## 106. LOCK AND CARD ACCESS GENERAL DESIGN INFORMATION

### I. General System Information

A. Supporting Software (not a contract bid item)

i. All card readers and equipment are managed through the Schlage Security Management Software (SMS) system, which is already available on campus and managed by the University Key and Lock Office.

a. The University is responsible for the software system preparation prior to installation/startup of new devices including area records creation, privilege set up and door schedule development.

b. The University is responsible for all software system preparation prior to the installation/startup and data entry and initial field programming for any new stand-alone/battery operated reader hardware devices.

c. The installation contractor or integrator is responsible for software/system preparation and database record creation for readers, controllers, relays, contacts, CIMs, automatic override task templates for each area, and any set up and testing of installed hardware components and devices.

B. All equipment and components to support the card access system shall be installed to manufacturer specifications.

**C. All** doors must contain a cylinder and core for hard key override operation. Cores and cylinders must meet KU Design Guideline requirements specified under Division 8 of the KU Design Guidelines

### II. Design and Installation Requirements:

**A. General:**

i. A door survey and hardware review meeting shall be conducted during the design of any project. Participants to include an architectural hardware consultant or professional with experience in the design of Schlage electronic lock systems, KU Key and Lock Shop representative, KU Project Manager, at a minimum.

ii. Installation, startup, and testing of electronic locking systems shall be completed by an integrator with demonstrated experience with Schlage electronic lock systems installations.

### III. Generic Requirements By Opening Type

**A. <u>Exterior Doors-</u>**

i. **Primary Entrances-**

a. Primary entrance points will be defined by the University for each project during door and hardware coordination/review meeting.

b. All exterior doors used as primary entrance points MUST have hard-wired, on-line card access readers (SMR10) with a hard key override.

c. All exterior primary entrance doors must have alarm monitoring including door position and door tampering controls. Door position and tamper monitoring will be monitored by the SMS Card Access Software.

d. Residence Hall primary entrances must contain alarms that should be reported locally through audible local alarms (horns) and reported remotely through the SMS Card Access Software.

Local horn devices should be connected to a card swipe (SMR10) in lieu of a key switch to allow for local reset of alarm condition.

e. All primary entrances must also include a request to exit device. Request to Exit **sensors** are the preferred REX type. Where multiple doors exist at a primary entrance, the on-line hardwired card access reader should operate (at a minimum) the handicapped entrance doors, if one exists.
f. Where a set of double doors are controlled by the door access system, both doors shall be locked/opened automatically via the system.
g. Primary entrances should use electric latch retraction devices as the locking mechanism. For openings with two doors in an opening, both leafs should contain electric latch retraction devices.
h. For vestibules that act as a primary entrance, both outer door leafs should contain electric latch retraction devices. If the inner set of doors has no other access point, these doors do not need locking mechanisms. In the case of a vestibule entrance where the inner set of doors has another access point (for example from an adjoining hallway), full electronic monitoring and locking shall be provided as is provided on the outer set of doors (electric latch retraction, door reader, request to exit sensor, door position monitoring).

ii. **Loading Docks and Service Entrances-**
a. Loading dock and service entrance locations will be identified and defined by the University for each project during door and hardware coordination/review meeting .
b. All loading docks must have hard-wired, on-line card access readers (SMR10) with a hard-key override for entrance.
c. All loading docks must have a hard-wired, on-line card access reader (SMR10) that acts as the request to exit.
d. All loading docks and service entrances must have alarms that should be reported locally through audible local alarms (horns) and reported remotely through the SMS Card Access Software. Local horn devices should be connected to a card swipe (SMR10) in lieu of a key switch to allow for local reset of alarm condition.

iii. **Secondary Doors (Emergency Exit Only)**
a. Secondary doors will be identified and defined by the University for each project during door and hardware coordination/review meeting.
b. All secondary doors (emergency exit only doors) must have alarm monitoring including door position and door tampering controls.
c. Door position and tamper monitoring will be monitored electronically by the SMS Card Access Software. Alarms should be reported locally through audible local alarms and reported remotely through the SMS Card Access Software.

