ACCESS CONTROL POLICY & PROCEDURES

SECURITY SERVICES

Customer & Support Services | Infrastructure Branch

Contents

1. Objective

The objective of access control is to regulate access and to ensure that unauthorised access is prevented. This is for the safety and security of all. Access Control is about supporting the life-cycle of user access until the time when no further access is required.

2. Card Issue

University of Adelaide ID cards are issued by Ask Adelaide including for Staff, Students, Visitors, Contractors and Co-Location Cards (AWRI, CSIRO, PIRSA & SARDI). Ask Adelaide provide replacement cards at cost. Security, who manage access control do not print cards.

3. Basic access for Staff and Students

All cards are provided with general access to Hub Central. Students are also provided with a standard set of access permissions related to the program enrolled, this is regulated by the student's enrolment through the Peoplesoft import

3.1 Contractor Card Issue is facilitated by the HSW induction system, Rapid Global Import and printed by Ask Adelaide.

3.2 Security Services provides Access Control. This Policy is for building access added to University of Adelaide ID cards after issue and for the management of access.

4. Cards to be carried and produced on request

ID cards, remain the property of the University of Adelaide. ID cards must be carried by staff, students and contractors at all times while on University premises. Other conditions are printed on the back of the card including the requirement to be **produced on request**.

4.1 Only authorised person(s) can demand for the card to be inspected. Authorised person(s) include Security Services and any person(s) with authority and / or a lawful reason. Security Services may ask anyone at any time to produce their card for inspection.

5. Principles of approving access

The addition of access to a card must follow the principles of only what is reasonable and necessary. **The 'owner' of the premises** may approve or remove access at any time. Owner being the Faculty, School, Division or entity that has been given lease or authority over the premises. This is generally allocated by Capital Projects and Facilities Management.

5.1 In authorising access the owner has the legal liability to comply with all internal policy and external legislation. This is particularly in relation to Health, Safety & Welfare, considering the risk, users and time of day as well as other factors. Safe Operating Procedures need to be established for all areas at risk, before providing access. **The risk of providing access needs to be balanced against the reasonable expectations of staff and students under the circumstances**.

6. Access can be Revoked and Card Voided

The right of access can be revoked at any time on advice of entities such as Security Services, Student Engagement, Legal & Risk, Counselling Support and others. This is particularly in relation to acts of endangerment, criminal activity, psychological/medical disorders and / or misconduct.

6.1 Any staff member, student or contractor that deliberately misuses a card or access point may have the card voided immediately. This includes lending a card to someone else, permitting unauthorised access to persons into a building, propping doors open, tampering with doors or trying to bypass security systems.

6.2 Where access is revoked an appropriate system of reporting must be used to ensure the offender is spoken to and enters into a behavioural contract before access is restored. Student reports should go to Student Affairs/Student Life for action as they relate to student behaviour and may impact on academic success. Reports of staff or contractor misuse should go to the relevant departments/schools, Human Resources, safety and welfare areas.

6.3 The University Student Charter Section 4 refers to studying in a safe and supportive environment, using University facilities in ways that are not inconsiderate to others and do not breach University Policy. Letting an unauthorised person into a university building or failing to report to Security an unauthorised person entering a building may subject the student to the Student Misconduct Policy, which if proved, Section 5, has penalties including a fine, exclusion from areas, cancellation, suspension or expulsion.

7. Awareness

It is quite common for people without access to wait for an authorised person to use their card to open a building then tail-gate/follow them in. Should this occur the cardholder has an obligation to phone Security on 831 35990 if it is just a routine suspicion or 831 35444 if it is more urgent.

7.1 An unauthorised person is anyone, who does not have a valid University ID Card, or attempting to obtain access to an area to which they do not have programmed access. This includes members of the public in what would normally be public access areas after closing hours. It may include family, friends, visitors, children, vagrants and people suffering from intoxication or mental illness, opportunists, those with mischievous or criminal intent.

