Facilities Access Control Policy

Responsible Officer
Executive Director, Infrastructure Services and Development

Approved by
Vice-Chancellor

Approved and commenced
December, 2014

Review by
December, 2017

Relevant Legislation, Ordinance, Rule and/or Governance Level Principle
University By-laws (Part II, Section 6)

Responsible Organisational Unit
Infrastructure Services and Development

CONTENTS

1 Objective ................................................................................................................... 2
2 Scope ........................................................................................................................ 2
3 Policy Provisions ....................................................................................................... 2
3.1 General ...................................................................................................................... 2
3.2 Access Control Hardware .......................................................................................... 2
3.3 Issue of Keys and Access Cards ............................................................................... 3
3.3.1 Key Entry ................................................................................................................... 3
3.3.2 Access Card Entry ..................................................................................................... 3
3.4 Control of Access Cards and Keys ............................................................................ 3
4 Responsibilities .......................................................................................................... 4
5 Definitions and Acronyms .......................................................................................... 4
6 Supporting Documentation ........................................................................................ 5
7 Versioning ................................................................................................................. 5
1 Objective

The objectives of this Policy are to:

- provide security to staff, students, facilities and property by regulating the issuing, allocation, control and return of electronic access cards and mechanical keys and
- ensure the integrity of the University’s facilities access control systems.

2 Scope

This policy applies to:

- all University building facilities, organisational units (OUs) and their operations and
- all persons issued with a University access card and/or key.

It does not apply to access control of non-fixed security boxes, safes, cabinets, joinery, refrigerators, freezers, research equipment and the like.

3 Policy Provisions

3.1 General

As a general security measure for staff, students and property, University buildings will be locked outside of the business hours normally observed by the building occupants.

Entry to buildings and areas that are deemed to be freely accessible will be enabled during business hours. Access outside of these hours must be arranged with University Security.

Infrastructure Services and Development (ISD) will maintain a central key register to facilitate the central maintenance and management of access cards and keys.

Records and Information associated with this policy will be created, maintained and retained in accordance with the University Records Management Policy, Procedures and Guidelines

3.2 Access Control Hardware

The University Access Control Strategy will provide the framework for design and management of the University’s access control systems and hardware.

All access control hardware will be controlled by ISD. Unauthorised installation or modification of access control systems and/or hardware is prohibited.

Cross-keying will not be provided except as part of a system design approved by ISD.
3.3 Issue of Keys and Access Cards

Access cards and keys will only be issued or activated by ISD or its nominee on the approval of the relevant Head of OU or delegate.

Once issued, an access card may be reissued or reactivated by University Security upon request from the card holder with the approval of the relevant Head of OU or delegate.

Unless delivered as part of building works, the cost of new and replacement access cards and keys will be borne by the OU requesting them.

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

Room(s) keys may be retained and reallocated by OUs. Where OUs choose to manage room(s) keys, the OU will be responsible for:
- allocating keys
- collecting keys from staff who no longer require them (e.g. upon relocation or cessation of their employment with the OU)
- maintaining an accurate key register and
- the cost of any replacement room(s) keys.

The duplication of a University access card/key and/or maintaining a ‘spare’ is prohibited, unless specifically authorised and enacted by Infrastructure Services and Development (ISD).

3.3.1 Key Entry

Building Key
Building Fire Wardens will be issued with a Building Key and will have full access authority for the relevant building on their access card.

Building Area Key
Heads of OUs and their senior executive staff may be issued with a Building Area Key upon request.

Restricted Room(s) Key
Restricted Room(s) Keys will only be issued to persons authorised to enter the relevant restricted space.

Building Entrance Key
Building Entrance Keys will only be issued by CSD in cases where a clear need for the key is demonstrated.

3.3.2 Access Card Entry

The level of building access provided by an access card will be determined by the relevant Head of OU.

3.4 Control of Access Cards and Keys

Access cards and keys are only to be used by the person to whom they have been issued.
Access cards and/or keys that are no longer required must be returned by the holder to ISD or University Security. The only exception to this are room(s) keys issued by an OU, which must be returned to the relevant OU in accordance with Section 3.2 of this Policy.

Where an access card/key holder has ceased to be employed by the University, Human Resources will not authorise final payment until all keys and access cards have been returned.

Access cards issued to students will expire annually, unless an alternative period of access has been arranged with CSD.

Lost, stolen, damaged or found access cards and keys must be reported to University Security immediately upon discovery.

4 Responsibilities

**Infrastructure Service and Development** is responsible for:

- design and management of the University’s access control systems and hardware
- allocating and retrieving keys and access cards, with the exception of locally managed room(s) keys, as specified in Section 3.2 of this Policy and
- maintenance of the central Key Register.

**Organisational Units** are responsible for:

- replacement costs associated with access cards and keys allocated to them; and
- management of keys retained and issued by the OU in accordance with Section 3.2 of this Policy.

**Heads of Organisational Units** are responsible for:

- authorising the allocation of keys and access cards to OU staff and
- determining the level of access to be associated with each access card issued to OU staff.

**All persons issued with a University access card/key** is responsible for:

- safe-keeping of the card/key, including not lending the card/key to any other person
- reporting any loss or theft of, or damage to, the access card/key to University Security immediately upon discovery of the loss, theft or damage and
- paying upon request any costs associated with the replacement of the card/key in the event of loss or damage.

5 Definitions and Acronyms

<table>
<thead>
<tr>
<th>Term/Acronym</th>
<th>Definition</th>
</tr>
</thead>
</table>

**Facilities Access Control Policy (December, 2014)**
Access Card
A card, fob or similar device used as an electronic key

Building Area Key
A mechanical key that opens all locks within a designated area of a building

Building Entrance Key
A mechanical key that provides building entry access only

Building Key
A mechanical key that opens locks to all general spaces within a building

Organisational Unit
College, Faculty, School, Centre, University Institute, other University Entity, Division, Section or University Business Enterprise.

Restricted Room(s) Key
A mechanical key giving access to areas that may only be entered by persons with the requisite training, licensing or system authority due to work health and safety hazards or systems security risk.

Room(s) Key
A mechanical key that opens locks for singular or multiple rooms only

University Security
Security Services provided by Infrastructure Services and Development

University
University of Tasmania

6 Supporting Documentation
- Access Control Strategy
- Access Control Procedure
- Records Management Policy

7 Versioning

<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Current Version</td>
<td>Version 3 – Access Control Policy (current document), approved December 2014, amended in December 2017 to incorporate the final academic structure.</td>
</tr>
</tbody>
</table>