d. Residence Halls: All secondary doors must be installed with delayed egress panic devices (CHEXIT), local audible alarm (horns), and door position monitoring. Alarms should be reported locally through the horn device and remotely through the SMS Card Access Software. Local horn devices should be connected to a card swipe (SMR10) in lieu of a key switch to allow for local reset of alarm condition.
e. All secondary exit doors should include signage indicated that doors are alarmed and to be used as emergency exits only. All secondary (exit only doors) should have hard key mortise locks installed on the exterior of the door to allow for emergency entrance if necessary.

**B. <u>Interior Doors</u>**

i. **Offices-** stand-alone card access lock (AD 200 Series office function lock) except when the only entrance to the office is an exterior door. In that case the exterior entrance to the office shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a stand-alone card access lock (AD 200 Series office function lock) unless otherwise specified by the University during the design process.

**ii. Residence Hall Rooms-** stand-alone card access lock (AD 200 series storeroom function locks) except when the only entrance to the residence hall room is an exterior door. In that case the exterior entrance to the residence hall room shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a stand-alone card access lock (AD 200 Series storeroom function lock) unless otherwise specified by the University during the design process.

iii. **Classrooms-**Wireless (AD 400 series classroom function locks) card access readers except when the only entrance to the classroom is an exterior door. In that case the exterior entrance to the classroom shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a wireless card access lock (AD 400 Series) unless otherwise specified by the University during the design process.

iv. **Stair tower Doors-**hard-key only except where monitored access or egress is required by departmental use requirements. Non critical stair tower doors will be free egress at all times. All perimeter doors shall be monitored by the access control system. Exterior stairwell doors shall be a Chex-it delayed egress device in compliance with local building and Life Safety codes. Acceptable manufacturer: Von Duprin No Substitutions.

v. **Mechanical Rooms-**stand-alone card access lock (AD200 series storeroom function locks except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a stand-alone card access lock (AD 200 Series) unless otherwise specified by the University during the design process.

vi. **Custodial Rooms-** stand-alone card access lock (AD200 series storeroom function locks) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a stand-alone card access lock (AD 200 Series) unless otherwise specified by the University during the design process.

vii. **Teledata Rooms-** stand-alone card access lock (AD200 series storeroom function locks) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a stand-alone card access lock (AD 200 Series) unless otherwise specified by the University during the design process. Exceptions include central server pool rooms. These spaces shall be on-line hardwired card access readers (AD300 series) with full monitoring.

**viii.** **Elevator Machine Rooms-** stand-alone card access lock (AD200 series storeroom function locks) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a stand-alone card access lock (AD 200 Series) unless otherwise specified by the University during the design process.

**ix.** **Laboratory Spaces-**Wireless card access readers (AD400 series) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a wireless card access lock (AD 400 Series) unless otherwise specified by the University during the design process.

x. **Departmental Storage Closets/Rooms-** stand-alone card access lock (AD200 series storeroom function locks) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the

space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a standalone card access lock (AD 200 Series) unless otherwise specified by the University during the design process.

xi. **Maintenance/Facilities Shop areas-**stand-alone card access lock (AD200 series storeroom function locks) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a standalone card access lock (AD 200 Series) unless otherwise specified by the University during the design process.

**xii. Building Maintenance Storage Rooms-** stand-alone card access lock (AD200 series storeroom function locks) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a standalone card access lock (AD 200 Series) unless otherwise specified by the University during the design process.

