University of BRISTOL

Policy and procedures

Buildings access control

Release: Issued
Date: 07 July 2010

Owner: Jerry Woods
Head of Security
Security Services

Author: Ralph Ballon
Information, Processes and Systems

Document version 1.0

1 Document control

Document Location

H:\ips programme office\Business Cases\University Card\Project file\Policy\Policy Statements\Access Control Policy v 0-5.doc

Contributors (Policy Group)

Guy Gregory	Personnel/staff (Chair)
Jayne Storey	Students
Jerry Woods	Security/contractors
Jennifer Scherr	Library
Tim Phillips	Data Protection
Christine Fraser	Faculty/Department Management
Paula Coonerty	Faculty/Department Management
Ralph Ballon	Project Manager

Document Owner
Head of Security Services

Revision History
Date of this revision: 07 July 2010

Revision date	Summary of Changes	Version	Marked ?
11 June 2008	Ist draft Issue to Steering Group	0.3	
26 June 2008	Draft Issue to UPARC	0.4	
3 Sept 2008	Course restrictions statement amended	0.5	
6 May 2010	Pre-production update	0.6	Y
24 May 2010	Minor corrections	0.7	
1 June 2010	Corrections to sections 7 & 9	0.8	Y
6 July 2010	First issue	1.0	

Approvals
This document requires the following approvals.

Name	Date issued
University Card Steering Group	25/6/08
UPARC	08/07/08
Data Protection	25/05/10
Freedom of Information	25/05/10
Secretary's Office	25/05/10
Access Control Steering Group	25/05/10

Contents

2 Introduction

This document defines the management policy and procedures for the Access Control System (*ACS)* ; both for the initial deployment; and as a guide for future system development.

Please note. During the validity of this policy document the Card Services department; its roles and functions; will be managed on a temporary basis by Library Membership Services, as described in Section 3.

3 ACS Management

The following stakeholders are responsible for the management and operation of the ACS.

3.1 Bursar's Office

The Bursar has primary accountability for the ACS.

3.2 Head of Security

The Head of Security is accountable for:

- Developing ACS services and functionality
- Agreeing and setting default levels of ACS entitlement for each category of cardholder
- Authorising devolved visitor access management responsibilities
- Liaison with the Card Services manager
- ACS problem resolution and arbitration
  Students should follow the student grievance procedure:
  http://www.bristol.ac.uk/secretary/grievances/leaflet.html
  staff should follow the staff grievance procedure:
  http://www.bristol.ac.uk/secretary/grievances
  Other users should contact their Sponsor.

3.3 Security Services

Security Services are responsible for:

- Day-to-day monitoring of the ACS
- Out of hours operation of the ACS help line
- Access revocation, temporary blocking, fraud and security control; for individuals, groups or buildings; as instructed, and without instructions in emergency situations
- Manage individual biometric controls
- ACS problem management
- ACS and hardware maintenance
- ACS configuration

3.4 Card Services

Card Services are responsible for;

- Problem management, during normal office hours
- Liaise with Security Services and Information Systems to resolve access control issues
- Access revocation, blocking, fraud and security control

3.5 Academic, Faculty and Buildings managers

- Define building and service access requirements to Security Services
- Manage visitor access and reception services
- Manage requirements for biometric controls
- Modify local access and service controls for groups and individuals

3.6 Building receptions

Responsible for issuing and management of re-usable Visitor *U*Cards.

3.7 Information systems (ISYS) service management

Information systems provides:

- Network support and maintenance
- ACS application support and maintenance
- ACS database administration and backup
- Operational usage reports

3.8 All Staff

For visitor management, University staff are responsible for visitor registration prior to arrival at their respective reception area.

- Notify arrival reception using either, hardcopy/e-mail notification or OnGuard Visitor management on the intranet.

4 ACS Administration

4.1 Operating hours

The ACS will operate 24 x 7 x 365, although some buildings may have restricted access on closure days.

4.2 Administration

Security Services are responsible for day-to-day ACS administration including:

- The operation of the ACS helpline (out of hours). (Card Services operate the help line during normal office hours)
- Access control blocking, fraud and security control.
- Liaison with Card Services and ISYS service management
- Monitoring ACS hardware support and maintenance (excluding IS systems)

5 Access entitlement

5.1 All ACS users

Where buildings have egress controls in place, unless specified otherwise, egress is always enabled for *U*Card holders. If the *UCard* holder was not entitled to be in the building however, this will set an alarm condition requiring investigation by Security Services.

5.2 Staff

Staff are salaried members of the University and registered on PIMS.

Staff can access all *ACS*-controlled buildings during normal opening hours, except for buildings where biometric readers are fitted or in pre-defined higher risk areas.

5.3 Students

Students are members of the University registered on SITS and engaged in a recognised period of full or part-time study.

In addition to public areas, students may only have access to buildings, zones or rooms required for their course. For high-risk areas additional access controls, e.g. biometric enrolment, may be also be required.

