



Policy: University Physical Security – Internal Campus Buildings and External Site Operations

Purpose

The purpose of this policy is to set principles that support the Australian National University (ANU) in providing a safe and secure working and learning environment for its staff and students.

This Policy provides a framework for the management of security and safety within buildings and throughout external spaces at ANU campuses and other ANU managed locations through the implementation of physical security controls.

The Policy will allow the University, as far as reasonably practical, to provide for the safety and security of the ANU community and the people who use the facilities by:

- * Proactively deterring crime and incidents;
- * Creating a safe environment for members of the University community to undertake work and study; and
- * Providing a responsive, effective, and efficient service to address the University's operational security needs.

Overview

The University has determined that all campuses and managed sites should be open and welcoming environments with some areas having controlled access where and when the need arises.

Security measures are implemented in accordance with the University's plans and objectives, available resources and, most importantly, in proportion to the assessed risk and threats to the University, its people, and physical assets. These threats may include vandalism, theft, intentional and accidental damage, natural disaster, violent incidents, terrorism, and other non-traditional threats.

Scope

This policy applies to all University members, including staff, students, visitors, tenants, contractors and physical university assets. This policy is not applicable to matters related

to security of research materials and access to restricted research and laboratory areas within buildings.

Policy statement

Principles

1. The University is a public institution that promotes openness and freedom. These principles are reflected in the open design of the campus, and the levels of access provided to staff, students and visitors. However, the University has an obligation to keep good order on campus, manage personal safety on campus, as well as protecting its property and academic activities. To that end, a wide range of practices has been established to enhance security on campus.
2. Specific research projects may be required to meet compliance with the principles of the Australian Government's [Protective Security Policy Framework \(PSPF\)](#) and, where applicable, [Defence Security Principles Framework \(DSPF\)](#).
3. The principles on which the policy is based include:
 - a. The University's role in providing a safe environment for staff, students and visitors.
 - b. Security is everyone's responsibility, and the University is committed to developing and fostering a positive security culture, which is critical to effective security outcomes.
 - c. The need to establish security arrangements that meet this goal without significantly compromising academic freedom.
 - d. The Facilities and Services Division's Security and Transport and ANU UniSafe teams will work in partnership with external agencies including police, fire services and other government agencies, with a high focus on threat intelligence, prevention and preparedness.
 - e. Ensuring that Deans and Directors have a formal role in assessing the risk profile for their areas whilst adhering to the University's [Risk Management Framework](#) and [Local Business Continuity Plan/s](#), as needed.
 - f. Establishing security arrangements that:

can be managed within the existing resources of the University, and respective departments; and have the right balance of central and local area controls, which capitalise on expertise and institutional knowledge.

Establishing University security arrangements

Design of buildings

4. The Director of Facilities and Services is responsible for establishing a minimum standard of security design for incorporation in all new or refurbished buildings. This includes location, building architectural features (including door and window design), electronic access, Close Circuit Television (CCTV), and mechanical locking standards. Where practical, new and refurbished buildings will apply CPTED (Crime Prevention through Environmental Designs) standards.
5. The Facilities and Services ANU UniSafe is responsible for regular internal audit of its Security Ecosystem, comprised of an intelligence driven threat management approach, coordinated emergency management system, enhanced system and infrastructure capability.

Electronic access systems

6. As part of the campus security strategy, most University areas are fitted with electronic access controls on designated entry/exit doors. A back up mechanical locking system is always installed as an alternative security measure in the event of electrical system failure. The ANU UniSafe electronic access control standards apply to all buildings.
7. Where electronic access is not fitted, the doors have appropriate mechanical locking systems and the local area management is responsible for ensuring that these doors are locked when not in use.
8. Local areas use the electronic access system identified by the University. In regard to this system, the following applies:
 - a. The Director of Facilities and Services has established specifications for the electronic system in accordance with the system standards adopted by the University.
 - b. The system is monitored by Facilities and Services (ANU UniSafe) on a 24-hours/7 days basis; and
 - c. Individual access profiles are determined by the relevant area management, in accordance with the security standards established for that building. The access is reviewed quarterly by the relevant delegated officer who keeps ANU UniSafe informed.

Access to buildings

9. University staff, contractors and students are automatically assigned limited access to campus common areas. For specific access relating to employment role or study

requirement, access will need to be requested through the relevant Dean, Director or delegated officer.

