Policy Title: ECU Access Control

Policy Owner: **Manager, Campus Operations and Resources**

Keywords: **1) Access** **2) Entry** **3) Security**

Policy Code: **PL263 [fs040]**

Intent
Organisational Scope
Definitions
Policy Content
Accountabilities and Responsibilities
Related Documents
Contact Information
Approval History

1. INTENT

The purpose of this policy is to ensure that access to internal and external areas of University premises are managed, allocated and secured in a controlled manner. The policy also seeks to inform staff of their responsibilities in regard to access matters.

2. ORGANISATIONAL SCOPE

Edith Cowan University staff, students, contractors and tenants.

3. DEFINITIONS

TERM	DEFINITION
Authorised	Having appropriate level of delegation.
Access card	Radio Frequency Identification (RFID) card used to access controlled buildings.
Access Control	Technology and physical controls typically (locks and/or access control system) limiting the access to specific areas.
Access Controlled area	Any area, which requires the use of a keys or access card in order to gain entry.
Alarm	Security Alarm System.
Contractor	The person, partnership or corporation who is bound to execute an agreed scope work under the contract.
Gallagher	Access control system used within ECU.
Security and Traffic Services Staff	ECU security employees and contract security staff.
University	Edith Cowan University.

4. POLICY CONTENT

To ensure the security of staff, students, contractors and tenants whilst on University premises. In addition to personal protection, the policy seeks to protect the assets of the University by maintaining the integrity of the building's access control and security officer management systems through appropriate levels of management and process control.

4.1 General Provisions

a) Security and Traffic Services is authorised to provide access to buildings, rooms and spaces throughout the University based on the need to access particular spaces and the associated risk that arises to stakeholders, assets and information.

b) Access may be granted through the use of electronic access card or alarm codes and is provided upon request by an authorised officer when warranted.

c) Authorisation for an individual's access to specific areas is granted by Security and Traffic Services in consultation with the various custodians of the spaces within the University.

d) Requests for access to specific areas is to be received on the appropriate access control request form and endorsed by the custodian of an area, typically a Head of School, Operations Manager or Centre Director (or authorised delegate).

e) After hours (ad-hoc) physical access to keyed areas will be granted by security officers only when the officer is satisfied that the requestor is authorised to enter the space.

f) During business hours ad-hoc access is granted through the Campus Support Office (CSO). The CSO will issue low level (non-master) keys should they be required. Access to areas requiring master key level access during business hours this will only be granted in accordance with the Master Key Policy.

g) Users must adhere to the terms and conditions as set out by the ECU Access Control Conditions of Use. The terms and conditions of use relating to the access control system are available via the ECU website, and also within the terms of employment.

h) Users of the access control system must take all reasonable steps to protect access cards and passwords. Sharing of access cards or alarm codes may result in access to spaces being removed from individuals.

i) As a general principle, Security and Traffic Services will decide if access will be granted based on the security risk to stakeholder, assets and information.

j) Areas fitted with combination door locks must be changed at the completion of each semester. It is the responsibility of the custodian of the area to ensure all combinations are changed and disseminated only to those requiring access.

4.2 Alarms

Access control alarm codes will be restricted based on need for access. User and operational requirements will be taken into consideration when alarm codes are requested. Alarm passwords must be memorised (not written) and kept confidential. Should a user sharing or documenting a password be identified access to alarm codes will be removed.

4.3 Access logs

Security and Traffic Services will be responsible for reviewing all available access control logs and audit trails. Access to this information will be granted to third parties (e.g. Police, custodians of an area, Risk and Assurance Services) only when requested in writing and authorised by the Manager Security and Traffic Services.

4.4 Access changes

It is incumbent on the custodians of respective areas within the University to notify *Security and Traffic Services* of the access control requirements of staff and students.

a) Students

Access rights for students relating to specific units of study within a teaching period must be communicated to *Security and Traffic Services* by the school operating those particular units of study a minimum of two weeks prior to the beginning of the teaching period.

b) Staff

i. Staff access right requests should be provided within a minimum of two days prior to the need for access. If circumstances do not allow for this then their access right will be granted after their commencement date.

ii. The custodians of an area must notify *Security and Traffic Services* of staff movements to and from their area to ensure correct access controls are kept up to date.

iii. Access rights will be removed by *Security and Traffic Services* as soon as practicable, upon receipt of a written request.

4.5 Tenanted Buildings

a) Where practicable, and with consideration to security and cost implications, access control systems to high risk areas shall be modified where necessary to be fitted with the ECU *Gallagher* control system prior to a new tenant taking occupancy of that premises.

b) All tenants or licensees occupying or utilising buildings, outbuildings and secure areas situated on University campuses are obligated to notify *Security and Traffic Services* of any changes in security requirements or additional security access required.

4.7 Lost & Found Access cards

a) Lost University access cards are to be reported immediately to *Security and Traffic Services*.

b) Upon receipt of advice of a lost card, *Security and Traffic Services* staff is to immediately disable all access to the cardholders profile in order to minimise potential misuse.

c) Found cards are to be handed directly to either;

i. Security and Traffic Services staff; or
ii. Student Central,

Security and Traffic Services staff will then either identify the rightful user and return, or destroy the card.

5. ACCOUNTABILITIES AND RESPONSIBILITIES

In relation to this policy, the following positions are responsible for the following:

The Manager, Campus Operations and Resources have overall responsibility for the content of this policy and its operation in ECU.

The Security and Traffic Manager has the overall responsibility to ensure that the administration and operational processes and procedures are managed as per the established Policy.

6. CONTACT INFORMATION

For queries relating to this document please contact:

Policy Owner	Manager, Campus Operations and Resources
All Enquiries Contact:	Security and Traffic Services Manager
Telephone:	08 6304 2271
Email address:	h.cotton@ecu.edu.au

7. APPROVAL HISTORY

Policy Approved by:	Vice-Chancellor
Date Policy First Approved:	June 2015
Date last modified:	May 2018
Revision History:	06/15 05/18
Next Revision Due:	June 2021
HPRM File Reference	SUB/65133