Note. It is recognised that course-based access control is a longer term objective. During normal opening hours, and as part of a phased introduction, all building main entrance points will be classified as accessible to all students, regardless of course registration. Managers wishing to maintain a higher level of security however, (e.g. in the Medical School) or for health and safety reasons, may still wish to restrict student access during these times.

5.4 Visitors

A visitor is anyone, not a member of the University, requiring access to University premises or services.

As well as Security Services other University staff, e.g. building managers, with devolved authorisation levels (assigned by Security Services) are able to set or amend building access rights for various categories of cardholders.

5.4.1 Day Visitor (valid for 1-5 days)

Visitor Cards are re-usable cards issued at the Card Services Desk or at reception desks around the University. Cards are only issued to visitors who have been pre-registered by a member of staff and are valid for a single building/faculty/area.

- Personalisation is not required for a Day Visitor card
- Day Visitor status lasts for up to 24 hrs, after which the card will become inactive
- The Day Visitor card can then be re-activated for 24 hours at a time. Actual access rights are controlled by building managers, e.g. front doors are only open to Day Visitors 08:00 – 18:00.
- Visitor cards are returned to the issuer for re-use.

5.4.2 Associates of UoB

This group includes Honorary academic and Honorary non-academic users.

5.4.2.1 Honorary Academic status

Honorary Academic status must be sponsored by a senior member of the academic staff (e.g. head of department) and the cardholder details registered on PIMS.

Honorary Academic status automatically receives Library membership.

Honorary Academic status may be set for up to 12 months by the Sponsor, after which the card will become inactive unless sponsorship is renewed

5.4.2.2 Honorary Non-academic status

Honorary non-academic status must be sponsored by a senior member of staff (e.g. head of department) and the cardholder details registered on PIMS.

Honorary Non-academic status may be set for up to 12 months by the Sponsor, after which the card will become inactive unless sponsorship is renewed.

5.4.3 Library services – public membership

Library membership Services are responsible for the authorisation and administration of external Library Members. This includes record creation on the ACS and the issue of Library Member or Library Visitor *U*Cards.

Library membership services have devolved access management responsibilities for all sites where libraries are located.

6 Access control

6.1 Door controls

6.1.1 Entry control

All buildings on the UoB estate will have contact-less (proximity) access control via an enabled smart card.

6.2 Biometric controls

Fingerprint readers will be used to control access to/from sensitive areas and in applications where rigorous authentication is required.

Where appropriate, biometric reader functionality will also be incorporated into portable readers.

6.2.1 Egress (exit) control

In most locations having a *U*Card will enable egress by default. An emergency exit control (green 'break-glass' switch) will also be fitted.
User specific egress control may be required in areas of high sensitivity. In these cases neither the *U*Card exit or emergency exit control will be available. An emergency call number will be provided instead, to contact Security Services.

6.3 Buildings opening hours

Standard access times will apply to all University buildings, although these may be modified locally by building managers. The following describes the default times applicable to University members.

6.3.1 Normal opening hours

08:00 – 18:00 Monday to Friday (may be building dependant)

- Entry and exit is controlled via the *U*Card.
- Day visitors are issued with a reusable visitor card from a controlled set reserved for the purpose
- Buildings not normally accessible by the public may have other restrictions during these hours

6.3.2 Outside normal opening hours

At other times

- Most buildings are 'locked down' to a single entry/exit point after 18:00.
- Entry is via an authorised *U*Card (biometric controls may also apply)
- Egress is via a *U*Card

6.3.3 Alarm reporting

A warning alarm will notify Security Services of any of the following conditions:

- 3 invalid attempts to access/egress a building
- Door held open for longer than 60 seconds, but may vary for some situations and for disabled users
- Forced door
- Egress with an unauthorised *UCard* (i.e. the cardholder is not authorised for that building, or at that time)
- Use of an emergency exit switch

6.4 Biometric control

Biometric readers will be used to control access to high-risk areas.
Recording biometric data onto a *U*Card is a function of Security Services or the authorised building manager. As biometric data is not stored on the ACS database a re-issued *U*Card will require re-recording (enrolment) of biometric information.

7 Disabled access

7.1 Accessibility statement

The ACS system will take into account the requirements of *U*Card users with disabilities. ACS development will follow the University's disability in the workplace policy and guidelines: http://www.bris.ac.uk/personnel/policies/disability-policy.html

and recommendations from the RNIB Scientific Research Unit, Tiresias
http://www.tiresias.org/index.htm

The Security Services and Card Service managers will review disability arrangements with services providers annually.

7.2 Modifying access control

By agreement with the *U*Card user, the *ACS* can include:

- A data flag to indicate that further time to complete the action or transaction is required; e.g. passing through a barrier, or using a cash loading facility.
- An alternative method, where appropriate, for verifying identity in high-risk areas.

7.3 Data Protection Act

Any preferences specified by disabled users will only be made available to authorised University staff in accordance with the Data Protection Act. In particular, information relating to an individual's health will usually constitute *sensitive personal data* under the Data Protection Act, and will therefore be subject to additional processing safeguards.

