Security Services - Access Control Policy

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.
This Policy is only for building access added to University of Adelaide ID cards issued by Ask Adelaide including Staff, Students, Visitors, Contractors and Co-Location Cards (AWRI, CSIRO, PIRSA & SARDI). Cards issued to staff and students are provided with a standard set of access permissions and is regulated by the staff member's employment or the student's enrolment through the Peoplesoft import. Contractor Card Issue is facilitated by the Rapid Global import. Ask Adelaide provide replacement cards at cost. Security do not print cards.

Security Services, Access Control provide all building access.

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**. Specifically, 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.

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 reasonable time. Owner being the Faculty, School, Division or entity that has been given lease or authority over the premises. This is generally allocated by Space Planning & Capital Projects.

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**.

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.

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 in any way.

Access Delegates are to be appointed from all University entities to authorise access for professional staff and students. Authorisation must be in writing by a head of school or department and a sample signature, personal and electronic supplied.

Access Delegates for Staff & Students:
An Access delegate must be a currently employed member of staff

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 Access Controllers

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.

Rules

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

An Access Delegate must:

- satisfy themselves as to the identity of the person requiring access, their enrolment or employment and the validity of their access need;
- have full knowledge of the area they are giving access to, the risks and rules associated with the area;
- complete the access request with sufficient detail for the request to be processed;
- always notify access control as soon as possible when circumstances have changed and access needs to be removed. E.g. staff end of employment or transferring to another area within the University of Adelaide.

An access delegate must not:

- request access to an area not under their control,
- have someone else submit the request on their behalf,
- release their e-mail password or electronic signature for the use of another or
- forward an access request without due prudence.

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.

Access Control Officers liaise with a number of clients to develop access systems:-

- Capital Projects for new building installations and alterations.
- Schools and Departments through Access Delegates to provide card access
- Ask Adelaide for new and replacement cards.
- Service Delivery and contractors to develop access solutions for projects and maintenance.

Access Control Officers (cont'd)

- are committed to the learning and understanding of Access Delegates and the development of access control;
- have a suitable security clearance, be committed to the University of Adelaide confidentiality agreement and be fully trained and competent in the use of access control;
- assess each request to ensure its validity and compliance;
- consider the most cost effective and efficient means to satisfy the request;
- have control over access, access delegates, and workflows within reasonable expectations; and
- are committed to personal development and improvements in access control.

Access Request Process

Access requests for staff and students are submitted by using the on-line Building Access Request
The access request must include sufficient detail to provide access including;

- Access delegates name, contact number and electronic signature
- The Supervisor or contact, and number if it is not the access delegate
- The Department or School
- Requestor's full name and card or ID number
- Building and rooms required
- Access level if known
- Expiry date for the access or special instructions

Project Managers working through Site Supervisors are to develop access solutions prior to commencement of the project. Thereafter the site supervisor can request access on a case by case basis.

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

Regular Contractors to Service Delivery will work with Security Access Control Officers to establish access solutions.

Ad Hoc Access Requests for maintenance, services & events can be provided by a variety of methods and / or means.

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.

Security Officers are permitted to void lost or stolen cards. Security assets that are outstanding and the cardholder is not contactable, has failed to respond or for reasons of misconduct which may result in the removal of access.

Security officers are only permitted to add access to visitor's cards held at the Security Office. This only occurs when an Access Control staff member is not available.

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.

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.

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