

Physical Security Infrastructure and Equipment Procedure

1 Purpose

To outline the responsibilities and processes for the management of Security Equipment and Security Infrastructure at University campuses and facilities.

2 Scope

This procedure applies to all University campuses and University controlled facilities.

3 Procedure Overview

This procedure describes the means by which, Physical Security Infrastructure, Physical Security Equipment is managed by authorised Campus Safety and Security at the University.

Physical Security Infrastructure and Physical Security Equipment includes, but is not limited to, Surveillance Equipment, access controls, access/ID cards, keys, lock cylinders, and radios.

4 Procedures

4.1 Provision and Maintenance of Physical Security Infrastructure

1. Physical Security Infrastructure is the responsibility of Campus Safety and Security.
2. Physical Security Infrastructure is a component of Facilities Management planning with specific objectives, priorities and expected timing identified as part of that process.
3. Departments may request Physical Security Infrastructure additions or change in the priorities or expected timing by contacting Campus Safety and Security and submitting a request supported by information relevant to the request.
4. Campus Safety and Security may require additional information at any time during consideration of the request.
5. Physical Security Infrastructure requests will be dealt with by Campus Safety and Security, and may be responded to by a Facilities Management financial delegate as follows:
 - a. Where the request is considered consistent with Facilities Management planning, and is an addition to the plan only, on the basis that priority and timing is at discretion of Facilities Management,

- i. approve and provide Facilities Management funding;
 - ii. approve on the basis that the addition is fully funded by the requesting party;
 - or
 - iii. declined.
 - b. Where the request is considered consistent with Facilities Management planning, and is an addition to the plan, including change in priority and timing,
 - i. approve and provide Facilities Management funding;
 - ii. approve on the basis that the addition is fully funded by the requesting party, including any costing impacts as a result of changes in priority and timing; or
 - iii. declined.
 - c. Where the request is considered consistent with Facilities Management planning, and is not an addition but a change to priority or timing,
 - i. approve and provide Facilities Management funding in support of the change in priority or timing;
 - ii. approve on the basis that the requesting party fully fund the accelerated works or change in priority for the works; or
 - iii. declined.
 - d. Where a request is considered not to be consistent with Facilities Management planning, advise the requesting party accordingly and that it is declined.
6. Any decision that a requesting party is dissatisfied with under paragraph 5 may be escalated by the requesting department's Vice-Chancellor's Executive member presenting information relevant to the request to the Facilities Strategy Board for further discussion.

4.2 Physical key and lock control system

1. Campus Safety and Security will co-ordinate the installation of all physical locks at any University campus or facility, whether a new installation or replacement of an of existing lock.
2. Physical locks must not be changed without prior knowledge and approval from Campus Safety and Security.
3. When buildings, facilities or campuses are added to the University, Campus Safety and Security 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.
4. It is the responsibility of any individual to whom a University key is issued to ensure its safekeeping. In addition, individuals have a duty to return the key/s to Campus Safety and Security when ceasing employment or role with the issuing faculty or department or when completing the assignment or other activity for which the key was provided.

5. University Members may submit an online request via the HUB, for the issue of an Individual or Departmental Key/s, this will require electronic approval by their direct supervisor or property manager. Once approved the applicant can collect the key from the relevant Campus Safety and Security office.
6. If an individual is locked out of a building/office for which they possess a key Campus Safety and Security must be contacted to arrange access. Note that in some cases, a local process may require the individual to demonstrate they possess approval to access the building/office outside of normal business hours.
7. All keys remain the property of the University.

4.3 Contractors and tenants in University buildings

1. Tenants and contractors are bound by this procedure.
2. 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.
3. Contractors are required to consult with Campus Safety and Security and their project supervisor prior to being issued keys. Campus Safety and Security 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.
4. 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. These provisions will be outlined in all University tenancy agreements.
5. 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 Campus Safety and Security for implementation.

4.4 Electronic Access Control system

1. The University uses electronic access control to manage access to campus facilities, restricted areas, and laboratories.
2. Campus Safety and Security is responsible for the design, scope, and co-ordination of electronic access control, at any University campus or facility, including ensuring compliance with the principles of the Protective Security Policy Framework (PSPF) and where applicable Defence Security Principles Framework (DSPF).
3. University Members 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 respective departments. Approval notification is to be sent through to Campus Safety and Security from respective departments, for implementation.