**xiii. Conference/Meeting Rooms-**

**a. Departmental conference and/or meeting rooms-** stand-alone card access lock (AD200 series classroom function locks) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a standalone card access lock (AD 200 Series) unless otherwise specified by the University during the design process.

b. **University-wide or centrally scheduled conference and/or meeting rooms-** Wireless card access (AD400 series) readers except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a wireless card access lock (AD 400 Series) unless otherwise specified by the University during the design process.

xiv. **Restrooms**

a. **Single Stall Private restrooms/Unisex Restrooms/Family Restrooms –**privacy lockset with Occupied/Unoccupied indicator, which is operated with lock/unlock and visible on the exterior of the door. Acceptable manufacturers: Schlage L9000 series, No Substitutions.

b. **Multi-stall restrooms and gang bathrooms**- hard key only on main door to restroom. In residence hall settings, double-sided deadbolts with hard key only is the standard.

xv. **Computer Labs-** wireless card access (AD400 series storeroom function) locks except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a wireless access lock (AD 400 Series) unless otherwise specified by the University during the design process.

xvi. **Research areas**- Wireless card access readers (AD400 series classroom function) locks except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a wireless card access lock (AD 400 Series) unless otherwise specified by the University during the design process.

xvii. **Hazardous Materials areas-**wireless card access readers (AD 400 series storeroom function) except when the only entrance to the space is an exterior door. In that case the exterior entrance to the space shall be an on-line, hardwired card access reader (SMR10). If there is both an interior and exterior door leading to the space, then the exterior door should be hard key only with door position monitoring and the interior door shall utilize a wireless card access lock (AD 400 Series) unless otherwise specified by the University during the design process.

xviii. **Sheds and other exterior/non-building and temporary storage structures including modular trailers-** hard key only.

xix. **Vehicle and pedestrian gates-** wireless card access readers (AD400 series). Link limits are up to 1,000 feet from the controller. Distances over 1,000 feet will require additional materials, such as repeaters or will require hardwired readers (AD300 series) with appropriate cabling. Must include appropriate hoods or covers to protect card reader from inclement weather.

xx. **Elevators-**Wireless card readers (AD400 series) should be installed in the elevator cab and floor control should be used where restricted access is required to or from the elevator or if there is no travel cable existing in the elevator shaft or where access cannot be controlled by a door to the elevator lobby.

## IV. Hardware Types

### A. Card Readers

#### i. Standalone/Battery Operated Card Readers-AD200 series

##### a. General Requirements

1. **All standalone/battery operated card readers shall be Schlage AD200 Series Electronic Locks. No Substitutions.**
2. Standard installation for all AD200 series leverset lock installations include AD200 lock, door position switch installation, and override core and cylinder.
3. All batteries must be new and installed within 30 days of turnover to the University.
4. All AD locks must have PIN and card swipe capability, along with audit trail functions.
5. All office AD locks must have office function buttons on the inside plates.
6. All AD lock plates on the inside of the door should have Schlage tamper proof Spanner screws ordered through Schlage. No substitutions.
7. All AD locks should have construction cores installed so tail pieces don't get lost. Construction keys should be supplied to lock shop and project manager.
8. All readers will use the Schlage Access Credential Option MSK which includes Mag card reader and keypad with a core override.
9. All reader units will specify cylinder options that will accept a small format, figure eight, interchangeable (7 pin) core.
10. All reader units will include the ATK or Audit trail option-mechanical cylinder. This feature allows audit trail of mechanical key overrides on the units.
11. All units should include option HSS or High-security spanner screws for the inside escutcheon. This will provide tamper-resistant access to battery packs and internal mechanisms.
12. All AD200,300, and 400 series units should be ordered with Door Positioning Switch option and the Door Position Switch is to be installed on the door opening for all installations, regardless of whether wiring is to be installed to report alarm conditions. This allows for the AD200 series lock to be easily upgraded in the future.
13. All AD200 and 400 series lock installations require four (4) fully charged (1.3-1.5V each) Alkaline batteries within 30 days of turn-over to the University. The

batteries must be checked and confirmed upon installation of the lock and before final programming.

14. A report detailing the battery charge/check on each unit should be provided to the University after installation and final programming.