7.2 Children (aged under 18 years) present a special risk. Whilst maturity for age may vary from child to child, a child under 11 years of age is considered a welfare risk and must always be accompanied by an adult or carer. The parent or carer must be within sight or sound of the child or it could be considered child neglect. Letting an unaccompanied child into a building after hours could be considered negligent. The younger the child the greater the risk. Unaccompanied children must be reported to Security. Child neglect (abuse) is a Reportable Incident to the Child Abuse Reporting Line (CARL) on 131 478.

8. Access Delegates

Access Delegates are appointed from all University entities to authorise access for professional staff and students, they must be a currently employed member of staff and authorisation approved by a head of school or area manager by completing the 'Authorised Access Delegates' form available on the Infrastructure website.

8.1 Qualities

An access Delegate needs to be available, approachable, responsible and methodical with attention to detail. They also need to be good communicators with staff, students and the Access Control Office.

8.2 Training

An Access Delegate needs to become familiar with all their staff, students and programs, all locations they have access to and the associated risks and the access levels that apply to their areas. Access Delegates need to be prepared to understand and develop access levels.

9. Principles and Procedures for approving Access Requests

Access is always allocated according to the needs of the user, always to the lowest privilege level possible.

9.1 An Access Delegate must:

a) satisfy themselves as to the identity of the person requiring access, their enrolment or employment and the validity of their access need;
b) have full knowledge of the area they are giving access to, the risks and rules associated with the area;
c) complete the access request with sufficient detail for the request to be processed;
d) notify the Access Control Office as soon as possible when circumstances have changed and access is required to be removed. E.g. staff end of employment or transferring to another area within the University of Adelaide.

9.2 An access delegate must not:

a) request access to an area not under their control,
b) have someone else submit the request on their behalf,
c) release their e-mail password for the use of another or
d) submit an access request without due prudence.

10. Access Control Officers

Access Control Officers work within the Security Services structure and use the SiPass system to develop and improve access systems to ultimately add access to cards as required.

10.1 Access Control Officers liaise with multiple clients to develop access systems:-

a) Capital Projects & Facilities Management for new building installations and alterations, access solutions for projects and maintenance.
b) Schools and Departments through Access Delegates to provide card access
c) Ask Adelaide for new and replacement cards.
d) Operations and contractors to develop access solutions for maintenance.
e) Access Control Officers are committed to the learning and understanding of Access Delegates and the development of University Access Control systems;
f) have a suitable security clearance, are committed to the University of Adelaide confidentiality agreement and fully trained and competent in the use of access control;
g) assess each request to ensure its validity and compliance;
h) consider the most cost effective and efficient means to satisfy the request;
i) have control over access, access delegates, and workflows within reasonable expectations; and
j) are committed to personal development and improvements in access control.

11. Access Request Process

Building Access requests for staff, students and co-location partners are submitted by using the on-line Building Access Request form available on the Infrastructure website.

The access request must include sufficient detail to provide access including;
The correct authorising delegate (access delegates' name) for the requested access

a) The cardholders full name, ID Number and or visitor card number
b) The Faculty, School or Department
c) Building and rooms required
d) Access Group/Level if known
e) Expiry date for the access or any special instructions

12. Project Managers, building works and Site Management

Project Managers, Contract Managers, Site Supervisors and Safety Officers are to develop access solutions prior to commencement of the project. Thereafter the site supervisor can request access on a case by case basis.

12.1 Contractor access will not be provided without prior notification in writing. This includes exploratory work for quotes and tenders.

12.2 Tendered Contractors to Capital Projects and Facility Management will work with the Security Access Control Officers to establish access solutions.

12.3 Ad Hoc Access Requests for maintenance, services & events can be provided by a variety of methods and / or means by Security Services following the current version of site Security instructions by the Access Control Officers or Control Panel Operators.

13. Security Officers

Security Officers can check access on a card and attempt to resolve any access issues.
If a card does not work it could be for a variety of reasons including not having access, the card has expired or been voided, damaged or card reader may be inoperative.

13.1 Security Officers are permitted to void lost or stolen cards. Security may also void a card where Security assets (Keys, access passes and valuable assets) are outstanding and the cardholder is not contactable or has failed to respond. Security Officers may also void a card for reasons of misconduct (Section 6).

13.2 Security officers are only permitted to add access to visitor's cards held at the Security Office. This only occurs when an Access Control Officer or Control Panel Operator is not available for programming.