10. The responsibility for establishing security arrangements (including access arrangements) within buildings, resides with the relevant Dean, Director or delegated officer. In determining these arrangements, the delegate balances the need for security against the need to maintain access for legitimate users. To that end, the delegate is to complete a risk assessment before finalising security arrangements for their building/s. As part of this assessment, the following is identified and evaluated:

- * risks, including to personal safety, loss or damage to physical and intellectual property and disruption to operational activities.
- * the most appropriate security measures to minimise the risks.
- * The impact of security measures on access of staff and students.
- * Whether the arrangements unreasonably compromise academic freedom.
- * The impact of security measures on personal freedom (including privacy).
- * Compliance with the [Privacy Act 1988 \(Cth\)](#) and the [ANU Privacy Policy](#).
- * Specific arrangements necessary for the safety of people or animals, within research areas.
- * Staff and Student Access Afterhours: If a University staff member or Student requires access to University property outside of normal operational hours, prior permission should be sought through their local area. The local area must then notify the ANU UniSafe of the permitted access.

11. There is no simple method of balancing security arrangements and procedures against the need for academic freedom. Each case requires an assessment of all issues before arrangements are established and at each time the circumstances change. As a guide, the primary concern of the delegate in determining new security arrangements is the safety of staff, students and visitors. Further, the risk to property and academic activity is formally assessed before any measures that compromise academic freedom are implemented.

Contractors and tenants in University buildings

12. Tenants of University owned/and or controlled buildings are normally required to use the same key systems as university departments and sections. New tenants will be provided with an initial issue of keys to existing doors. Any additional keys and locks required will be provided at the tenant's expense.

13. Contractors are required to liaise with the ANU UniSafe and their project supervisor prior to being issued keys. The ANU UniSafe will determine if keys can be signed out on a temporary basis to the contractor directly or if physical custody of the keys must be maintained by the project supervisor or building custodian.
14. If a tenant or contractor loses or cannot produce a key on reasonable request, they will be liable for the total cost associated with replacing the lock/s to the area/s compromised.
15. Contractors with an ongoing relationship with the University may be issued an electronic access card. Approval must be sought from the University representative contract manager and provided to *Fix My Campus* for implementation.

Key management

16. The relevant Dean, Director or delegated officer are responsible for the management of keys within their areas. They are to ensure that:
 - * A key register is maintained and regularly checked for accuracy.
 - * Issuing of master keys is limited to essential personnel (as a guide, no more than two master keys for an area should be issued). A master key for the area is to be supplied to and held by the ANU UniSafe for extraordinary use only.
 - * Any individual to whom a university key is issued is aware of their responsibility for ensuring safekeeping. Keys are returned by staff and/or students when they are no longer required.
 - * When buildings, facilities or campuses are added to the University, the ANU UniSafe must be informed and must review and provide a recommendation of what is required to bring the physical key and lock control system of the new facility in line with University standards.

After hours contacts

17. All areas are to nominate officers as after-hours contacts in the event of emergency. Areas are responsible for ensuring an up-to-date contact list is provided electronically to Facilities and Services (ANU UniSafe) each time staff or delegation arrangements change.

Site security

18. The Director of Facilities and Services is responsible for managing security on campus grounds. As part of assessing the security requirements, the Director conducts site audits (including lighting audits) as required. The security arrangements established for the site balance the desire to maintain an open campus with the need to protect community and property. The relevant Dean,

Director or delegated officer are required to appraise themselves of the risks (potential and realised) in their area of activity. Facilities and Services, through the ANU UniSafe, can provide advice and assistance on the assessment and treatment of site security risks.

19. Facilities and Services, on behalf of the University, maintains the following services to support site security:

- a. A central security service on a 24 hours/7 days roster;
- b. Lighted pathways on designated pedestrian routes across campus;
- c. An after-hours security escort service to accompany staff and students, between buildings and to car parks on campus;
- d. The design, scope, and co-ordination of electronic access control, at any University campus or facility;
- e. Limiting access to buildings after hours, and ensuring access is provided for staff or students with valid university ID cards; and
- f. Updating after hours building access in public areas during periods of decreased traffic, including semester breaks or teaching free periods.

20. The Facilities and Services Division may introduce other measures from time to time. Any measures introduced must be consistent with University policies, as well as relevant ACT and Commonwealth legislation.

Demonstrations on campus

21. Demonstrations by ANU staff and students are permitted on campus grounds in line with this policy, the [Academic Freedom and Freedom of Speech](#) policy, the [Code of Conduct policy](#), the [Student Conduct of Conduct policy](#) and all relevant Commonwealth, ACT and University laws or regulatory guidelines.