**b. Applications**

**1. Cylindrical Lock applications:**

a) Office Function: Model # AD-200-CY-50

1) The outside lever is maintained locked or unlocked by pushbuttons on the inside escutcheon or by a Toggle Mode access credential. The inside lever is always free. The unit may be unlocked from the outside with an approved access credential.

b) Classroom/Storeroom Function: Model # AD-200-CY-70

1) The outside lever is normally locked. The inside lever is always free. The unit may momentarily be unlocked from the outside with an approved access credential. The unit may be maintained unlocked by using a Toggle Mode access credential.

**2. Mortise Lock applications:**

a) Office Function: Model # AD-200-MS-50

1) The outside lever is maintained locked or unlocked by pushbuttons on the inside escutcheon or by a Toggle Mode access credential. The inside lever is always free. The unit may be unlocked from the outside with an approved access credential.

b) Classroom/Storeroom Function: Model # AD-200-MS-70

1) The outside lever is maintained locked or unlocked by pushbuttons on the inside escutcheon or by a Toggle Mode access credential. The inside lever is always free. The unit may be unlocked from the outside with an approved access credential.

3. **Panic Device Applications** -Model # AD-200-993- model exit trim

a) For Use with Von Duprin 98/99 Series Exit Devices including Rim, Surface Vertical, Concealed Vertical and Three-Point latching models:

b) Access Credential Option: MSK (Mag card reader and keypad)

c) Emergency mechanical key override option

d) Key cylinder to accept small format, figure eight, interchangeable (7 pin) core

e) Trim: ATK Audit trail of mechanical key override

f) Standard installations for all applications include reader and door position switch.

**ii. Online Readers**

**a. Wireless Card Readers (Schlage AD400 Series Electronic Locks)**

**1. General Requirements**

a) Standard installations include reader, door position switch, connection to Reader Interface Module, and connection from Reader Interface Module to Controller, at minimum.

b) All batteries must be new and installed within 30 days of turnover to the University.

c) All AD locks must have PIN and card swipe capability, along with audit trail functions.

d) All office AD locks must have office function buttons on the inside plates.

e) All AD lock plates on the inside of the door should have Schlage tamper proof Spanner screws ordered through Schlage. No substitutions.

f) All AD locks should have construction cores installed so tail pieces don't get lost. Construction keys should be supplied to lock shop and project manager.

g) All readers will use the Schlage Access Credential Option MSK which includes Mag card reader and keypad with a core override.

h) All reader units will specify cylinder options that will accept a small format, figure eight, interchangeable (7 pin) core.

i) All reader units will include the ATK or Audit trail option-mechanical cylinder. This feature allows audit trail of mechanical key overrides on the units.

j) All units should include option HSS or High-security spanner screws for the inside escutcheon. This will provide tamper-resistant access to battery packs and internal mechanisms.

k) All AD units should be ordered with Door Positioning Switch option and the Door Position Switch is to be installed, with appropriate wiring to reader interface modules and controller connections.

l) All AD lock installations require four (4) fully charged (1.3-1.5V each) Alkaline batteries within 30 days of turn-over to the University. The batteries must be checked and confirmed

upon installation of the lock and before final programming.

l) A report detailing the battery charge/check on each unit should be provided to the University after installation and final programming.

**2. Applications**

a) Classroom/Storeroom Function Mortise Lock: Model # AD-400-MS-70

1) The outside lever is maintained locked or unlocked by the Schlage Security Management (SMS) software system. The inside lever is always free. The unit may be unlocked from the outside with an approved access credential.
2) Approved manufacturer: Schlage No Substitutions

b) Classroom/Storeroom Function Cylindrical Lock: Model # AD-400-CY-70

1) The outside lever is maintained locked or unlocked by the Schlage Security Management (SMS) software system. The inside lever is always free. The unit may be unlocked from the outside with an approved access credential.
2) Approved manufacturer: Schlage No Substitutions

c) Classroom/Storeroom Function Exit Device Trim: Model # AD-400-993

1) The outside lever is maintained locked or unlocked by the Schlage Security Management (SMS) software system. The exit device is always free and allowing free egress. The unit may be unlocked from the outside with an approved access credential.
2) Approved manufacturer: Schlage No Substitutions.

