non-technical measures to help identify and prevent Information Security risks and provide an effective response in cases where those measures fail.

Responsibility

- The Information Security Steering Group (ISSG) is responsible for all aspects of Information Security governance as defined by the Information Security Management System.

- UNSW takes direction from the Business Reporting and Intelligence and Data Governance team who provide identification, classification, stewardship and maintenance of University wide information.

- UNSW Australia Divisions and Faculties are responsible for the protection of their information. UNSW Divisions and Faculties; decide levels of risk, provide adequate resources, enforce the IT Security Policy and related Security Standards in their respective areas.

Scope

This Statement establishes the expectations for all users of UNSW Australia ICT resources – including (but not limited to) staff (including casuals), students, consultants, contractors, third parties, agency staff, alumni, associates, honoraries, conjoint appointments and visitors to the University.

Policies

UNSW IT Security Policy and a list of security-related Standards is available at https://isms.unsw.edu.au