Security Policy

Section 1 - Preamble

(1) Charles Darwin University ('the University', 'CDU') is committed to ensuring a safe and secure environment for the University community and University assets. Security is a shared responsibility and is integral to the University's governance, risk management and business continuity standards.

(2) The University has the right to regulate access to University premises and to control the entry of persons and their operations within the premises.

(3) 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 protect physical and digital assets from crime, misuse, loss, damage or disruption; and
c. there is a cohesive system of proportionate, risk-based security controls, including closed-circuit television (CCTV), access control, and physical and logistical controls which enable the University to maintain business continuity.

Section 2 - Purpose

(4) This policy provides the framework for the management of the University's security of people, physical assets, and operations.

Section 3 - Scope

(5) This policy applies to

a. all staff, students, visitors, volunteers, and contractors of the University;
b. all campuses, study sites, residences, events, activities and off-campus locations owned, operated, leased or otherwise controlled or undertaken on behalf of the University;
c. University assets, including buildings, infrastructure, systems, equipment, various security surveillance technologies, such as closed-circuit television (CCTV) and access control systems, and, as far as practicable, property and equipment brought on campus by staff and students; and
d. physical access and entry into University-owned or operated spaces.

(6) It does not apply to:

a. premises managed or utilised by partner organisations; and
b. the security of University information, financial assets or reputation, or the management of emergencies and critical incidents as these matters are dealt with under other relevant University policies and procedures.

Section 4 - Policy

(7) It is the responsibility of Property and Facilities (PF) to manage security on behalf of the University in a manner that supports compliance with relevant legislation, regulatory obligations, applicable standards, and University governance documents, including the Privacy and Confidentiality Policy.

(8) Breaches of security will be reported in accordance with legislative requirements and University governance documents.

(9) Security standard operating 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 property;
b. physical security, so that University and tenant property, infrastructure and equipment are 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 about physical security, including access logs and CCTV footage, and cybersecurity of that information, in alignment with the Information Security and Access Policy; and
e. security awareness education and training.

(10) The University is committed to:

a. providing appropriate resources to develop and maintain an effective approach to security;
b. achieving and demonstrating achievement of this policy through a program of audits and reporting the findings of those audits;
c. regularly reviewing the implementation and effectiveness of this policy with staff, students, other clients and stakeholders;
d. 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);
e. developing, reviewing and promulgating University governance documents to assist in the implementation and understanding of this and other related policies and procedures; and
f. identifying competency needs and providing appropriate training and professional development for staff to meet those needs.

Closed-circuit Television (CCTV) and other surveillance technologies

(11) The University may use CCTV and other surveillance technologies for legitimate University purposes, including:

a. enhancing the safety and security of members of the University community and visitors;
b. protecting University assets and infrastructure;
c. deterring and detecting unlawful or unauthorised activity; and
d. supporting incident response, investigation and business continuity.

(12) CCTV and other surveillance technologies will only be used where they are necessary, proportionate, and reasonably aligned with identified security risks.

(13) Personal information collected through surveillance will be handled in accordance with the University's Privacy

and Confidentiality Policy and the Information Security and Access Policy.

(14) Access to surveillance data will be restricted to authorised personnel with a legitimate business need and will be managed in accordance with University governance documents.

(15) Surveillance data may only be used for the purposes for which it was collected, or for other lawful purposes, including investigations, safety management, or as required by law.

(16) Disclosure of surveillance data to external parties will occur only where authorised, lawful, and appropriate, including to law enforcement or regulatory authorities.

(17) Surveillance data will be protected through appropriate technical and administrative controls to prevent unauthorised access, misuse, loss or alteration.

(18) The retention and secure disposal of surveillance data will be managed in accordance with legislative requirements, records management obligations, and the Records and Information Management Policy and Procedure.

Access to University Premises

(19) Access to University premises is the responsibility of and controlled by Property and Facilities.

