Policy

Property and Facilities - Security Policy

1. PREAMBLE

1.1. The University is committed to ensuring a safe and secure environment for the University community and the physical assets of the institution. The University will undertake its activities in a manner whereby:

a. all members of the University community, including students and other clients, staff, visitors and contractors, are provided with a safe and secure environment in which to function;

b. precautions are taken to keep assets safe from crime, attack, misuse, or danger; and

c. there is a cohesive system of physical and logistical controls, which enable the University to maintain business continuity.

2. PURPOSE

2.1. The intention of this policy is to provide the framework for management of the University's security of people and physical assets.

3. SCOPE

3.1. This policy applies to all staff, visitors, volunteers and contractors, and students of the University.

3.2. The policy applies to all campuses, study sites and off-campus locations owned, operated, leased or run in agreement with the University.

3.3. The policy applies to University property, plant and equipment, and, as far as practicable, to property and equipment brought on campus by staff and students.

4. POLICY

4.1. This policy will be implemented in a way that ensures compliance with relevant legislation, regulations, standards, and University governing documents.

4.2. Breaches of security will be reported in accordance with legislative requirements.

4.3. Security procedures will be developed, maintained and monitored to safeguard:

a. personal security, so that individuals are protected from criminal and offensive behaviour including threats to personal safety, and damage to or loss of, personal possessions;

b. physical security, so that University and tenant property and equipment is secured against loss, deterioration or damage;

c. administrative security, including policies and procedures, incident reporting, emergency management and business continuity procedures, and threat, risk and hazard assessment, management and mitigation;

d. information security, considered under the University's Information and Communication Technologies Security Policy. and

e. security education and awareness.

4.4. The University is committed to:

a. providing appropriate resources to develop and maintain an effective approach to security;

a. achieving and demonstrating achievement of this policy through a program of audits and reporting the findings of those audits;

b. regularly reviewing the implementation and effectiveness of this policy with staff, students, other clients and stakeholders;

c. basing security arrangements on risk assessment and risk appetite, so that cost effective counter-measures can be introduced to protect the University and ensure continued viability (refer to the Enterprise Risk Management Policy);

d. developing, reviewing and promulgating University governing documents to assist in the implementation and understanding of this and other related policy; and

e. identifying competency needs and providing appropriate training and professional development for staff to meet those needs.

Specific Responsibilities and Authorities

4.5. The Director, Facilities Management is responsible for ensuring that adequate security services are in place in the University.

4.6. Deans are responsible for ensuring the Security Policy is implemented in their Colleges and for monitoring its observance.

4.7. Senior Managers are responsible for ensuring compliance with the Security Policy in local-level activities.

5. NON-COMPLIANCE

5.1. Non-compliance with Governance Documents is considered a breach of the Staff Code of Conduct or the Student Code of Conduct, as applicable, and is treated seriously by the University. Reports of concerns about non-compliance will be managed in accordance with the applicable disciplinary procedures.

5.2. All staff members have an individual responsibility to raise any suspicion, allegation or report of fraud or corruption in accordance with the Fraud and Corruption Control Governance Framework, Fraud and Corruption Control Policy and Whistleblower reporting (Improper Conduct) Procedures.

RELATED AND SUPPORTING DOCUMENTS

Legislation	AS ISO 31000:2018 Risk Management – Principles and guidelines Work Health and Safety (National Uniform Legislation) Act 2011
Policy	Information and Communication Technologies Security Policy Work, Health and Safety Policy Educational Quality and Excellence Policy Enterprise Risk Management Policy Critical Incident Policy
Procedures	Emergency Management Procedure

Definitions	CDU Glossary

GOVERNANCE

Responsible Executive	Deputy Vice-Chancellor Operations	
Implementation Officer	Director Facilities Managment	
Category	Management Policy	
Approving authority	Vice-Chancellor	
Effective date	14 October 2021	
Review date	14 October 2024	
Version	2.00	Pol - 037
Content enquiries	governance@cdu.edu.au	

DOCUMENT HISTORY AND VERSION CONTROL

Version	Date Approved	Approved by	Brief Description
1.00	4 May 2005	Council	• Creation of original document and upload to CDU website.
1.07	15 December 2017	Governance	• Conversion to new Governance template due to new University branding • Updated definitions, hyperlinks and titles
2.00	14 October 2021	Vice-Chancellor	• Complete review of Document • Updated standards and related policies