13.3 The use of All Area or All Building access is to be avoided. The basic principle is to restrict access to only what is necessary and approved.

13.4 Expired Contractor Access - Security Officers are permitted to update or extend the expiry date on a Contractor's card by up to a week pending re-induction on Rapid Global.

13.5 Induction needs to be renewed every 12 months. Security Officers may check Rapid Global and verify induction prior to changing end date.

14. After-Hours Access

This section covers After-hours access to bookable spaces and Common Teaching Areas (CTA). Quoting the principle of access control:-

The risk of providing access needs to be balanced against the reasonable expectations of staff and students under the circumstances.

14.1 Whereas a School, Faculty of Department may exercise control over their areas they do not control access to CTA or areas not under their control.

14.2 CTA's are booked on Syllabus Enterprise and are usually electronically unlocked on a time schedule. Some teaching staff may be granted card access to a CTA but CTA access will not be added to undergraduate student cards. CTA's are restricted to ensure no unauthorised access (No access without a booking). CTA's are kept locked unless booked to prevent staff or students from setting up in or altering any empty room they can find. Staff with card access to a CTA may not use the room without a booking and if in the room must vacate it for those that have a valid booking.

14.3 Extra caution needs to be exercised as bookable spaces can be booked by people outside of the University, or booked by University departments for external providers or organisations (Visitors). All visitors must be made aware of and comply with after-hours access and security requirements.

15. Bookings - After Hours and Weekend Access to University Buildings

There are Security requirements for bookings in any building that is normally locked after hours. All people making or taking bookings need to ensure Visitors are aware of these when taking the booking.

The user or person making the booking is responsible for organising security.

15.1 **The building cannot be left unlocked and unprotected, exposing it to risk of unauthorised entry**.

15.2 Options are to **have a responsible person at the door to meet and greet guests.** Only invited guests and people with authorised access may enter. To prove they are authorised they must use their card on the electronic access card reader on the door and get a green light. Security must be advised of any suspect unauthorised person who enters the building.

15.3 Using this option Security can unlock the door whilst it is attended and relock it when people have gained access. A note should be left on the door including a contact number for one of the event organisers for any late comers. Security will not attend to let in late comers.

15.4 Lunch and tea breaks can also be regulated by the same method. Buildings are fitted with push button exits. A person can be stationed at this button to regulate entry or re-entry. **Doors may not be propped open** with chairs or other items as it will damage the mechanisms. Door frame eyes are not to be taped over as it may cause an unnecessary service call.

15.5 **The other option is to pay for a Security Officer to be stationed at the door**. They are not a University of Adelaide Security Officer, rather a private contractor. The minimum charge is for four hours and can be arranged by Room Bookings or

Security on request, two weeks' notice is preferred. An account code is to be provided with the request.

15.6 **In some cases one or more access cards can be made up to provide access**. These can be provided by a School, Department or by Security, advanced notice is required.

15.7 In all cases advise Security of your arrival and departure. Security will not unlock unless there is someone there to take charge of the venue. Telephone **Security on 8313 5990.** Security will usually attend immediately, but 5 to 20 minutes can be expected depending on the circumstances at the time. **Please arrive early to avoid any inconvenience**

15.8 Security provide emergency response and are responsible for a large number of tasks and clients. Most unlocking is electronic and programmed or done over the phone (831 35990). Unless it is urgent, Security will not physically attend, open up early and leave unattended, wait for or stand by for guests to arrive. The organiser, making the booking, is responsible to organise access, meeting and greeting.

16. Building Project (Construction) and Contractor Access

Access needs to be risk assessed with a key and access solution worked out before commencement of works. The use of Building Master Keys and all areas card access is not permitted.

16.1 Contractors cannot turn up at the Security office and request access. This requires some foresight and planning by Project Managers. Written notification of all works needs to be provided in advance and responsible people identified on both the University and contractor side. This is the job of the Site Supervisor, Safety Officer or a delegated person. Even if the work is only exploratory Security need to know the scope of works before providing access. No access without the paperwork.

16.2 All contractors must have completed the University (Rapid Global) online induction and have a University photo ID card before access can be provided.

