University of St Andrews

Access control specification

Document type	**Policy**
Scope (applies to)	Public
Applicability date	14/02/2024
Review / Expiry date	11/02/2025
Approved date	14/02/2024
Approver	Chief Information Officer
Document owner	Associate Chief Information Officer (Cyber Security and Resilience)
School / unit	IT Services
Document status	Published
Information classification	Public
Equality impact assessment	None
Key terms	Information technology/Digital standards
Purpose	The University of St Andrews Access Control Specification to afford the University reliable, performant and standards

Version number	Purpose / changes	Document status	Author of changes, role and school / unit	Date
1.03	Items added and formatting adjustments.		Pam Reid Campus Card Services Supervisor	18/09/23

1. Objective

The University of St Andrews Access Control specification is designed to afford the University reliable, performant and standards compliant data infrastructure.

2. Application

This specification must be adhered to in all access control installation works by or for the University of St Andrews. No other specification, howsoever obtained, is valid for any access control installation works at the University of St Andrews. The version of the specification used for works shall be the latest version published at the date of commencement of the cabling works. [1]This specification is applicable to new builds, refurbishment and work on existing installations

Deviations from this specification are not expected and should only occur where there are technological advancements and following authorisation from the Campus Card Services Supervisor. Unauthorised deviations will not be accepted or signed off and may cause a delay or additional cost to a project.

3. Preliminary information

3.1 Prior to work starting, contractors must report their presence on site to Estates Small Works Team and notify the Campus Card Services Supervisor (01334 462755). Contractors must also, before commencing any works, have received an Asbestos pack/brief from the University or their main contractor. If any contamination is found or suspected in any location in the course of works, work should be halted pending confirmation from Estates (01334 463999). Each contractor should also be familiar with the University's Health and Safety policies. Advice may be sought from Estates staff in case of any doubt.

3.2 Advice upon any aspect of this specification may be sought from the following personnel in IT Services:

Pam Reid, Campus Card Services Supervisor – 01334 462755 – par@st-andrews.ac.uk

3.3 If a contractor is in any doubt as to what action to take, or what product to use, or if any item they are working on is omitted from this standard, advice must be sought from the above personnel, and a positive response received before they proceed. It will not be acceptable afterwards to state that either this standard was not clear or did not cover any matter.

3.4 All access control installation works must be carried out by: -

- Manufacturer approved contractors.
- Use materials approved by manufactures (listed below) and marketed under their primary brand.
- The fitting contractor must be suitably manufacturer approved to provide a manufacturer/insurance-backed warranty of a minimum of 12 months.

Deviation from this specification is not permitted, unless agreed by one of the personnel listed above, in writing, on university headed paper.

3.5 It is the responsibility of the contractor to ensure that all quotations for access control installation + works, howsoever provided to the University of St Andrews, adhere to this specification, and that if any rectification works are required to bring an installation in-line

with this specification, the cost of these works shall be borne by the fitting contractor. Please see sign off at the bottom of this document.

3.6 Provision should be made for the contractor to install final connections from cabling to active equipment. Please note: **Access control cabling cannot use the same containment as the data cabling.**

3.7 For all cabling specifications and requirements please see the Universities Data and Telecom Cabling Specification.
https://www.st-andrews.ac.uk/policy/information-technology-digital-standards/internal/data-and-telecommunications-cabling-specification.pdf

3.8 All works must be carried out to relevant British and International standards. The latest revisions of the following (and other) standards may be applicable, and industry best practices which exceed the requirements of these standards must be followed throughout:

EN179 Abloy EL420, EL520, EL560 & EL561
EN1634 -1 Abloy EL420, EL520, EL560 & EL561
EN61000 -6 -1 Abloy EL420, EL520, EL560 & EL561
EN1303 (cylinder) Abloy EL420, EL520, EL560 & EL561
EN14846 Abloy EL420, EL520, EL560 & EL561
BS EN1125 Dormakaba 9000 series
EN16005:2012/AC:20015 Automatic Swing Door Operator DFA 127 IN (inverse)
DIN18650-1/-2:2005 & 2010 Automatic Swing Door Operator DFA 127 IN (inverse)
BS EN1670 Winkhaus autoLock AV2 + AUTOMATIC Multi-Point Locking System

Access Control Lock Specification

Standard Door - Read In only Standard Door - Read In/Read Out	Abloy EL560 Electric Lock Abloy EL561 Electric Lock
Standard Double Leaf Door Opening Leaf Read In/Out Static Leaf Door Or Both leaf's of doors open	 Abloy EL560 Electric Lock Dormakaba 9000 series Push Panic Bolt (Mechanical) Dormakaba 9000 series Push Panic Bolt (Electric)
Standard Double Leaf Door Opening Leaf Read In/Out Static Leaf Door Or Both leaf's of doors open	 Abloy EL561 Electric Lock Dormakaba 9000 series Push Panic Bolt (Mechanical) or Flush Bolts Dormakaba 9000 series Push Panic Bolt (Electric)
Standard Double Leaf - **Fire Exit Door** Opening Leaf Read In Only Static Leaf Or Both leaf's of doors open	 Dormakaba 9000 series Push Panic Latch (Electric) Dormakaba 9000 series Push Panic Bolt (Mechanical) or Flush Bolts Dormakaba 9000 series Push Panic Bolts (Electric)
Standard Disabled Door - Automatic Operator	Automatic Swing Door Operator, DFA 127

Standard Disabled Double Leaf Door – Operator + Access Control - One door operation Opening Leaf Read In Only Static Leaf Or Both leaf's of doors open	Automatic Swing Door Operator, DFA 127 Abloy EL520 Motorised Electric Lock Dormakaba 9000 series Push Panic Bolt / Latch or Flush Bolts Dormakaba 9000 series Push Panic Bolts (Electric)
Standard Disabled Fire Exit - Automatic Door Operator + Access Control – 2 door operation.	2 x Automatic Swing Door Operator, DFA 127 Dormakaba 9000 series Push Panic Bolts (Electric)
Standard Single Leaf Disabled Automatic Operator Door Lock	Abloy EL420 or Abloy EL520
Internal Aluminium Glazed Door	Abloy EL460
External Aluminium Glazed Door	Winkhaus autoLock AV2+ AUTOMATIC Multi-Point Locking System

Access Control Reader Specification

Standard Door	Desfire HID SE Reader (BLE)
Restricted Access Door (High Security)	Desfire HID RSK40 Card + Pin Reader (BLE)
Student Bedroom/Studio/Flat Door/kitchen Door	APERIO E100 BLE V3 HF 40-50 No Cylinder

4. Commissioning

4.1 Provision should be made for the contractor to install doors onto the ARX database

Device Outlet details

- Door location
- Door controller type LCU9016 or LCU9101
- Data point outlet number
- Door controller MAC address

4.2 **Override key**

- Contractor to have during installation then handover to Security & Response Team once installation is complete.

4.3 **Handover checklist**

Item	***Criteria***	***Yes/No***
Door	Type of doors meet the brief – Single/Double leaf etc.	
Card Readers	Correct model of readers installed at each door.	
Locks	Correct lock mechanisms in use.	
Door Controller	Correct number of door controllers installed.	
Commission information	Correct information submitted to the networks project patching schedule.	
Approved by:		
Date:		

Version number	**Purpose / changes**	**Document status**	**Author of changes, role and school / unit**	**Date**
1.02	update		Pam Reid Campus Card Services Supervisor	22/03/23
1.03	Add checklist. Link to data spec. Handover section.		Pam Reid Campus Card Services Supervisor	18/09/23