**b. Hard-Wired Card Readers (Schlage AD 300 Series or SMR10 Electronic Locks)**

**1. General Requirements**

**a) Exterior Doors**

**1)** SMR10 reader. No substitutions.
2) Standard installations include reader, door position switch, electric latch retraction, power supply, request to exit device, connection to Reader Interface Module, and connection from Reader Interface Module to Controller, at minimum.

3) Must include weather guard/weather shield
4) Standard color is black **.**

2. **Applications**

**a)Handicapped Door Operation**

1) Exterior Handicapped Button
    a. Door operation: Valid card swipe will retract electric latch retraction device and allow the exterior actuator to be used to signal auto operators. It will also sequence inside vestibule door to open. Free egress from inside always. SMS (Security Management System) to be used to turn on exterior actuator for public function use.
2) Interior Handicapped Button
    a. Door operation: Interior actuator is used to signal lock, request to exit, and opener at all times.

**b) Panic Devices**

1) **Delayed Egress Panic Devices**- for applications requiring delayed egress panic devices, the University standard is a Chex-it panic devices. Acceptable manufacturer: Von Duprin No Substitutions.
2) **All Other Panic Devices** -
    **a.** Von Duprin 98. No substitutions.
    **b.** All other panic devices must include door monitoring (door contacts) connected to Control Panel via Reader Interface Module.

**B. Controllers (Reader Door Control Panel)**

i. Controllers shall be Schlage Security Management (SMS) panels with a capacity of controlling up to 16 hard-wired or wireless doors.
ii. In facilities where residence hall spaces are in the same physical building structure with academic or general use spaces such as classrooms or offices, separate control panels shall be installed for the residence hall areas for proper operation and control of the residence hall spaces.
iii. All Reader Door Control Panels (Controllers) shall be connected to emergency building power or shall contain extended life battery backup power source (15+ hours installed to support power supplies).
iv. Acceptable manufacturer: Schlage, no substitutions.
**v. Wiring Specifications**

a. All the system components shall utilize "Distributed Processing" concepts. The distributed processing shall include the ability to download the operator parameters to any centrally installed reader door control panel (controller) (SRCNX) thus allowing the field panel to provide full operating functions independent of the access control software.

**b. Access Control Equipment Location (Telecommunications Room/Data Closet)**

1. All Access Controllers will be placed in the mechanical or dedicated building maintenance space closest to the telecommunications room serving the floor. Examples of acceptable locations in order of preference include:
    a) Mechanical rooms
    b) Electrical rooms without High Voltage Equipment
    c) Custodial rooms without damp conditions
    d) Controllers will **not** be installed into any Telecom Network closets as in the past
    e) High voltage electrical rooms are not acceptable locations for reader door control panels (controllers).
2. All wiring from the reader interface modules should be brought to the reader door control panel (controller) which should be located in a mechanical or dedicated building maintenance space closest to the telecommunications room serving the floor.
3. All 110Vac and network requirements are to be provided by the Division 16 contractor. (1 quad power outlet connected to a generator backup panel and 1 CAT6 drop per controller). If a deviation is necessary it must be pre-approved by the University. The dedicated hardwired network drop will be required with the following stipulations:
    a) Facilities approved vendor will contract out to a university approved Berk-Tek Oasis certified Telecommunications contractor.
    b) Contractor Qualifications include:
        1) The Telecommunications contractor must be an approved Ortronics Certified Installer at a Plus tier (CIP, CIP-Gold, CIP-Platinum, and multi-site/national contractors) and Berk-Tek Certified OASIS Integrator. A copy of the company certification documents must be submitted with the quote in order for such quote to be valid. The Telecommunications contractor is responsible for workmanship and installation practices in accordance with the Ortronics CI/CIP Program and Berk-Tek OASIS Program. Ortronics/Berk-

Tek will extend a NetClear 25-year Static, Dynamic and Applications Warranty to the end user once the Telecommunications contractor fulfills all requirements under Ortronics and Berk-Tek OASIS Program. At least 30 percent of the copper installation and termination crew must be certified by Berk-Tek and Ortronics or by BICSI with a Technician Level of training.