17. Requests for Access Reports

Access reports can be generated to identify who has access to a door or who has accessed a door over a period of time.

17.1 Access reports over a time period of time will only be generated by Security for a valid incident or crime related reason. This includes, damage, theft, criminal matters or unauthorised access.

17.2 Reports will not be generated by Security for administrative or statistical purposes such as to check on staff or student access over a period of time. These matters should be referred to Human Resources or Student Life.

17.3 Non-Security related reports for access over a period of time may be generated but will be subject to approval and on a user pays basis.

17.4 Security will edit reports to ensure compliance with confidentiality, privacy and secrecy provisions.

17.5 For probity there must be a written request (e-mail communication) for all reports and the request must be from an authorised person (access delegate). In the case of an incident or investigation, the authorised person is the police or head of school.

17.6 A report of who has access to a door (cardholders) can be requested by an authorised access delegate for auditing purposes.

18. Investigation

There are dangers in individuals, departments or schools trying to conduct their own investigation. The initial action is to report the matter to Security. The Security Manager or Supervisors can provide advice and liaise with the appropriate people depending on the seriousness of the matter.

18.1 Investigation should be left to the Police or referred through Legal & Risk. Security can run access reports and view CCTV to provide limited information and do basic investigation, but there is a point at which we may hinder a police investigation or subject ourselves to litigation.

18.2 For reports or CCTV to be released to Police, Security will require a SAPOL Tasking number (SAP), warrant or subpoena.

18.3 Access Reports released to an Access Delegate, Manager or Head of School may not be released to a third party without express permission by Legal & Risk.

18.4 All criminal matters must be referred to the Police. Internal staff or student matters should be referred to Human Resources or Student Life.

19. Door Programming

The objective of access control is to regulate access and to ensure that unauthorised access is prevented. This is for the safety and security of all. Access Control is about supporting the life-cycle of user access until the time when no further access is required.

The risk of providing access needs to be balanced against the reasonable expectations of staff and students under the circumstances.

19.1 The University by its location, adjacent the City of Adelaide and being a walk-through to the River Torrens and North Adelaide, is both accessible to the public, on public walkways, and vulnerable to criminal or opportunist activity.

19.2 **Public Areas:** The University has many what might be called public areas where people can walk into buildings when open. These include building entrances, Hub Central, libraries and any performance venues or teaching spaces. Lockable doors are used to prevent access to areas that are private or restricted. However, in some buildings the absence of lockable corridors allow people to obtain quite extensive access.

19.2 Whenever new building works or modifications are made Project Managers should ensure security improvements are made to compartmentalise or restrict unauthorised access using access control doors.

19.3 In keeping with sections 14 to 15 ‘After Hours Access’, doors are programmed in accordance with the risk, given the information available at the time. This will change from time to time. Factors include Core Hours, **Common Teaching Area times (CTA)** or holidays, seasonal changes, events, threats and criminal activity in the area.

19.6 Currently CTA is aligned to Core University hours (7.00am to 7.00pm Monday to Friday) except for the summer vacation (December to February) and partially during the mid-semester break where areas are programed to be closed, on card access

only. A risk assessment is made against each teaching space and public space during vacation periods.

19.7 Generally any building which has a booked CTA will be programmed to be open to give access to the teaching venue from 7.00am to 7.00pm Monday to Friday. Openings for buildings without CTA may vary down to standard business hours 9.00am opening to 5.00pm close or less. Building hours will be negotiated with the teaching or business units occupying those buildings. Where there are multiple occupants the risk assessment method will be used. Openings outside of those hours are covered by sections 14 to 15 After-Hours Access.

19.8 Requests for Programming (Time schedule variation) must be in writing (email) from an authorised person (Access Delegate or Manager). Only one time schedule modification can be made for a door at a time. Varied schedules cannot be banked up over several months. A reminder must be sent for each time schedule modification.

20. Event Management.

For large events a lead time of 8-12 weeks is required. This is to prepare an Event Management and Security Services Plan. The aim of this plan to minimise the disruptive effect on staff and students for normal work, teaching and research.

20.1 A large event will require safety inductions, University ID cards and programming of card access in advance of bump-in.

