University of Cincinnati Access Control Specifications

Updated10-29-19

General Information

The University of Cincinnati utilizes a Lenel OnGuard system for access control. The OnGuard system is used to control exterior and interior doors on all UC campuses. The OnGuard system is not used for housing or Tangeman University Center. Housing and TUC are controlled by a Blackboard access system. The below standards are for buildings controlled by the OnGuard system.

Exterior Doors

All building perimeter doors are controlled by the University access control system.

Main and service entrances to buildings will be provided with card access.

Secondary entrances that must be open for public use during normal business hours will be provided with electric locks.

Emergency exits are monitored for doors being propped open, and have no exterior hardware.

Doors intended for emergency exit use only, will be provided with delayed egress locking hardware (delay to be no longer than 30 seconds). Areas will be monitored to ensure that doors are not propped open. Delayed egress hardware shall be Von Duprin QEL series.

No perimeter or public area doors are designed to require manual locking or unlocking.

Perimeter Doors

Perimeter doors shall be set up in one of the following three configurations:

Card access: Main entrances to the building will be equipped with an electric lock controlled by a card reader. Where banks of multiple doors occur, only one door needs to be equipped with a card reader; the others may be electrically locked only. Where a handicap operator is in place, that door should always be equipped with a card reader.

Electrically locked: Entrances that need to be open for normal public access but do not need after-hours access will be equipped with an electric lock, but without a card reader.

No exterior access: Doors that are intended only as emergency exits will be configured with mechanical locking hardware only. This configuration should be with either no exterior hardware or key access only from the exterior (storeroom function lock). Optionally, emergency exit doors may also be equipped with a delayed egress alarm system, tied into the building fire alarm system.

Door Position Monitoring

All building perimeter doors, regardless of their locking configuration, will also be equipped with a magnetic contact allowing monitoring of the door position.

Mechanical Key Access

All doors equipped with electric locks will also be provided with a cylinder for key bypass (emergency access). All locks will use University standard cylinders.

Control Panels

Control panels for card access will be located a maximum distance of 150 feet from the card reader. They may be located up to 250 feet from a controlled door. The panels will be located on the same floor as the door they control and will be placed in the nearest telecommunications closet. Any alternative location for the panels, must be authorized by Public Safety Access.

Panels may not be placed within 10 feet of power transformers. When mounting the panel, the top of the panel cannot exceed 8 foot from floor level, to allow for servicing the panel.

For each panel, a minimum mounting space 3 feet wide by 4 feet high on a ¾-inch plywood backboard will be provided. A 120VAC, 20A emergency power outlet will be provided in the closet for powering the panel and associated equipment. A UC local area network (LAN) connection will be provided for each panel, except where multiple panels are co-located. The number of panels in a chain will not exceed 3 panels (one host and 2 downstream) In this case, one LAN connection may serve all panels located in one room.

The panels will communicate across the University LAN.

Control Panels will Life Safety Power model number FPO75/150-C4C82D8PE8M, which will control up to 8 doors. Alternative models must be approved by the access control office.

A completed copy of the UC Micro Sheet must be placed inside of each Micro.

Card Reader

Card access doors shall be provided with a system compatible card reader mounted on a single gang box located 42 inches above the finished floor (AFF). All mounting boxes will be plastic, metal boxes shall not be used because of interference issues. The box and reader will be mounted vertically. Exterior doors require that the card reader be in a sheltered location (no direct rain/snow). If this is not possible, a weather shield should be provided above the reader. All readers will be HID RP40 or RPK40 Bluetooth readers. Readers must be ordered with UC programming for Bluetooth.

All readers must be labeled with the appropriate micro and port number.

Junction Box

A Micro Junction Box will be provided above every door or set of doors that have card access. The box will be located above the ceiling where accessible or immediately below the ceiling. The location of the junction box must be noted on the As-Built drawings.

Conduit/Cable Tray

All wiring will be run in either conduit or cable tray. Conduit will be sized to allow a minimum of 20% excess capacity, and will have a pull string left in place. The As-Built drawings must indicate the cable path and whether the cable was ran in conduit or in a tray.

