Policy: Security - buildings and site

Purpose

To provide the framework for management of security on campus, both within buildings and across the site.

Overview

The University's framework for management of security on campus, both within buildings and across the site.

Scope

This Policy applies across the University.

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 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. These arrangements include the Universitys duty of care to staff, students and others, as well as our need to protect property and operations, with the need to provide academic freedom.

2. This policy defines the overall approach to the management of site, building and personal security, and applies to all staff and students, as well as (where appropriate) third parties resident on campus. Other matters related to staff safety or security of research materials, and access to restricted research and laboratory areas within buildings are covered by other University policies and procedures. Specific research projects may be required to meet additional Commonwealth security.

3. The principles on which the policy is based include:

- The University's obligation to provide a safe environment for staff, students and visitors

- The need to establish security arrangements that meet this goal without significantly compromising academic freedom
- Ensuring that Deans and Directors have a formal role in assessing the risk profile for their areas.
- Establishing security arrangements that can be managed within the existing resources of the University, and respective departments
- Establishing security arrangements that have the right balance of central and local area controls, which capitalise on expertise and institutional knowledge

Establishing University security arrangements

4. The University has established security standards within its grounds and in buildings, that are appropriate to effectively manage personal and property risks. In doing so, the desire to maintain an open campus and facilitate academic freedom has been considered. The following sections detail responsibilities for various aspects of security management.

Design of buildings

5. The Director, 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 and mechanical locking standards. Where practical new and refurbished buildings should apply CPTED (Crime Prevention Through Environmental Designs) standards.

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 should always be installed as an alternative security measure in the event of electrical system failure.

7. Where electronic access is not fitted, the doors have appropriate mechanical locking systems and area management is responsible for ensuring that these doors are locked when not in use.

8. Areas use the electronic access system identified by the University. In regard to this system, the following applies:

- The Director, Facilities and Services, has established specifications for the electronic system in accordance with the system standards adopted by the University.

- The system is monitored by Facilities and Services (ANU Security) on a 24-hours/7 days basis.
- Individual access profiles are determined by the relevant area management, in accordance with the security standards established for that building

Access to buildings

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

- Identification of risks, including personal safety, loss or damage to physical and intellectual property, disruption to operational activities
- Identification of 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)
- Specific arrangements necessary for the safety of people or animals, within research areas.

10. 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 delegated officers in determining new security arrangements should be the safety of staff, students and visitors. Further, the risk to property and academic activity should be formally assessed before any measures that compromise academic freedom are implemented. Another matter that must be considered is whether there are areas within the building, which require broader community access, such as a library facility. If that is the case, arrangements need to be established facilitate ease of access to these areas, without compromising the security of the staff and students or the building. Similarly, buildings with higher level security arrangements should not, as a general rule, be used for meetings involving staff/students/visitors from other areas on campus

Key management

11. Deans, Directors or equivalent are responsible for the management of keys within their areas. They are to ensure:

- 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 ANU Security for extraordinary use only.
- Keys are returned by staff and/or students when they are no longer required.

After hours contacts

12. 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 Security) each time staff or delegation arrangements change.

Security risk assessments

13. The University conducts risk assessments as required, including lighting audits and internal security reviews. The responsibility for managing site assessments resides with the Director, Facilities and Services. From time to time, the University may also elect to commission external audits of campus security arrangements, including arrangements established in specific areas.

14. Where appropriate, the University area can seek the assistance of the Director, Facilities and Services, in completing a risk assessment for their area.

15. Any measures introduced must be consistent with University policies, as well as relevant ACT and Commonwealth legislation.

Site security

16. The Director, 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. Deans, Directors and Senior staff need to appraise themselves of the risks (potential and realised) in their area of activity. Facilities and Services, through the ANU Security Unit, can provide advice and assistance on the assessment and treatment of site security risks.

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

- A central security service on a 24 hours/7 days roster
- Lighted pathways on designated pedestrian routes across campus
- An after-hours security escort service to accompany staff and students, between buildings and to car parks on campus
- An after hours Campus Bus Service

18. Facilities and Services may introduce other measures from time to time.

The role of ANU Security section

19. 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.

20. Other functions of the ANU Security Section 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
- Pastoral support of staff and students
- After-hours management of the University switchboard
- Conduct of security risk audits in accordance with AS4360 and the *Commonwealth Protective Security Manual 2005,* where applicable.

Closed circuit television

21. 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.

22. The Director, 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.

Community awareness and individual responsibility

23. The University has established, and funds, a corporate program (UniSafe) to promote individual awareness of security issues, including personal safety and property protection. A representative committee coordinates the program and provides advice on

specific issues as required. The Director, Facilities and Services, provides support to the committee and manages the budget for the Unisafe Program.

24. Deans, Directors or equivalent are responsible for ensuring staff and students are briefed on the security requirements of their areas.

25. Staff and students are responsible for ensuring that they do not compromise University security arrangements through any deliberate or negligent act. Any deliberate breach of security arrangements may result in disciplinary action.

26. 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.

Document information

Title	Security - buildings and site
Document Type	Policy
Document Number	ANUP_000463
Version	6
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	20 Jul 2017
Review Date	31 Dec 2023
Responsible Officer	Director, Facilities and Services
Approved By	Vice-Chancellor (eo.vc@anu.edu.au)
Contact Area	Facilities and Services (fs.director@anu.edu.au)
Authority	Australian National University Act 1991
Printed On	22 Sep 2023