22. Demonstrations on campus must:

- a. Be orderly, peaceful and not make other campus users feel harassed or intimidated;
- b. Not unreasonably disrupt the good order and operations of the University, including teaching, exams, events and research;
- c. Not damage University property or the property of other campus users;
- d. Not unreasonably disrupt access to and from the University premises and grounds, in particular emergency assembly points and evacuation routes;
- e. Not disrupt, limit or prevent others from going about their normal business;

- f. Comply with reasonable directions from ANU UniSafe or a delegate of the University to ensure the good order and safety of the campus users;
- g. Comply with ANU safety policies and procedures; and
- h. Comply with Australian Work Health and Safety laws.

23. ANU UniSafe is responsible for putting in place reasonable and proportionate security measures following their assessment of the risk that a campus user will become the target of demonstrators, counter demonstrators or other threats.

Sleeping on campus

24. ANU provides students and staff with spaces to study, rest, socialise, eat and reflect. Napping for a short period is permitted for students on campus, so long as the use of space is reasonable, safe and in line with this policy and other applicable ANU policies. The highest priority is student welfare in regard to this issue and the University is committed to providing:

- a. A range of support services that provide short term options of safe accommodation for students who are facing difficulties including programs through residential accommodation, including ANUSA and community support programs; and
- b. ANU UniSafe wellbeing checks on any reports of individuals napping on campus.

25. ANU acknowledges that safe sleeping arrangements are essential for wellbeing. Sleeping or living (outside of designated accommodation on university premises or affiliated colleges) on campus is not permitted. This includes sleeping in vehicles on campus, setting up beds, tents or temporary structures, the use of blankets, pillows or sleeping bags, moving furniture or other University property, or creating other living arrangements, temporary or permanent at any time of day. For clarity, this does not apply to designated accommodation on University premises or affiliated colleges.

26. Authorised ANU Staff Members or ANU UniSafe may approach campus users who are sleeping to check identification (including asking for a student ID card/staff access credentials and other forms of photo identification on request). Campus users found resting, napping or sleeping on University premises and grounds that are not ANU staff or students may be asked to leave University premises and grounds by Authorised ANU Staff Members or ANU UniSafe. This may occur to ensure the safety and security of all campus users.

27. The Director of Facilities & Services may approve exemptions to this section to enable education, research, community or fundraising events at their discretion.

The role of ANU UniSafe section

28. The University has established a central security unit within the Facilities and Services Division. The role of this area is to oversee security on site, while also monitoring internal security within buildings by use of the electronic access system, fire system, closed circuit television and building management systems.

29. Other functions of ANU UniSafe include:

- * Managing initial response to site emergencies
- * Management of the after-hours call out list for areas
- * Site patrols, including locking up of designated areas
- * After-hours management of the University switchboard
- * Conduct of security risk audits in accordance with AS4360 and the Commonwealth Protective Security Policy Framework (PSPF), where applicable.

Patrols & Escorts

30. ANU UniSafe is responsible for regular patrols of University buildings, car-parks and the surrounding grounds, taking reasonable action to regulate access and behaviour of people whilst on University premises, to maintain a safe and secure environment and undertake welfare checks.

31. ANU UniSafe provides escort services on campus to University Members and Students, requiring assistance to safely transit from their place of work or study to their vehicle or Residential Hall/Lodge. To request an escort, either activate the University's mobile application ANUOK or call ANU UniSafe.

Management of Lost Property

32. Management of lost property is the responsibility of ANU UniSafe.

33. Unattended property that appears to be abandoned or left unattended in University buildings or grounds may be treated as lost property.

34. Individuals who have lost their property may visit the ANU UniSafe Office to determine whether their item has been turned in.

35. Individuals may file a report with ANU UniSafe so that they can be contacted if their item is found.

36. If lost property has not been claimed, all items are managed in line with the [Uncollected Goods Act 1996](#).

Closed circuit television

37. The University has established Closed Circuit Television in buildings as well as in external areas across campus. The purpose of close circuit television is to monitor activities within buildings and on site, and, where appropriate, record events for subsequent investigation or reference to police.
38. University equipment will not be hidden and will be installed and operated in line with the [ANU Privacy Policy](#). Equipment is not and will not be installed in areas in which individuals have a reasonable expectation of privacy, such as toilets, parental rooms, showers and change rooms.
39. Notices (prominent signage) regarding the use of Surveillance Equipment is placed at the entrance ways leading into areas under surveillance.
40. The Director of Facilities and Services is responsible for defining the system specifications for closed circuit television and approving the installation of new systems within buildings and across campus.
41. An appropriate procedure for the use, monitoring, retention and access of footage (aligned with the *Workplace Surveillance Act 2005*, the *Workplace Privacy Act 2011*, and the *Privacy Act 1988 (Cth)* and the ANU Privacy Policy) and relevant records legislation) has been established.