20.2 A traffic management plan must be prepared by the event organiser in liaison with University representative as appointed by the Director, Customer and Support Services.

20.3 Liquor licencing approval may be required, where applicable, within University Policy and legislation. This includes employment of Security Officers licenced to provide security for the Responsible Service of Alcohol (RSA).

20.4 It is the responsibility of the event organisers to ensure regulations are complied with for the supply of sufficient toilets, water and first aid facilities.

20.5 Programming may be required to ensure University Staff and Students suffer minimal disruption. Where significant programing is required it will be will be on a user pays basis.

21. Access Requests for Student, Staff or Visitors Cards

With reference to Sections 8 to 11 of this policy (Access Delegates and requests). When requesting access through https://www.adelaide.edu.au/infrastructure/campus-services/build-grounds/access/ or buildingaccess@adelaide.edu.au. There is a choice of Staff, Student, Visitor, Contractor or one of the co-location partners.

21.1 Students must be enrolled for their card access permissions to function. **If a student does not enrol by the end of February (the following year) their building access will expire.** A student's end date cannot be extended by the Access Control Office as it is determined by the student's enrolment. Enrolment for undergraduate and postgraduate coursework students is online or through the Adelaide Graduate Centre for Higher Degree Research (HDR)

21.2 For students who need to complete work when no longer enrolled particularly HDR students who have submitted their thesis the faculty, school or business unit may request (and pay for) a **Visitor's card**. There are two visitor card options, a Departmental Visitor or a Photo Visitor Card. These are arranged through Ask Adelaide using the ID Card Request form.

21.3 Visitor's Cards have an annual end date and do not come with access. When the Visitor card has been issued by Ask Adelaide the online building access request can be completed and authorised by an access delegate.

21.4 **Contractor** cards are arranged through the Rapid Global online induction and then access is requested through the Project Manager or Site Manager to Security. Security Services manage contractor access directly.

21.5 **Students working as staff**. Where a staff appointment has been made through Human Resources (HR) to employ a student a new card identity will be made through the Peoplesoft system. The new staff member (full time or fixed term) must collect their card from Ask Adelaide (casual staff will be required to request and pay for a card). Staff building access can then be requested for the staff card. The Staff card must be used for staff purposes and the student card for any enrolment related purposes. Staff access should not be added to a student card.

21.6 **Requesting access for a new Staff member**. Access can only be assigned for a new employee (Full time, fixed term or titleholder) 5 days prior to their commencement date. There is no benefit in submitting a building access request until five days before the staff member's commencement date.

22. Restricted Areas. (Excludes plant alarm monitoring and duress alarms)

For an area to be classified as restricted, requiring monitoring, certain conditions must be satisfied. Communication is essential to ensure the client, project manager and installer speak to Security prior to installation to establish expectations and costs. Security will not automatically monitor or respond to any alarm at any location.

22.1 All risks associated with the area must be provided to Security along with the names of three people as points of contact with mobile telephone numbers, available 24/7 before the installation can be completed. It is the responsibility of the primary point of contact and/or access delegates to ensure security are updated of any risks or incidents in the area.

22.2 Renaming of the Alarm Point and Access Level names must include the restriction. The location on SiPass plan must be correctly identified and highlighted and tested once the alarm class has been created by Security.

23. Safety Audits

Safety Audits are to be conducted in a systematic method via the appointed access delegates. (Managers, Safety Officers, etc., are to go through the Access Delegates whose role it is to appoint and monitor access)

22.1 One or two access delegates must be appointed as a single point of contact for all access adding, removing and auditing. It is their responsibility to initiate an audit of the area annually.

Only the access delegate can request a report of who has accessed the area over a period of time. This must be incident related only and narrowed down to a short search.

22.2 The Security and Access Control officers will determine the best method of obtaining data and ensuring compliance with privacy and related legislation. Reports and investigation will only be conducted in relation to a reported incident, not for analytical, statistical or Human Resource related matters.

22.3 Any non-incident related request will be on a user-pays basis outsourced to an appointed private contractor.

24. Review of Access Control Policy

This Policy will be amended by the Access Control Team as required.

The next annual review due July 2020