GENERAL:

To provide minimum standards for Access Control Systems.

PART 1 Common Work Results for Access Control System

1.1 Owner will provide server and software for connecting control panels through the use of the owner provided TCP/IP network.

1.2 Owner shall provide necessary means for Access Control System Integrator to configure all controllers using Owner's server and existing control software installation. The Access Control System Integrator shall configure all controllers and doors in the Owner provided software.

1.3 The system shall be capable of utilizing the existing LAN / WAN connecting the buildings or a dedicated security Ethernet network for controller and client communications.

1.4 After installation, the Owner shall be able to perform hardware configuration changes as desired without the services of the Integrator.

1.5 Control panel usernames and passwords shall not remain the default username and password. Upon Contractor's request, Owner will provide Contractor usernames and passwords for all hardware requiring passwords.

1.6 Owner shall utilize existing campus ID cards. Integrator shall not provide cards for use with the system.

1.7 Integrator must provide Authorized Dealer Certificate and Certified Training Certificates of Integrators who will be working on this project.

1.8 Integrator shall provide shop drawings to include:

1.8.1. Drawings showing layout of equipment

1.8.2. Field controller equipment location wall layouts, including size requirements

1.8.3. Detailed wiring diagrams of field controllers, door details, and head-end devices

1.8.4. Load calculations of all security equipment for proper sizing of electrical and standby emergency generator circuits

1.9 Integrator shall provide as-built drawings prior to final acceptance by Owner.

1.10 Integrator shall be a Company specializing in intrusion detection and access control systems with a minimum of three years' experience on systems of similar size and scope. Technicians performing installation, configuration, and final terminations on the access control system shall have been certified by the manufacturer of the controller and software used for this project in accordance with the manufacturer's requirements.

1.11 All equipment, materials, and labor shall be warrantied for a period of 12 months from the date of final acceptance by the Owner. During the warranty period, the Contractor shall repair any fault in the system or hardware failure within 72 hours of the Owner reporting an issue to the contractor.

1.12 Doors shall be controlled by control panels located on the same floor as the door itself. Controlling doors from control panels located on floors above or below the connected door is not permitted unless approved by the Project Manager.

1.13 All doors shall be equipped with a card reader, request to exit device (REX), and a door position switch.

1.14 Control wiring shall be installed in conduit until above ceiling level; above ceiling level, cable may be installed in cable tray or J-hooks. Contractor shall label all cables.

1.15 Controls panels shall be located in a lockable room, typically the telecommunications closet.

1.16 All control panels and door hardware power supplies shall be connected to emergency power.

1.17 A backup battery shall be provided for all control panels, and runtime on batteries shall be a minimum of 30 minutes.

1.18 All doors shall fail secure.

1.19 Install wiring for detection and signal circuit conductors in conduit. Use 22 AWG minimum size conductors.

1.20 All Hardware, Channels and Access Levels shall be named in access control software upon creation in accordance Owner's convention. Integrator shall follow naming conventions documented in "Missouri S&T Electronic Access Control Naming Convention." This document can be found on the Missouri S&T Design & Construction Management's Contractor webpage at http://designconstruction.mst.edu/contractors/.

1.21 Where electric panic is specified, do not allow mechanical latching (unlocking) of panic device to override the access control system (do not include method for "dogging down" of panic hardware).

1.22 Electric strikes must accept pre-load.

1.23 As part of the ordering process of the custom HID Multiclass SE readers, all vendors order must be pre-authorized by the Owner before HID will allow a purchase. Upon award of contract, the Integrator shall submit the following information to the Owner for ordering authorization:

1.23.1. Vendor/Company Name

1.23.2. HID Customer ID (if available)

1.23.3. Company Address

1.23.4. Contact info for vendor/company point of contact

PART 2 Acceptable Door Hardware Configurations

2.1 Single doors not requiring panic hardware

2.1.1. Electric strike, door position switch, motion detector, smart card reader

2.2 Single doors requiring panic hardware

2.2.1. Electric panic hardware with RQE integrated into panic, door position switch, smart card reader

2.3 Double doors

2.3.1. Electric panic hardware with RQE integrated into panic (each door), door position switch (each door), smart card reader (operates one door). Card reader shall operate one of the two doors. Other doors to be monitored and unlocked/locked through input/outputs.

2.4 Exterior entrance locations having a bank of doors:

2.4.1. Electric panic hardware with RQE integrated into panic (each door), door position switch (each door), smart card reader (operates one door of the bank of doors). Other doors in bank to be monitored and unlocked/locked through input/outputs.

PART 3 Operation

3.1 Doors requiring automatic door operators

3.1.1. Locked mode

3.1.1.1. Pressing secure side automatic door opener actuator opens door.

3.1.1.2. Pressing unsecure side automatic door opener actuator without presenting valid card performs no action.

3.1.1.3. Presenting valid card unlocks door. Pressing unsecure side automatic door opener actuator within unlock timeframe activates automatic door opener.

3.1.2. Unlocked mode

3.1.2.1. Pressing automatic door opener actuator on either side activates automatic door operator

PART 4 Products

4.1 Control Software

4.1.1. RS2: Software and licenses provided by owner. RS2 system shall be specified unless otherwise noted.

4.1.2. Hirsch Velocity: Software and licenses provided by owner. Hirsch Velocity system shall only be specified upon specific instruction by Owner.