Wiring

New installations and wiring replacements will be done with Windy City 4461030, Belden 658AFS or equivalent approved access control cable. Equivalent cable must be submitted to Public Safety Access office for prior approval. Wiring will be installed with industry standard color coding:

Gray: Lock

Power Blue:
Request to Exit
White: Door
Contact Orange:
Card Reader

For existing access and repairs, cable will be provided as shown on the typical configuration drawings. This includes the following:

- 6-Conductor, 18-gauge shielded cable from the micro/5 to the Micro Junction Box
- 2-Conductor, 18-gauge cable from the Micro/5 to the Micro Junction Box
- 4-Conductor, 18-gauge cable from the Micro/5 to Micro Junction Box.
- 2-Conductor, 14-gauge cable from the Power Supply to the Micro Junction Box
- 4-Conductor, 18-gauge shielded cable from the Micro Junction Box card reader
- 2-Conductor, 18-gauge cable from the Micro Junction Box to the Door Contact
- 4-Conductor, 18-gauge cable from the Micro Junction Box to the Request to Exit
- 2-Conductor, 14-gauge cable from the Micro Junction Box to the Door Lock

All wiring will be installed in accordance with the current National Electric Code (NEC) and National Fire Protection Act (NFPA) codes.

All cable will be plenum rated cable.

All exposed cable less than 10 feet above the floor will be run in conduit or Wiremold. Conduit and Wiremold must be properly secured to the wall and sealed if in an outdoor or wet environment.

Cable run above a drop ceiling will be in conduit or lay in cable tray. Cable will not be laid loose above ceiling tiles, or tied to conduit or water pipe.

All wiring must be

- Soldered and taped or provided with crimp on connectors inside a junction box
- Ran direct to junction box or device. Wires will not be spliced inline
- Labeled on both ends. Labels will be printed, not handwritten
- All card readers to be labeled with micro number; card number, address number.

Labels are to be printed, not handwritten.

Interior Doors

Interior doors shall be configured for card access using the same specifications and hardware listed above for exterior doors. Card access shall be considered for any area that requires either controlled access by large numbers of persons or an audit trail of persons entering the space.

Examples include faculty mail rooms, college records offices, and computer labs that are not attended. Mag locks are prohibited on UC property.

Card Access

Options for interior access control include the use of electrically locked doors and a card reader, as installed on the perimeter doors. Additionally, keypads may be used in conjunction with card readers. The keypad will allow the user to lock and unlock the door manually.

Wireless Locks

Interior doors may also be outfitted with wireless locks for access control. Wireless locks can be used in many, but not all circumstances. The wireless locks are available in 2 main varieties, pure wireless and wireless to hub. Each lock has its own strengths and weaknesses. Wireless locks cannot be used on exterior doors or high security areas.

Pure wireless locks are suitable for IT closets, maintenance areas, storage areas etc. These locks cannot be directly controlled in an emergency.

Wireless to hub locks are suitable for classrooms, area entrances and other secure areas.

The use of any wireless lock must be approved by the card access office to ensure the proper Locks are being specified for an area.

Door Hardware

In the interests of performance and maintainability, specific types of door hardware are recommended for use with the access system. The University standards for door-locking hardware should also be consulted. Technicians must stay current on applicable building codes and University standards.

Fire and Panic Hardware

Doors requiring fire or panic hardware shall be provided with UC approved hardware in either mortise or rim-locking versions, configured for Fail Secure operation, and with the request-to- exit (RX) option.

The use of vertical rod-locking versions is **prohibited** because of long-term maintenance problems.

Panic hardware will be VonDuprin QEL series (electric latch retraction) or equivalent for all doors. Equivalent hardware must be approved by the access control office. Electrified panic hardware shall not have dog screws installed.

The door hardware schedule must include the appropriate power supply located within 50 feet of the door. The supply is to be located on the same floor in an electrical or telephone closet, where available, or in an accessible location above the finished ceiling if necessary. All power supplied with a manufacturer's lifetime warranty. The supply must be fed from an emergency power source. If the power supply is not on an emergency power supply, they will be installed with battery backup. Batteries will be labeled with install date. The location and type of the power supply, emergency power or battery backup must be noted on the As-Built drawings.

"Emergency Exit Only" Doors

Doors that are intended for emergency exit use only, and where an alarm function is needed, shall be provided the appropriate UC approved hardware series hardware. Provision must be made to interface the door control with the building fire alarm system in accordance with NFPA

101. This interface is normally accomplished with a Simplex control ZAM located at the lock power supply.

If no delayed egress or alarm function is needed, the standard exit hardware set for the building may be used, with no exterior hardware on the door.