2) The contractor shall have at least five (5) years' experience installing and servicing Telecommunication systems.
3) The contractor shall have at least three (3) years' experience working at an educational institution
4) The successful bidder shall maintain an office or competent technical presence with appropriate testing equipment and replacement parts within a 60 mile radius from this project.
5)

c) Telecommunications contractor must be approved by the University Office of Information Technology.
d) KU Facilities will provide the MAC address to Network Services at least 2 weeks prior to the controller activation date.
e) KU Information Technology Network Services will provide a patch cord at both ends to complete the connectivity and assign a static IP address.

4. The SRCNX series of network access controller uses proprietary software by Schlage for setup and monitoring purposes. The SRCNX-x panel requires 110Vac drawing approximately 4 amps. The SRCNX-x communicates with the system software via a TCP/IP, LAN/WAN connection utilizing the existing University network. This panel is to be installed in a secure area such as a mechanical room. The SRCNX-x communicates to downstream devices using an RS-485 connection utilizing Belden 8723 or equal. The access controller is a proprietary model through Ingersoll Rand Security Technologies.

**C. Reader Interface Module (SRINX)- (All On-line reader applications including SMR10, AD300 series and AD400 series reader devices and door position monitoring devices)**

i. The SRINX reader interface module supports multiple read head technologies and connects one read head to the reader controller via an RS-485 connection utilizing Belden 8723 or equal. Connect all door

devices including reader, door contacts, and request to exit devices to this module. The reader interface module control shall be mounted in a lockable enclosure on the secure side of the reader accessed door.

ii. The reader interface module (SRINX) shall be mounted within 15 feet of the door, on the secure side of the door served and must be enclosed in a lockable cabinet. All door device cabling shall be connected to this interface. The interface shall communicate with the reader door controller (controller) located in the mechanical or secured maintenance storage space closest to the teledata closet serving each floor. The interface shall be powered from the access controller via the RS-485 path.

**D. Door Position Switches/Door Monitoring Contacts**

i. Door monitoring contacts should be installed in all hard-wired and wireless access control applications.

ii. Door monitoring contacts will be used to sense if a door is open or closed. The preferred installation of door monitoring contacts shall be concealed/recessed, surface mounted contacts are by exception only upon approval of university. If surface mounted is the only option, armored cable must be used from the contact to the reader interface model.

iii. Cabling from the door contact to the reader interface is to be Belden 8444.

iv. The door contacts are to be provided by the Section 08710 contractor.

v. Acceptable vendors include Von Duprin and Schlage. No substitutions.

**E. Key Switches**

i. Key switches for alarm controls are not to be used without the express permission of the Kutztown University Key and Lock Office. Where possible, operation of alarms or controlling on/off conditions for the door security system should be managed by an SMR10 reader instead of a key switch.

**F. Electric Locking Devices and Electrified Hardware**

i. Door locking mechanisms (electric strike, electric lock, magnetic lock, latch retraction, electrified panic devices, etc.). All electric locking devices should be 24VDC, continuous duty solenoids, fail secure Mortise Lock Devices.

ii. All installations shall include appropriate power supply devices.

iii. Acceptable vendors are Von Duprin or Schlage. No substitutions.

**G. Request to Exit Device (REX):**

i. Acceptable vendors include Von Duprin and Schlage. No substitutions.

**H. Request-To-Exit (REX) Sensors:**

i. Acceptable vendors include Von Duprin and Schlage. No substitutions.