7.4 ACS readers

The height of readers, use of prominent signage, entry/exit times, and emergency procedures must be considered in the development of the ACS.

In order to ensure readers are accessible to all *U*Card users, as far as possible the ACS system will:

- Use a consistent user interface for all readers, which do not rely on card orientation
- Identify readers with clear *U*Card signage
- Place readers at the same height and position to enable a blind person to locate readers reliably.
- Position the readers at a height which can be conveniently reached by all *U*Card users

7.5 Cardholder Support

If a disabled user has any issues or suggestions related to the *ACS* they should contact the Card Services manager during normal office hours or Security Services at other times.

7.6 Emergency procedure

The procedure to be followed should be described in the *U*Card user's PEEP (personal emergency escape plan), and agreed with Health & Safety Office and Security Services.

8 Business continuity

Security Services will liaise with the ACS service provider and ISYS services management to resolve ACS system failures.

A regular review of business continuity issues, between the stakeholders, should take place at least quarterly so that improvements can be fed back into system management.

Information Systems service management will provide monthly reports on the ACS to the Security Services manager:

- ACS management system issues and down-time
- Application and database support time and activity

The follow describes potential business continuity problems and the likely impact.

8.1 Network or server related

Local (building) controllers retain sufficient *U*Card user information to enable access/egress during a network or server outage. New or updated *U*Card user information however, will not be available during this period.

8.2 Power failure

Building access control will continue to function during a loss of building power via battery backup within the local building controller. There is sufficient battery power to control access for 24 hours.

8.3 Complete failure

During a period of complete power failure (where battery power has been exhausted), or the controller has malfunctioned, or doors are in a fail CLOSED situation, manual inspection of identity cards may be required for buildings access control. This will be co-ordinated via Security Services.

8.3.1 Normal opening hours

If complete failure occurs Monday – Friday 08:00 - 18:00 All buildings, with the exception of high-risk buildings, fail open and the rest will fail CLOSED.

8.3.2 Outside normal opening hours

Based upon the building risk category, outside of normal opening hours, most building access points will fail CLOSED. Most doors also have an emergency (break glass) override to manually open the door as a safety feature. Where an emergency override is not installed an emergency call number will be provided to contact Security Services.

9 Information Management

9.1 Data protection

- Personal data will be processed in accordance with the Data Protection Act 1998
- ACS system managers and administrative staff will ensure that ACS data is only used for its intended purpose.
- Personal usage information will not be extracted from the ACS or shared with other University systems without the explicit consent of the Secretary/Director of Legal Services or his/her representative. (See also 9.3 Personal access reports)
- Unless specifically requested, for legislative or academic reasons, personal usage data will be removed from the system after 90 days.
- Access preferences, for disabled users, may only be made available to an authorised member of University staff.
- Information relating to an individual's health will usually constitute Sensitive Personal Data under the Data Protection Act, and will therefore be subject to additional safeguards when processed.

9.2 Personal access reports

Personal access information will not routinely be divulged to any third parties. Typical reasons for requesting this information may include; a disciplinary investigation; after a crime has occurred or because of health and safety concerns. If approved, the Secretary/Director of Legal Services will inform the Security Services manager to release the requested information to the enquirer.

UCard users can make a subject access request for their own usage information via the Secretary's Office

In an emergency Security Services may also make use of personal access reports, as part of its crime prevention and safety role, without prior authorisation from the Secretary or Director of Legal Services.

Personal access information will not be divulged to third parties unless the cardholder is the subject of a Data Protection Act request by a relevant external agency (e.g. the police).

9.3 Freedom of Information

All freedom of information requests should be submitted to the University's Information Rights Officer, or his representative.

10 Definitions

The following definitions apply only to the ACS management system.

ACS Authoriser	A staff member able to register one or more types of visitor and/or grant service user rights.
Contact-less reader	See proximity reader
Data **in** the card	Information stored on a smart card chip
Data **on** the card	Information printed on a *U*Card
Egress control	Buildings exit management
Entry control	Buildings entry management
Honorary academic staff	Honorary academic staff are registered on PIMS and have the same (default) access right as staff.
Honorary non-academic staff	Honorary non-academic staff, (contractors, consultants, agency staff, etc) are registered on PIMS but have no access rights, by default.
Proximity reader	A device using radio frequency identification (RFID) technology to read information on a 'smart card' without any contact between the two.
Sponsor	Individual OR system (e.g. PIMS or SITS) required to register a cardholder prior to *U*Card issue and setting access rights
Staff	Staff are automatically registered via the PIMS personnel system. Staff entitlement supersedes other entitlements.
Student	Students, undergraduates and graduates, are automatically registered via the SITS student system.
*U*Card	The brand name for the University smart card management system
Visitor (Day)	A Day Visitor is anyone (not a member of the University), authorised by a member of staff to access a building or a service for a max. period of 24 hours. Card expiry is renewable daily and is usually limited by local buildings access settings, e.g. Mon – Friday 08:00 – 18:00.