DIRECTORATE OF ESTATES AND FACILITIES

PROCEDURE AND INFORMATION MANUAL

EPM PM11 – Standard Access Control Specification

Document Originated:	January 2005	**By:**	Roy Smith
Issue Number:	1	**Number of pages:**	5
Approved by EMG:		**Status:**	Working Document
Last revised:	October 2018	**By:**	**Policy & Procedure WG**
Next revision:	October 2019	**By:**	John Ashton

1.0 Purpose of the document

1.1 This document sets out the standards to be adopted for all electronic access control systems across the University of Manchester property portfolio to enable design teams to specify appropriate systems to be incorporated on new build and refurbishment projects.

2.0 System Objectives

2.1 The principle objective of the Access Control System is for the Directorate of Estates and Facilities Security department to have full control over the University of Manchester out of hour's doors, and wider management of selected internal doors by using the TAC Continuum web server browser graphics page.

3.0 Existing University system

3.1 The University's Networked Swipe-card Access Control system comprises of a Windows 2008 R2 Enterprise Fileserver loaded with Windows SQL 2008 server database.

3.2 A Windows 2008 R2 Webserver with a cut down version of TACs Continuum version 1.94 SP 1 program loaded with a twenty five concurrent user license dongle.

3.3 There are four TAC Continuum 1.94 SP1 Cyber stations running Windows 7 University image, located as below:

- Two located in the Access Control Managers Office which is the Secondary Access Distribution Server Cyberstation1, and one back up, Cyberstation4,
- One located in the North Campus Security lodge Cyberstation2
- One located in the Precinct Control room which is the Primary Access Distribution Server Cyber station MT.

3.4 The system utilises a custom ABA2 Proximity (Desfire) dual function card, which can be read by the access control systems on campus.

3.5 The ABA2 magstripe and the Proximity card can also be used on the ASSA swipe-card system without any detrimental effect (an additional interface will be required to fit a proximity reader to this system).

3.6 Swipe Cards also have the facility to access the University Library's turnstiles through the use of the barcode on the front of the card.

4.0 System Requirements

4.1 All new installations / buildings shall incorporate the TAC Continuum access control system, and shall comply fully with the current Building Regulations and the Design Team Guide especially in regard to BS 7273-4:2007: Code of Practice for the operation of Fire protection measures, Actuation of release mechanisms for doors.

4.2 All Out of Hours door Controllers to the building should be of the type Schneider Electric ACX 5720 Controller or the latest version of, this can control up to 4 doors (read in read out), and can also hold 450,000 personnel records.

4.3 Areas requiring multiple card access should use the type Schneider Electric ACX 5740 Controller or the latest version of

4.4 The ACX 5720 and 5740 will each require a dedicated network connection on the University LAN, an IP address will then be allocated to these controllers from within the swipe card system dedicated V-lan.

4.5 There are a number of older access control systems controllers on the Continuum system, namely TAC CX 9900 and TAC CX 9940 these can still be expanded upon (up to 32 doors) used in conjunction with the TAC AC1 plus FT Door access controllers and cable lengths can be up to 600m away from the main controller.

4.6 Access control contractor must be BS EN ISO 9001:2000 registered and a member of the British Security Industry Association.

5.0 Locks

5.1 The use of Level 3 or 4 Magnetic Locks, Mortise type Electric locks or Electric strikes with a holding force of between 7 and 10kN BS EN 50133 -1 shall be used for the Main front doors of buildings.

5.2 The slim-line Level 1 and 2 Magnetic Lock versions which have a holding force of 3 to 5kN can be used on internal doors.

5.3 Clearance heights on all doors shall be a minimum of 1981mm after the Magnetic lock has been fitted, i.e. the Magnetic Lock must not protrude down below this height.

5.4 No shear type locks to be fitted

6.0 Readers & Associated Equipment

6.1 HID SmartID S10 readers shall be used. The University has its own dedicated HID part number, HID SmartIDS10 02SMR-5735.
This reader being pre-configured to read the Universities unique card format and can only be supplied with the University Of Manchester's express permission. Any other reader can be integrated with the access control system but care must be taken to ensure this is fit for purpose and is capable of reading the correct card-format.

6.2 KGG200SG Break Glass Unit to be fitted with Perspex cover at each door.

6.3 'Request to Exit' button to be fitted at each door.

6.4 Fire Alarm relay to be fitted to interface with the Door Controller, to operate that when the Fire Alarm is raised the power is dropped to the locks and the doors fail safe open. This satisfies the regulations mentioned above.

6.5 In close proximity to the ACX 5720/5740 Controller a 13amp (un-switched) Fused Connection Unit is required for the power supply along with the Fire relay, and a dedicated live network point.

7.0 Other Access Control Systems

7.1 High Risk Areas such as Cat 3 Labs, Radio Active Labs, Laser Labs all warrant special consideration for Access Control Systems. Policy for all high risk areas shall be agreed as early as possible in the design phase with both Faculty staff and the Access Control Manager.

7.2 At present the Car Park system is a standalone system managed exclusively by the card park permit office but with the same specification as the normal building access control system (continuum 1.94).
ACX 5740/5720 controllers with HID SmartIDS10 02SMR-5735 readers shall be used on entry and where appropriate exit barriers, and the use of Anti-pass back on the access system is to be initiated to stop tailgating etc.

7.3 Access control to specific areas as identified by Estates will be via the Simons Voss wireless locking system. This system uses wireless door handles and cylinders that are battery operated and communicate wirelessly using a network enabled wireless gateway. This system operates on a stand-alone database and is managed and administrated by the Estates CSU team. Additions to the system and access requests should be made to the relevant person or project manager within Estates. Simons Voss specifications can be sort by specialist contractors or agents who are licenced Simons Voss installers; a list is available if required.

7.4 ASSA Aperio is a wireless solution that can be integrated into the campus wide Continuum access control system. This uses wireless door handles and cylinders that are battery operated and communicate wirelessly using a networked hub located close to the door(s). The system uses the conventional student/staff card for access and access can be enabled and disabled by an appropriate person via the webclient software package. This system is suitable for low volume doors or where fitting cables may be difficult. Advice should be sought before installing this product and should only be installed by ASSA Aperio specialist contractors licenced and trained by ASSA Abloy.