4. Refer to the Physical Security Procedure for the application of a University identification card.

4.5 Surveillance Equipment

1. The University uses Surveillance Equipment to promote a safe and secure environment for the University community, and for the purpose of identification or investigation of incidents or other investigations conducted either by the University or an external law enforcement agency.
2. Surveillance Equipment used by the University consists of, but is not limited to non-auditory Closed Circuit Television (CCTV) on University property and on the intercampus bus services, and photographic identification images from the electronic access control system.
3. The University's Surveillance Equipment is monitored 24 hours a day, 7 days a week by authorised Campus Safety and Security personnel.
4. All imagery captured by the University's Surveillance Equipment will be stored locally on site, and disposed of in accordance with the Records and Information Management Policy.
5. Requests for external parties to become authorised users to view "Live" and "Recorded Footage", can be submitted to Facilities Management. Approval will be assessed on a case-by-case basis, in line with the Privacy Policy.

4.5.1 Surveillance Equipment installations

1. University Surveillance Equipment will not be hidden and will be installed and operated having regard to the Privacy Policy. Surveillance 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.
2. Notices (prominent signage) regarding the use of Surveillance Equipment will be placed at the entrance ways leading into areas under surveillance.
3. The installation locations of Surveillance Equipment is determined by Facilities Management, in coordination with key stakeholders.
4. A plan of the current locations of fixed Surveillance Equipment on each campus will be maintained by Facilities Management. A copy of this plan may be obtained from the

Campus Safety and Security upon written request with appropriate justification.

4.5.2 Surveillance Equipment data disclosure request

1. In accordance with the Privacy Principles, formal application for the University's Surveillance Equipment and photographic identification data must be made to the University for consideration. Applications to be reviewed by the Privacy Officer or their delegate.
2. In an emergency situation, the application process is not necessary, the Executive Director (Facilities Management) or their delegate will give permission for relevant data to be released to the University or an external law enforcement agency.

4.6 Complaints

1. Complaints about the use of Surveillance Equipment or the disclosure of information obtained through such Equipment will be managed in accordance with the relevant University Policy on Complaints.

5 References

Nil.

6 Schedules

This procedure must be read in conjunction with its subordinate schedules as provided in the table below.

7 Procedure Information

Accountable Officer	Executive Director (Facilities Management)
Responsible Officer	Director (Estate Services)
Policy Type	University Procedure
Policy Suite	Physical Security Policy
Subordinate Schedules	
Approved Date	1/2/2024
Effective Date	1/2/2024

Review Date	13/7/2027
Relevant Legislation	<i>Information Privacy Act 2009</i> <i>Invasion of Privacy Act 1971</i> <i>Public Interest Disclosure Act 2010 (Qld)</i> <i>Public Records Act 2002</i> <i>Right to Information Act 2009</i> <i>Surveillance Devices Act 2004</i>
Policy Exceptions	Policy Exceptions Register
Related Policies	Delegations Policy Privacy Policy Procurement Policy Property, Plant and Equipment Assets Policy Records and Information Management Policy Records and Information Management Policy Research Code of Conduct Policy Right to Information Policy
Related Procedures	Parking and Traffic Management Procedure Physical Security Procedure Property, Plant and Equipment Assets Procedure Right to Information Procedure
Related forms, publications and websites	Office of the Information Commissioner - Camera Surveillance and Privacy Guidance Privacy website Queensland Police Service Information Request Form Privacy Application (RTI) Protective Security Policy Framework

	Defence Security Principles Framework
Definitions	Terms defined in the Definitions Dictionary
	Closed Circuit Television (CCTV) A television system in which signals are designed to be monitored rather than publicly broadcast, typically for surveillance and security purposes.
	Security Infrastructure Semi-permanent or permanent equipment installed at the University to increase the physical security of those present and to deter criminal activity. Includes but not limited to alarms, panic buttons, duress buttons, emergency lighting, security signage, electronic access control equipment, surveillance equipment, keys and locks.
	Student A person who is enrolled in a UniSQ Upskill Course or who is admitted to an Award Program or Non-Award Program offered by the University and is: currently enrolled in one or more Courses or study units; or not currently enrolled but is on an approved Leave of Absence or whose admission has not been cancelled.
	University The term 'University' or 'UniSQ' means the University of Southern Queensland.
	University Members Persons who include: Employees of the University whose conditions of employment are covered by the UniSQ Enterprise Agreement whether full time or fractional, continuing, fixed-term or casual, including senior Employees whose conditions of employment are covered by a written agreement or contract with the University; members of the University Council and University Committees; visiting, honorary and adjunct appointees; volunteers who contribute to University activities or who act on behalf of the University; and individuals who are granted access to University facilities or who are engaged in providing services to the University, such as contractors or consultants, where applicable.
	Definitions that relate to this procedure only
	Security Equipment

	<p>Items regularly used by Campus Safety and Security team in the course of their duties to maintain the physical security of the University.</p> <p>Surveillance Equipment</p> <p>Equipment used to maintain close observation of locations, persons or groups.</p>
Keywords	Panic button, Duress button, Emergency lighting
Record No	21/181PL