Duress Alarms and Infrastructure

42. Site risk assessments may require the installation of a fixed or mobile duress button.
43. The University utilises duress alarms in areas meeting a defined criteria to allow community members to contact ANU UniSafe via silent alarm. Those areas with authorised duress alarm installations must meet the defined criteria, participate in quarterly testing, annual training, and bi-annual review of conditions resulting in the installation.
44. Local areas are responsible for providing an immediate response, as per the established risk assessment by the relevant Dean, Director, or delegated officer.

Community awareness and individual responsibility

45. The relevant Dean, Director or delegated officer are responsible for ensuring staff and students are briefed on the security requirements of their local areas.
46. Staff and students are responsible for ensuring that they do not compromise University security arrangements through any deliberate or negligent act. Any breach of security arrangements may result in disciplinary action.

47. ANU UniSafe has developed and will maintain a contemporary security awareness training module, available as mandatory to all staff at the University.
48. The University does not take responsibility for the loss or damage of personal property held on campus. Staff, students and visitors must take personal responsibility for the protection of their own property.
49. ANU UniSafe work in liaison with relevant University organisational units on security measures to support:
- a. an open, safe and welcoming environment;
 - b. reduction of incidents and the minimisation of risk;
 - c. the personal safety of individuals;
 - d. protection of premises, physical assets, including property and vehicles;
 - e. reduction of unauthorised access to secure areas of the University estate, and where necessary to take additional security measures to protect high value assets, and high-risk facilities; and
 - f. clear, regularly reviewed policies and procedures.

Incidents and Reporting

50. All security incidents which occur on University premises are reported to ANU UniSafe. It is the responsibility of ANU UniSafe to escalate these reported incidents through to the appropriate delegated authorities and determine escalation to the University's Incident Controller if the matter is deemed critical.
51. If an individual has suffered loss or damage to personal property, it is the responsibility of that individual to report the incident to ANU UniSafe. ANU UniSafe may encourage or facilitate the reporting of the incident to the police.
52. If an individual is suspected to have been engaged in criminal activity on University grounds, ANU UniSafe may take photographic or video evidence of the suspect in order to provide evidence to the police. In doing so, ANU UniSafe will abide by the mandates of the University's Privacy Policy.
53. Any physical security incidents which may have broader implications beyond the ANU UniSafe team, will be escalated through to the appropriate authority (e.g. matters pertaining to foreign interference risks).

Campus Closure/Lockdowns

54. The University may be required to either partially or completely close one or more of its facilities, in response to an emerging or current crisis.

55. ANU UniSafe may implement restrictions to University members, refusing entry and limiting electronic access (swipe) to the University facilities, as determined by the Crisis Management Team (CMT) or other University working groups or committees with the required delegated authority.
56. Lockdown is a process during which individuals on campus receive instructions to immediately protect themselves from perceived or declared threat on campus.
57. In the event of a crisis on the University grounds, the Crisis Management Team (CMT) will implement, through ANU UniSafe, an emergency lockdown of specific areas, an entire campus, or all University controlled facilities.
58. Electronic Lockout will be applied to specific areas or an entire campus, where electronic access control is fitted to buildings. This action will result in a Lockout, restricting access into or through buildings.

Document information

Title	Security - buildings and site
Document Type	Policy
Document Number	ANUP_000463
Version	
Purpose	To provide the framework for management of security on campus, both within buildings and across the site.
Audience	Staff
Category	Administrative
Topic	Buildings & Grounds
Subtopic	Security
Effective Date	3 Aug 2024
Review Date	2 Aug 2029
Responsible Officer	Chief Campus Environment Officer
Approved By	Vice-Chancellor (eo.vc@anu.edu.au)
Contact Area	Campus Environment (fs.director@anu.edu.au)
Authority	Australian National University Act 1991 Privacy Act 1988 Tertiary Education Quality and Standards Agency Act 2011 Education Services for Overseas Students Act 2000 Higher Education Standards Framework (Threshold Standards) 2021 National Code of Practice for Providers of Education and Training to Overseas Students 2018
Printed On	22 Mar 2025

Please ensure you have the latest version of this document from the Policy Library website before referencing this.