Monash University Policy

Policy Title	Access to Controlled Areas Policy
Date Effective	12-September-2016
Review Date	12-September-2019
Policy Owner	Executive Director, Buildings and Property Division
Category	Operational
Version Number	3.0
Content Enquiries	finance-policy@monash.edu
Scope	This policy applies to all staff and students of: - Monash University at the university's Australian campuses and off-campus facilities; and - Monash College Pty Ltd business units at the university's Australian campuses.
Purpose	Access control credentials are issued by Monash security offices to allow students, staff and contractors access to controlled areas of the university. All persons to whom an access control credential has been issued must only use the credential to enter areas of campus for which they are currently authorised. Access credentials must be used only by the person to whom they have been issued. They must not be lent, given to or used by any other person to enter a controlled area for which they have no authorised right of entry. Anyone possessing of using an access control credential (including a PIN code) to enter university premises without authorisation will be subject to disciplinary actions from the university, or criminal charges where appropriate.

POLICY STATEMENT

Access control credentials are issued by Monash security offices to allow students, staff and contractors access to controlled areas of the university.

All persons to whom an access control credential has been issued must only use the credential to enter areas of campus for which they are currently authorised. Access credentials must be used only by the person to whom they have been issued. They must not be lent, given to or used by any other person to enter a controlled area for which they have no authorised right of entry.

Anyone possessing of using an access control credential (including a PIN code) to enter university premises without authorisation will be subject to disciplinary actions from the university, or criminal charges where appropriate.

Supporting Procedures	Access to Controlled Areas Procedures
Responsibility for implementation	Executive Director, Buildings and Property Division
Status	Revised

Approval Body	**Name:** Chief Operating Officer and Senior Vice-President (Administration) **Date:** 12-September-2016
Endorsement Body	**Name:** Buildings and Property Divisional Executive Group **Date:** 08-September-2016
Definitions	**Access Control Credential**: Any electronic access control device or token such as a magnetic stripe card, proximity card or key-ring fob which can be used to activate a locked or electrically controlled door, turnstile, boom-gate or similar barrier when programmed to do so. For the purposes of this policy the word "credential" includes codes or personal identification numbers (PIN) used for access purposes. **Department/Faculty Access Coordinator**: A staff member in a given department or faculty who has been delegated the authority by their dean or department head to grant deny or revoke access privileges to controlled areas for which the faculty or department is directly responsible. **Controlled Area**: Any area or space on campus to which general or public access is not available at that time, and this may be characterised by signs, locked doors, fences, boom-gates, sentinel tape, or be defined by the instruction of a campus security officer or designated member of staff. **Monash Identification Card (ID)**: An official photographic identity card issued by Monash University. **Security Representative**: A person appointed to the role by the university.
Legislation Mandating Compliance	
Related Policies	Access Control (Electronic) Policy Electronic Security Alarms Policy Key Policy
Related Documents	