ACCESS CONTROL TO CAMPUS BUILDINGS AND PROPERTY POLICY

Policy number	COR 5.11
Policy name	Access Control to Campus Buildings and Property Policy (Issue Four)
Applicability	All Bond University Staff, Students, Contractors and Visitors
Policy owner	Director, Commercial Services
Contact person	Director, Commercial Services
Policy status	Approved policy
Date created	31 March 2008
Date last amended	18 November 2019
Date last exposed	May 2016
Date last reviewed	
Date of next review	18 November 2022
Related policies	

1. OVERVIEW

The purpose of this Policy is to outline University procedures regarding the building access and provision of proximity cards and keys. Bond University is committed to the safety and security of staff, students, and their property. The development of building access procedures assists in identifying authorised individuals on University premises.

2. THE POLICY

2.1. Access to Buildings

2.1.1. Staff

Access to buildings on Campus is controlled by proximity card and granted on a building by building basis according to the position description requirements of the staff member. All Bond University staff are issued with a proximity card at the commencement of duty with the University. If a staff member is eligible for access, the Faculty/Office Authority will complete the Building Access Application and forward to Campus Security. This card, once appropriately coded by Campus Security, will allow access to necessary buildings and property according to the individual's position description and duties performed.

If the position warrants access to multiple areas on Campus, written approval must be sought from the Director Commercial Services or the Vice President Operations. This written approval must be supplied with the Building Access Application form when submitted to Campus Security.

2.1.2. Students

Student identity cards are programmed by Campus Security according to their status, i.e. residential student.

2.1.3. Campus Security Access

Campus Security will have access to all areas. Campus Security will carry Great Grand Master Keys and proximity cards.

2.2.4. Commercial Tenants

Commercial Tenants are responsible for their own security and access. Keys to tenanted areas will be held with Campus Security. Access to tenanted areas will only apply with written approval from the tenant or approved delegate. In the event of a safety or emergency situation approval to access a tenanted area can be approved by the Director, Facilities Management, Director, Commercial Services, Vice President Operations or Vice-Chancellor.

2.1.5. Other

Permanent contractors (Campus Security Contractor, Cleaners) will be issued with proximity cards.

All visitor and special access cards are to be issued by Campus Security and signed for by the individual requesting access, on a visit by visit basis.

2.1.6. After Hours or Restricted Area Access

If a staff member requires access into restricted areas and/or access outside of the normal operating hours (i.e. on weekends), permission must be authorised by the Faculty/Office Authority to whom that staff member reports. Any person found inside a building after hours without authorisation will be asked to leave the building immediately.

Student ID cards are coded for afterhours access to the MLC, Library, and Building 1B (computer labs). All other out of hours' access to buildings, including PhD or Master's Degree students, will require authorisation as per the Proximity Card and Key Control Guidelines.

Persons working alone in a laboratory or other potentially dangerous area *outside normal working hours* are requested to advise Campus Security, by email or telephone, that they are in the area, the intended duration of the stay and on departure.

2.2. Keys

2.2.1. Building Master Keys

The Building Master Keys will be held in the Campus Security office. Only one key is to be issued to an individual at any one time. A Building Master Key will not be issued permanently.

2.2.2. Section Master Keys

Section Master Keys will be held in a Locked Box in the Faculty Business Director's office with access restricted to the Executive Dean, the Executive Dean's Executive Assistant and the Faculty Business Director. These keys will be available within the Faculty to allow access to offices or rooms under their control in emergency situations, or to provide access to staff under their control. Section Keys in Administrative Offices will be held by the Manager of the area.

2.2.2.1. Office or Room Keys

Staff will be issued with individual room keys only. Access to buildings outside of normal office hours will be as per clause 2.2.1, providing the relevant authorisation procedures are in order. Office key(s) and proximity card(s) are not to be kept together (such as on a chain or lanyard). Staff will keep their proximity card and office/room key in separate locations.

2.2.2.2. Key Register

All keys will be signed out by Campus Security, either on a permanent basis or as needed. Campus Security will have the responsibility of ensuring all keys are returned when they are not in use. All permanent key holders must sign their keys in and out at the start and end of their tenure at Bond University (refer to section 5: Related Guidelines and Forms: Proximity Card Register form).

2.2.2.3. Lock Change Keys

The University approved key supplier will hold Lock Change keys for the assembly of key barrels. Two Lock Change keys will be held on Campus in the key safes under the control of the Office of Facilities Management and the Security Office. The contracted key supplier signs out the Lock Change key as required.

3. AUTHORITY DELEGATION

See Schedule 1 for authority delegations.

4. DEFINITIONS

Campus	Includes the campus at University Drive, Bond Institute of Health & Sport (BIHS), Bond University Clinical Education and Research Centre (BUCERC).
Proximity Card	Electronic Access Control Card. A proximity card is coded to enable access to Bond University buildings and property.