The door hardware schedule must include the appropriate specified power supply, located within 50 feet of the door. The power supply is to be located in an EIDF room, electrical or telephone closet, where available, or in an accessible location above the finished ceiling if necessary. All power supplied with a manufacturer's lifetime warranty. The supply must be fed from an emergency power source. If the power supply is not on an emergency power supply, they will be installed with battery backup. Batteries will be labeled with install date. The location and type of the power supply, emergency power or battery backup must be noted on the As-Built drawings.

Interior Mortise Locks

Interior doors requiring standard mortise locks shall be provided with UC approved hardware. When not contained within the Life Safety Power can, the appropriate power supply will be provided within 150 feet of the door. The supply is to be located in an electrical or telephone closet, where available, or in an accessible location above the finished ceiling if necessary. All power supplied with a manufacturer's lifetime warranty.

The supply must be fed from an emergency power source. If the power supply is not on an emergency power supply, they will be installed with battery backup. Batteries will be labeled with install date. The location and type of the power supply, emergency power or battery backup must be noted on the As-Built drawings. The drawings must also indicate the manufacturer and model number of locks installed

Power Transfer

Wiring to electric locks is by either power transfer or electric hinge, as appropriate. The use of a power transfer is preferred because it provides greater ease of service in the event repair is required. Power transfers will be used on new exterior doors. Electric hinges may be used where retrofitting to an existing frame, or for interior wood doors. Door cords are prohibited.

Request-to-Exit Devices

A request-to-exit device must be provided for all doors that are equipped with an electric lock. This device will normally be a passive infrared detector. In special circumstances a card reader may be used to control exit through a non-designated egress door; however, an emergency break-glass release must be provided.

Magnetic Locks

Due to ongoing maintenance issues, magnetic locks, “Mag Locks” are prohibited on UC campuses.

Programming

The security vendor will program panels, doors and readers to the current UC guidelines.

Programming will be done by a certified technician. The Public Safety technician assigned to the project will provide this information before programming.

Before the installation, the panel Ethernet address must be obtained from UCIT. This action should be initiated by the Project Manager.

Communications from the panel to the host will be encrypted by triple DES.

Startup and Commissioning

To verify proper operation, the access vendor will test each card reader or controlled door in the presence of the assigned Public Safety technician. Testing shall include placing the door in the controlled mode, using a valid card to release the door, using the request-to-exist device to release the door, and placing the door back in the unlocked mode. Doors will also be tested using a non-valid card.

Each alarm function of a portal will be tested, including door forced open, door held open, cabinet tamper, AC loss, and low battery.

Before the system is placed online, the vendor must complete the access system acceptance form and submit to the access office with as-built drawings. Once the form is submitted, an access technician will inspect the installation and note any discrepancies that must be fixed or approve the installation. After the installation is approved, the doors may be programmed into the access system. Both the installer and the access technician must sign off on the form before the installation is approved.

The Public Safety technicians will field audit the installations to verify that the design standards, including the appropriate wiring practices, have been followed.

Vendor will provide a minimum of one year warrant on all labor, installation and materials. The warranty on each installation will commence upon completion of the field audit and University acceptance of the installation.

The Contractor shall repair any system malfunction or installation deficiency discovered by the owner or their representatives during the burn in and warranty period. The Contractor shall correct any installation deficiencies found against the contract drawings and specifications

Vendor will provide As-Built drawings in PDF and CAD formats. Drawings will indicate location of alarm panels, devices and wiring paths. Drawings will also indicate wire numbers for all cables on both ends.

Maintenance

The vendor will assist Public Safety IT personnel with a redundant system for all server related activities. This would include working with Public Safety Information Technology area for support, and performing installations and upgrades. The vendor should perform the following tasks.

- Performance monitoring through dial up or onsite
- Propose server configurations to UC
- Review final server configuration
- Build any new servers or upgrade existing servers with operating system, applications, PPRS, modules, interfaces, scripts, etc
- Test network connectivity between servers and panels
- Restore database on new or existing servers following installation or upgrade
- Restore or bring up web browser workstations on new or existing equipment
- Test imaging stations and peripheral equipment
- Verify/test UC IDM connection