ACCESS CONTROL PROCEDURE

SCOPE

This policy applies to:

- all Monash University students, staff, associates;
- visitors and contractors to all University locations; and/or
- those who are engaged in a University activity.

For the purpose of this procedure, references to 'the University' includes activity at Monash University Australia, Monash University Indonesia, Monash University Malaysia, Monash Suzhou, the Monash University Prato Centre and World Mosquito Program Ltd (and its subsidiaries), unless indicated otherwise.

PROCEDURE STATEMENT

This procedure explains the University's access control system and establishes processes that address the issue, use and management of access credentials.

1. Specification and installation of access control systems

1.1 The University's access control system consists of methods and equipment for regulating access to buildings and areas across University locations.

1.2 The selection, installation and maintenance of any component of an access control system must be approved by Security Services.

1.3 Security Services is responsible for maintaining the Monash University Electronic Security Specification (MU-ESS), a single standard access control specification (contained within the Monash Design and Construction Standards) for the access control system across the University. Hardware and software components of the MU-ESS (e.g. cards, card readers, software, locks) should be uniform and consistent across the University.

1.4 Amendments to the MU-ESS are made by Security Services in consultation with relevant stakeholders.

1.5 The design, installation, upgrade, maintenance or replacement of any part or component of the access control system in accordance with any minor or major capital works project must be compliant with the MU-ESS.

- Security Services is responsible for assessing compliance with the MU-ESS.
- In developing specifications for the works required, and in assessing compliance with the MU-ESS, Security Services will appropriately liaise and consult with the relevant project, asset or maintenance manager and/or Access Coordinator.
- Final approval from Security Services must be obtained before any work on the access control system proceeds.

2. Access authorisation and credentials

2.1 Access to controlled areas across the University requires authorisation and the issuing of access credentials.

2.2 Access credentials are part of the access control system and facilitate access to buildings and areas across University locations.

Approval for issue of access credentials

2.3 Access credentials will only be issued in conjunction with the appropriate access approval. Approvals for access (and the issue of associated access credentials) are coordinated through the relevant Access Coordinator, ordinarily nominated by heads of department/unit.

2.4 The relevant Access Coordinator is responsible for liaising with Security Services to coordinate an access approval.

2.5 If a student, staff member or contractor is unsure who the relevant Access Coordinator is, they should contact Security Services.

Use of access credentials and entry to controlled areas

2.6 A person must not knowingly access a controlled area without authorisation.

2.7 An access credential must only be used by the person it has been issued to. This means:

- access credentials must not be lent or given to another person;
- an access credential must not be used to enter an area the person is unauthorised to access; and
- a person must not knowingly use an access credential that has been issued to another person.

2.8 Where a person is known or suspected to have accessed a controlled area without authorisation, or used an access credential improperly, the incident should be immediately reported to Security Services.

2.9 An access credential must not be copied or duplicated without authorisation from Security Services.

2.10 Additional terms and conditions apply specifically to an M-Pass access credential.

2.11 All access credentials remain the property of Monash University and may be recovered at any time.

Damage, loss or theft of access credentials

2.12 The damage, loss or theft of any access credential must be immediately reported to Security Services.

Presentation of access credentials

2.13 Any student, staff member, contractor or visitor who has been issued with an access credential must present that credential on request by a member of Security Services.

Withdrawal of access

2.14 An Access Coordinator may request that a person's access be reduced, amended or revoked. Security Services may refuse, reduce, amend or revoke access at any time, including upon request by an Access Coordinator.

2.15 An Access Coordinator or member of Security Services may request at any time that a person leave an access controlled area, even if that person has previously been authorised to enter.

2.16 Access Coordinators are responsible for retrieving access credentials as required when a person's access is reduced, amended or revoked.

DEFINITIONS

Access control system	The University's system, method and equipment for controlling access to buildings and areas including, but not limited to, electronic code-pads, card readers, remote arming stations, passive infra-red detectors, duress buttons, reed switches, mechanical barriers, mechanical or electronic locks and keys, digital credentials, bluetooth or radio-frequency based access technology, and the use of identification cards, signs, definitions and instructions that are used to define spaces which certain people may or may not enter.
Access credential	A component of the University's access control system that facilitates building or area entry/egress by a particular person including, but not limited to, swipe cards (such as the University's M-Pass card), mechanical keys and locks, electronic keys, and access technology that is bluetooth or radio-frequency based.
Access Coordinator	The designated access coordinator for a building or area.
Security Services	For a University location or University activity within Australia - means the Security Services business unit within Community Safety and Security. For a University location or University activity outside Australia - means the physical security arrangements at the relevant location overseen by Global Security and Crisis Response.
University location	As defined under 'university precinct' in the Dictionary to the Monash University (Council) Regulations, means the whole or part of any land, building or facility owned or occupied by the University or used by it, or by one or more students for the purpose of conducting a University activity.

GOVERNANCE

Parent policy	Community Safety and Security Policy
Supporting procedures	Safety and Security Incident Reporting Procedure Surveillance Devices Procedure
Supporting schedules	Nil
Associated procedures	Nil
Related legislation	Surveillance Devices Act 1999 NO. 21 (Vic) Privacy and Data Protection Act 2014 (Vic) Personal Data Protection Act 2010 (Malaysia)
Category	Operational
Approval	Chief Operating Officer 17 November 2021
Endorsement	Executive Director, Campus Community Division 9 November 2021
Procedure owner	Director, Community Safety and Security
Date effective	1 January 2022
Review date	1 January 2025
Version	1.1 *(minor amendments effective 27 May 2022)*
Content enquiries	safety@monash.edu