**I. Power Transfer**

i. All door jambs should be prepped for EPT10 where power transfer is to be used.

ii. University standard for power transfer is EPT10.

iii. Acceptable vendors include Von Duprin and Schlage. No substitutions

**J. Power Supplies:**

i. Access Control Power (ACP) supplies shall be the most up to date model with battery back- up wired and installed and key lockable panel door. - includes power supplies for both the locking hardware and the controller boards.

ii. Power supplies for both locking hardware and locking hardware controller boards are to be supplied by the Section 08710 supplier.
iii. The electrified locking hardware power supplies shall be mounted above ceiling level on the secured side of the door wherever possible. In the event a wall mounted solution is required a suitable location shall be identified and installation will take place with approved materials to provide a secure installation. The lock power supplies shall be interfaced with the reader interface modules to provide activation of the locking hardware upon valid card reads. All lock power supplies are to be provided by the Section 08710 contractor.
iv. The power supply should be labeled to identify the location of the electrical panel, the electrical panel number, and the breaker number.
v. Acceptable vendors include Von Duprin or Schlage. No substitutions.

**K. Enclosures:**

i. Controller enclosures must be supplied by Ingersoll Rand Security Technologies and are part of a standard reader package. No substitutions.

**L. Secondary Security Devices:**

i. All secondary security devices such as audible horns, bells, door positioning switches, PIR, request to exit sensors, local alarms, etc. should be connected to the reader interface module for each door.

**M. Communications Cable Pathways**

i. The electrical contractor shall provide pathways for all access control system devices. These shall include conduits, wire ways, junction boxes, pull boxes, pull strings, sleeves and other accessories required to install raceways.
ii. The minimum conduit trade size per cabling component shall be 3/4".
iii. Conduit sections that exceed 100' shall be equipped with a 4" x 4" x 2&3/4" deep J-box placed as a pull point.
iv. No section of conduit shall have more than 2-90 degree bends without a suitably sized J-box placed as a pull point.
v. All J-boxes placed to support the Card Access System shall be labeled on the cover with the location of the serving door and the serving communications room.
vi. All J-boxes shall be mounted facing down in the pathway run for identification from below the ceiling grid.
vii. At the termination location the J-box may be mounted on the wall as approved in accordance with approved practices and preserving the wall rating.
viii. All cable pathways in the frames and doors shall be accessible with no sharp edges or spaces that are not continuous.

**N. Communication Cables**

i. Communication cable runs shall be installed parallel to the building lines, in the hallways as much as possible. All cabling shall be placed in the 1" minimum sized conduit to all locations labeled at both ends. At the Access Controller location provide a minimum of 25 feet of extra length on all cables, coil and identify as required. No cabling shall exceed 500'. All cabling shall be installed according to approved industry practices.
ii. All installations must adhere to Horizontal Cabling Specifications referenced in section 2.2 of the Telecommunication Design Guidelines.

iii. All installations must adhere to Horizontal Cabling (Outlets) referenced in section 2.3 of the Telecommunications Design Guidelines.

**O. Equipment Termination**

i. The approved contractor shall be responsible for the connectivity of all cabling used for the Card Access System.

ii. Field wiring shall be connected to the Reader Door Control Panel (Controller) through the use of screw clamp type connectors, which can be removed from the panel. The connections on the Reader Door Control Panel (Controller)shall be spaced in such a manner as to prevent cross wiring of neighboring circuits.

**P. Cabling**

i. A continuity test shall be used to verify conductors are free of cable faults and verify cable identification and labeling.

**Q. System Test**

i. After all cabling and components have been installed and connected, the contractor shall perform a test of operability with a Kutztown University Key and Lock Office representative to confirm proper operation.

**R. Labeling**

i. Cable tags or markers: Shall be self-adhering, preprinted vinyl-type markers. Cables shall be tagged with appropriate designations supplied in this document.

ii. The contractor shall identify and tag the cable as follows:

a. PL = Power Local
b. PR = Power Remote
c. D = Data
d. PX = Proximity Reader
e. AC = Access Controller
f. DN = Door Number
g. C = Cable Type