5. RELATED PROCEDURES, GUIDELINES AND FORMS

Schedule 1: Authority Delegations
Proximity Card and Key Control Guideline Version 1
Building Access Application (Campus Security)
On Campus Accommodation Resident Handbook
Proximity Card Register form (Campus Security)
CS-SEC-FRM-003 Counter Statement
CS-SEC-GDE-001 Lost Key Risk Assessment

SCHEDULE 1: Authority Delegation

Faculty, School, College or Office Authority	
Chancellery	Vice-Chancellor
Bond Business School	Executive Dean
Faculty of Law	Executive Dean
Faculty of Health Sciences and Medicine	Executive Dean
Faculty of Society and Design	Executive Dean
Bond University College	Deputy Vice-Chancellor (Academic)
Student & Academic Services (incl. Student Services)	University Registrar
Strategy, Systems & People	Executive Director, Strategy, Systems & People
Sport	Executive Director of Sport
Future Students and Marketing and Communication	Executive Director, Future Students
Office of Alumni and Development	Director, Alumni & Development
Information Technology Services	Director, Information Technology Services
Financial Services	Director Financial Services
Human Resources	Director, Human Resources
Office of Research Services	Director of Research
Office of Learning and Teaching	Director, Learning & Teaching
Office of Facilities Management	Director, Facilities Management
Office of Commercial Services	Director, Commercial Services
Library Services	University Librarian

PROXIMITY CARD AND KEY CONTROL GUIDELINES

1. Proximity Cards

All University staff are required to:

- Maintain, secure and be responsible for any proximity card or key issued.
- Report the loss, theft or damage of proximity cards or keys to Campus Security, Facilities Management, and to the Faculty/Office Authority within 24 hours of discovery of the loss, theft or damage. Individuals who have lost or damaged their assigned key/s or proximity card should advise Campus Security immediately. If it is the key to the residential accommodation, the Accommodation Office staff should also be notified as soon as possible. The student will be charged for a replacement key as per the On Campus Student Handbook.
- Return all issued proximity cards and keys to the Faculty/Office Authority at the end of tenure or enrolment at the University.

PhD or Master's Degree students requiring access to buildings *out of hours* for purposes of research or study will adhere to the following procedure:

- Present authorisation notification, including student name and Student ID number and signed by the relevant Executive Dean or designate (Executive Officer), to Campus Security.
- On presentation of the student's ID card, Campus Security will issue a proximity card and retain the student ID until the return of the proximity card.

1. Issue of Locks / Keys

In conjunction with the University's key supplier, a Master Key Schedule will be designed for each Campus building to fit into the Keying Plan for the University.

The following features should be incorporated into the re-keying plan:

- One (or more if deemed necessary to facilitate secure access) external designated after-hours door/s shall be allocated to each building which will be fitted with the Bond University Access Control System (BUACS). All other external doors shall be electronically locked and connected to the BUACS as determined by the Director Facilities Management and Campus Security Manager (or their delegates). All electronic doors shall be keyed alike, and keys issued only to Security and Maintenance for emergency use. This increases the security of the building as all after-hours access to the building is through the designated after hours door/s.
- Areas within the building can either be keyed alike or keyed differently.
- Maison keying is where a service level key can open the key coded door to which it's designated, as well as one or more other service level keyed doors. No Maison keying shall occur within the University.
- Common use areas shall be keyed alike to limit the number of keys that need to be issued.
- Re-keys shall be kept at the lowest level (service level) of keying possible. Areas shall not be re-keyed to a system where people are reliant on Master Keys to obtain access to several areas; these areas should be keyed alike or fitted with the BUACS.

Re-keying planning will occur at a meeting between the Director Facilities Management, Campus Security Manager (or their delegates), and stakeholders.

The normal scale of key issue will be:

- One service level room key to each occupant of a separate room in the building interior, as is the case for Professional, Research and Academic staff. If, a decision is made to permanently issue a master or higher-level key permanently to an individual staff member, then a detailed risk assessment needs to be completed in consultation with the Director Facilities Management and Campus Security Manager.
- Master or higher-level keys permanently issued to individual staff members should be locked in an approved cabinet when not in use.
- To minimise the financial risk associated with rekeying, master or higher-level keys must not be taken off Campus without the written approval of the Vice-Chancellor.
- Keys to common use areas (general office spaces, resource rooms, photocopy areas, tea rooms, lunch rooms, etc.) are to be issued to those people who are required to access these common use areas before anyone else on a daily basis. Another key to these areas should be kept in the key cabinet for short-term sign out and issue as required.
- One proximity access card for the after-hours access door/s to the building for those persons provided with a room key as above, upon establishment that after-hours access is required on a frequent basis.

- All keys that are not issued are to be stored in approved "secure key cabinets". Director Facilities Management or Campus Security Manager (or their delegates) will determine the type and size of key cabinet required after a brief risk assessment has been conducted.

2. Lost or Stolen Keys

If keys are lost or stolen, and after a 24-hour period are still not found, a report shall be made to the Campus Security in the form of an Incident Report or Counter Statement, detailing the circumstances and events which occurred resulting in the key/s becoming lost or stolen.

The Campus Security Manager in consultation with Director Facilities Management and Director Commercial Services and stakeholders, shall undertake a Risk Assessment.

Risk assessment will be conducted as per Campus Life Lost Key Risk Assessment Proforma.

3. Key Audits

Every year a full Great Grand and Grand Master key audit and 30% Master Key audit (via a sampling methodology) shall be conducted by the Director Facilities Management or their delegate. The Director Facilities Management or their delegate will nominate audit dates and compliance periods. The Director Facilities Management is responsible for checking the audit results, follow up on audit outcomes and reporting of results to the Vice President Operations.