Facilities Access Control Procedure

Contents

Purpose

This procedure guides security access to and within University buildings and the management of access cards, keys and keying systems for University buildings.

Applicable governance instruments

Instrument	Section	Principles
Facilities, Infrastructure and Assets Policy	4 Facilities Access	Principle 4.1

Procedure

1. General Access Principles

Access control strategy, operations and hardware are managed by Infrastructure Services and Development (ISD) to provide safety and security to people and assets.

The University Security Strategy provides the framework for design and management of the University's access control systems and hardware.

The general principles are:

- University facilities will be open and accessible to students, staff and members of the community where possible, subject to the safety and security of people and assets.
- Buildings and/or spaces that are deemed freely accessible to students, staff and the public will be openly accessible during the business hours normally observed by the building occupants.
- Access control points (locked doors) will be established within facilities based on consideration of operations, functions and associated environments. Generally the following conditions or environments lead to an access control point:
  - Staff spaces connected to public spaces, where staff and/or assets within the staff space need to be protected.

- Spaces with plant/equipment that present a safety risk.
- Spaces where hazardous tasks are undertaken or that produce a hazardous environment.
- Spaces with a high confidentiality requirement.
- Spaces with easily removable attractive equipment (high theft risk) or infrastructure that would cause loss of business continuity.
- Space under the control of other (external) parties such as commercial tenancies.

Electronic access control is preferred to key access due to the benefits associated with management of access cards, monitoring movement and providing flexibility of control.

2. Access Structure

Perimeter doors to major buildings are preferably fitted with electronic access, with a manual key over-ride system to primary perimeter doors.

Various areas or spaces on campus that are "out of bounds" to staff, students and/or maintenance staff are master keyed to restricted access keys because of the health and safety risks that these areas pose. Typical areas include:

- radioactive material stores;
- lift motor rooms;
- roof access and panels through external walls;
- examination paper security rooms;
- IT and security node rooms;
- gas stores; and
- confined space zones.

Some spaces and equipment are 'keyed alike' to allow maintenance service personnel simplified access. These include:

- plant rooms;
- service ducts; and
- automatic door controllers.

Key allocation principles:

- Great/Grand Master keys will only be issued to the fire brigade and University Safety and Security.
- Building Key: The building Fire Warden and School Heads are the only people entitled to possess a building master key.
- Building Area or floor-level master keys: Executive and senior staff such as Executive Deans, College Executive Director Operations, Heads of School/Section, Heads of Division and their senior staff may be issued with a building area key.
- Restricted Room Key: Restricted room keys will only be issued to people authorised to enter the relevant restricted space.

Building entrance keys (for buildings without an electronic access system) and access cards with after-hours authorisation will be issued only to people with a demonstrated need for after-hours access to a building.

The University's keying is established under a registered key system. Independent keying of rooms and areas outside of the master key structure is not permitted.

Lessees are not to change University key or access system infrastructure.

3. Control of Access Cards and Keys

Staff and students may be issued with card access/key for the building(s) and work area(s) they need to access for their duties/course. (Access cards are integrated with the student/staff identification (ID) card.)

Access cards and changes to access will be activated by ISD or its nominees (Shared Services, and Safety and Security) on approval of the requestor's line manager, Head of School or delegate.

Keys are approved and issued by ISD or its nominees (Shared Services, and Safety and Security) on approval of the requestor's line manager, Head of School or delegate. Requests for Master Keys and Grand Master keys require additional approval by ISD.

Access to specialised spaces, eg. labs, requires approval of the designated space manager, eg. lab manager.

Requests for new or amended access (key or card) must be submitted to Campus Services via the *Building and Facility Access Form* available from the Service Now website https://utas1.service-now.com/selfservice/. Student requests are submitted through school administration staff.

Registered contractors requiring access to secured areas must obtain the necessary access card or key(s) from Safety and Security or ISD.

Accommodation Services manage access cards/keys for student accommodation facilities.

ISD will maintain a register of keys issued centrally through its nominees (Shared Services, and Safety and Security).

A register of access cards is automated through the University's access control system database, managed by ISD.

Room keys may be retained and allocated by Schools or Sections. Where Schools or Sections choose to manage room keys, they will be responsible for:

- allocating keys; and
- maintaining a register of keys issued (including recipient name and date of issue).

The duplication of a University access card/key or maintaining a spare is prohibited, unless authorised by ISD.

Student ID access cards are issued for the expected term of their course.

When a student or staff member leaves the university, deactivation of access cards will occur as part of the offboarding process through People and Wellbeing or the Student Management System linking with IT Integration. Heads of Schools/Sections or line managers must:

- advise Safety and Security to deactivate the access card if the need for this is immediate;
- advise Safety and Security to delete access to specific areas for an ongoing student or staff members if access authorisations change; and
- recover keys from students/staff when a student or staff member is no longer authorised to use the key.

Restricted keys recovered by schools/sections must be returned to ISD, unless they are to be reissued to another staff member. If they are reissued, ISD must be advised of the new holder.

Where a key holder has ceased to be employed by the University, People and Wellbeing will not authorise final payment until all keys have been returned.

4. Access Card and Key Use and Responsibilities

People who have been issued with an access card/key are authorised to use the card/key to gain access to only the areas and facilities necessary for the performance of their work/studies.

Access cards/keys are to be used only by the person to whom they have been issued.

People who have been issued with a University access card/key accept responsibility for their:

a. appropriate and legitimate use; and

b. safe keeping.

Access cards/keys that are no longer required (eg. when a person changes location within a School/Section or is no longer employed the University) must be returned by the holder to their Head of School/Section or line managers.

Master Keys, including area/section keys, must be kept on person and not in offices, unless they are held in a suitable key safe or KeyWatcher type key issuing system.

Lost, stolen, damaged or found access cards/keys must be reported to University Safety and Security and U-Connect immediately.

All costs resulting from the loss or non-return of a key shall be borne by the key/access card holder or the School/Section responsible for the safe keeping of the key/access card. Such costs will vary, depending on the extent of the University facilities affected by the loss or non-return.

Related procedures

Nil

Versions

Version	Action	Approval Authority	Responsible Officer/s	Approval Date
Version 1	Approved	Chief Operating Officer	Executive Director ISD	12/05/2021