4.1.3. CBORD Access: for use with Residential Life facilities only.

4.2 Controllers

4.2.1. Mercury Security Hardware

4.2.1.1. EP1502

4.2.1.2. EP1501: Permitted only upon Owner’s approval

4.2.1.3. MR-52

4.2.1.4. MR-16

4.2.1.5. MR-51e: Permitted only upon Owner’s approval

4.2.2. CBORD Squadron Hardware: for use with Residential Life facilities only

4.2.3. No Substitutions

4.3 Smart Card Readers

4.3.1. Custom HID Multiclass SE (for use with RS2 system only)

4.3.1.1. R10 Form Factor Manufacturer's Part Number: 900NWNNEKE00KG

4.3.1.2. R15 Form Factor Manufacturer's Part Number: 910NWNNEKE00KG

4.3.1.3. R40 Form Factor Manufacturer's Part Number: 920NWNNEKE00KG

4.3.2. Custom HID Multiclass SE (for use with Hirsch Velocity system only):

4.3.2.1. R10 Form Factor Manufacturer's Part Number: 900NWNNEKE0535

4.3.2.2. R15 Form Factor Manufacturer's Part Number: 910NWNNEKE0535

4.3.2.3. R40 Form Factor Manufacturer's Part Number: 920NWNNEKE0535

4.3.2.4. RK40 Form Factor Manufacturer's Part Number: 921NWNNEKE0535

4.3.3. Custom HID Multiclass SE (for use with CBORD system only); applies only to Residential Life facilities:

4.3.3.1. R10 Form Factor Manufacturer's Part Number: 900NWNNEKE00GK

4.3.3.2. R15 Form Factor Manufacturer's Part Number: 910NWNNEKE00GK

4.3.3.3. R40 Form Factor Manufacturer's Part Number: 920NWNNEKE00GK

4.4 Magnetic Stripe Readers

4.4.1. Not permitted

4.5 Door Position Switches

4.5.1. Schlage flush mount magnetic switches

4.5.2. Substitutions permitted upon Owner approval.

4.6 Electric Strikes

4.6.1. Von Duprin

4.6.2. HES

4.6.3. Substitutions permitted upon Owner approval.

4.7 Electrified Panic

4.7.1. Von Duprin EL/RX 99-L

4.7.2. No Substitutions

4.8 Motion Detectors

4.8.1. Bosch

4.8.2. Substitutions permitted upon Owner approval.

4.9 Power Transfer Hinges

4.9.1. Von Duprin EPT-10

4.9.2. Von Duprin EPT-2

4.9.3. No Substitutions

PART 5 Commissioning

5.1 Pre-Function Tests

5.1.1. Complete "Electronic Access System Hardware Form" to Owner to obtain IP addresses for system hardware. Form shall be submitted to the owner 3 business days prior to the Contractor's need for system IP addresses. This document can be found on the Missouri S&T Design & Construction Management's Contractor webpage at http://designconstruction.mst.edu/contractors/.

5.1.2. Contractor shall obtain login information to server and locks control software for programming and testing. Request login information from Owner's Access Control Specialist.

5.1.3. Test and document security device connections with a multi-meter to verify proper termination and operation.

5.2 Operational Field Test

5.2.1. System Channel, Hardware, and Access Level naming shall be completed prior to Operational Field Testing with Owner. Owner must approve naming 72 hours prior to start of operational field testing.

5.2.2. Electronic as-built drawings shall be provided to the Owner 72 hours prior to the start of the Operational Field Test.

5.2.3. Complete Contractor section of "Electronic Access Door Commissioning Form" for each door connected to the electronic access system, and submit one copy to Owner 72 hours prior to Operational Field Test. This document can be found on the Missouri S&T Design & Construction Management's Contractor webpage at http://designconstruction.mst.edu/contractors/.

5.2.4. Operational Field Testing can be scheduled once the communications cabling contractor has completed the portion of the voice and data network which supports the electronic access system.

5.2.5. Conduct a system test of each alarm point and door. Owner shall document results on "Electronic Access Door Commissioning Form." While conducting this test, the Contractor shall be in direct communication with Owner's Access Control Specialist as he/she observe the signals in the software. The following functions shall be tested for every door in the system:

5.2.5.1. In card-only mode:

a. Access granted with card

b. Access denied with card

c. Door forced open (simulate by using physical key)

d. Exiting from secure side (no alarms should be present)

e. Door held open

f. Power fail test

g. For doors with automatic opener:

1) Access granted with card, then automatic operator button pressed from unsecure side: door should unlock then automatic operator open door

2) With no card presented, automatic operator button pressed on unsecure side: no operation should be observed

3) Operator button pressed on secure side: automatic opener should operate

5.2.5.2. In unlocked mode:

a. Open door from secure side: observe door opened in system, then door closed

b. For doors with automatic opener:

1) Operator button pressed on unsecure side: automatic opener should operate

2) Operator button pressed on secure side: automatic opener should operate

5.2.6. If any function fails in the Operational Field Test, failures must be noted and a full test (only on doors that failed Operational Field Test) must be performed at a later date to ensure compliance.

5.2.7. The Owner's Access Control Specialist must be present for all Operational Field Tests and re-tests.

5.3 Integrated Systems Test

5.3.1. Test critical system interfaces such as fire alarm and elevators.

5.4 Substantial Completion Requirements

5.4.1. All devices and alarm points must pass operational field test