(20) Staff, students and other persons with a legitimate reason to access University premises may enter these premises, provided that:

a. entry has not been prohibited by any security officer or by any law or regulation; and
b. they comply with any conditions which may be applicable to their access to the University premises.

(21) All members of staff (including contract and casual staff) and students of the University are issued with CDU identification cards, which must be:

a. carried during attendance at University premises; and
b. shown in response to any reasonable request from any security officer or from any other member of staff who might require such identification in the course of their duties.

(22) Any person can be requested to leave the University premises if there is reason to believe that the person has no legitimate reason to be present, and the assistance of the Police can be sought to have that person removed if necessary.

(23) Any person who requires access to University premises outside of normal operational hours must obtain prior permission through their department or faculty.

Specific Responsibilities and Authorities

(24) The Director Property and Facilities is responsible for the coordination and operational delivery of security services across the University.

(25) Senior Executive Team (SET) members are responsible for ensuring that the Security Policy is implemented in their organisational units and for monitoring compliance.

(26) Managers are responsible for ensuring compliance with the Security Policy within their areas of responsibility.

Section 5 - Non-Compliance

(27) Non-compliance with governance documents is considered a breach of the Code of Conduct - Employees or the Code of Conduct - Students, 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 outlined in the Charles Darwin University and Union Enterprise Agreement 2025 and the Code of Conduct - Students.

(28) Complaints may be raised in accordance with the Complaints and Grievance Policy and Procedure - Employees and Complaints Policy - Students.

(29) 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 Policy and Whistleblower Reporting (Improper Conduct) Procedure.

Status and Details

Status	Current
Effective Date	24th September 2026
Review Date	24th September 2029
Approval Authority	Vice-Chancellor
Approval Date	14th September 2026
Expiry Date	Not Applicable
Responsible Executive	Penny Szybiak Vice-President Corporate
Implementation Officer	Anthony Hornby Director Property and Facilities
Enquiries Contact	Anthony Hornby Director Property and Facilities Property and Facilities

Glossary Terms and Definitions

"Critical Incident" - Critical Incident means an Incident that poses extreme risk to life, business continuity and / or reputation. It may also have implications at the local, state or national level. A “Critical Incident” is any actual or alleged event or situation that creates a significant risk of substantial or serious harm to the physical or mental health, safety or wellbeing to human life.

"Partner organisations" - An organisation, in conjunction with whom the University offers a program of study or a component of a program of study.

"Professional development" - Defined by the Australian Skills Quality Authority (ASQA) as activities that develop and/or maintain an individual’s skills, knowledge, expertise and other characteristics as a trainer or assessor. This includes both formal and informal activities that encompass vocational competencies, currency of industry skills and knowledge and practice of vocational training, learning and assessment, including competency based training and assessment. Examples of professional development activities include: participation in courses, workshops, seminars, conferences, or formal learning programs; participation in mentoring, professional associations or other learning networks; personal development through individual research or reading of publications or other relevant information; participation in moderation or validation activities; and participation in industry release schemes.

"Business Continuity" - Business Continuity means the planning and preparation undertaken by the University to make ensure it overcomes serious incidents or disasters and resumes its normal operations as safely and quickly as possible post incident.

"Risk" - The uncertainty associated with the delivery of the strategic goals of the University, which could result in either a positive or negative outcome.

"Risk management" - A coordinated set of components (processes, activities and methods) that are used to support and sustain risk management throughout the University. It includes all the processes involved in identifying, assessing and evaluating risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

"Organisational unit" - A faculty, centre or other academic unit; a department, or other administrative unit within

the University.

"University" - Charles Darwin University, a body corporate established under section 4 of the Charles Darwin University Act 2003. The University is comprised of the various faculties, CDU TAFE, organisational units, and formal committees, including the governing University Council and Academic Board.

"Governance document" - means policy or procedure published in the Governance Document Library. Policies and procedures are collectively called ‘governance documents’ and are often referred to as ‘policy’ or ‘University policy’.