DIVISION 28 – ELECTRONIC SAFETY & SECURITY

1 ELECTRIC DOOR HARDWARE

1.1 The access control system must meet all performance requirements defined in this specification. A specific manufacturer or platform is not named to allow competitive evaluation and selection during procurement. Once selected by the institution and approved by the Physical Security Oversight Committee (PSOC), the approved access control platform becomes the standard for all future campus-wide deployments, expansions, and upgrades. All components must be fully compatible with the approved system architecture and certified by the manufacturer for the deployed environment.

1.2 The Physical Security Office (PSO), as the coordinating authority for the approved access control platform, shall be provided design documents for major renovations and new construction to review and approve proposed physical access control hardware and configurations. PSO approval is required prior to implementation.

1.3 Any request to deviate from these standards must be submitted in writing to the PSO for review and approval. Where exceptions are granted, all other standards remain in effect.

1.4 All electric hardware shall be pre-wired at the factory with standardized connectors.

1.5 Devices (readers) used for Credentialed Access - These Devices should use low in rush current to open and hold open (1 amp) directly from the control panel without auxiliary power supply.

1.6 Coordinate with door and frame manufacturers for wiring harness

1.7 Wiring Elevations - Provide, as part of the hardware schedule, a door and frame elevation that shows the location of each item of electric hardware, including a written description of operation

1.8 Wiring Diagrams - Provide point-to-point wiring instructions with all electric hardware

1.9 Coordinate all electrical hardware with identified access control suppliers

1.10 For all new construction and major renovation projects, exterior doors that provide access to public circulation areas must, at a minimum, be equipped with physical access control sensors. These sensors shall be hardwired and fully integrated into the campus-wide physical access control system. Integration must include all necessary hardware components to support full access control functionality.

1.10.1 Logging: All door components shall be provided to allow alarms to log the following events in real time: Door Open, Door Close, Door Held Open, Forced Entry Attempt, Door Propped Open.

1.10.2 Control: All door components shall be provided to remotely lock/unlock doors within the physical access control solution.

1.11 For new construction and major renovation, the main entrance(s), as identified by Planning Design and Construction (PDC) and a secondary door, as identified by PDC, shall meet 1.10 requirements and have physical access control readers.

1.11.1 In addition to 1.10, doors with readers shall log Access Granted/Denied

1.12 For existing buildings expanding physical access control readers, the main entrance(s), as identified by Planning Design and Construction (PDC) and a secondary door, as identified by PDC, shall be accessible by Reader. Where neither the main nor secondary doors meet ADA pathway requirements, a third door meeting ADA access requirements shall be identified and reader installed. All equipment requirements specified in 1.10 shall be applicable for ADA expansion.

1.12.1 In addition to 1.10, the readers shall log Access Granted/Denied.

1.13 For new construction and major renovation, all interior and exterior entrances to research laboratories shall include physical access control readers. All requirements from 1.10 shall be met; in addition the readers shall log Access Granted/Denied.

2 PHYSICAL ACCESS CONTROL MANAGEMENT SYSTEM (ACCESS CONTROL PANELS)

2.1 The Access Control capabilities shall include, but are not limited to

2.1.1 Access control panel, reader interfaces, readers, conduit, OSDP-485 standard wire and accessories required to provide a complete operational system

2.2 The equipment and installation shall comply with the current applicable provisions of the following standards

2.2.1 National Electric Code

2.2.2 Local and state building codes

2.2.3 All requirements of the local authority having jurisdiction

2.2.4 Underwriters Laboratories, Inc.

2.2.5 The system and all components shall be listed by Underwriters Laboratories, Inc., for use in Access Control Systems under the following standards as applicable. UL 294 Access Control System Unit

2.3 All access control panels shall be housed in a cabinet designed for mounting directly to a wall or vertical surface, fire-resistant backplane is required.

2.3.1 Fire rating label shall be visible after installation.

2.3.2 Security panel mounting rack/cabinet as required by manufacturer's specifications.

2.3.3 Panel mounting on fire-rated backplane

2.3.4 The access control panel cabinet shall contain a key lock and shall be physically accessible for flashing, replacement, and upgrading in place.

2.3.5 For new construction and major renovations, this shall be within a dedicated physical access control closet, complete with a dedicated reader and cored physical key access as backup at door entry. Shall be within standard range of OSDP-485 wiring, contain standard power and network jacks, and with connections to uninterruptable power supplies and generator power, where applicable. Only equipment approved by the PSO shall be installed in this closet.

2.3.6 Network And Power Supply

2.3.6.1 Provide one (1) dedicated network jack per planned PACS panel.

2.3.6.2 Each PACS panel group shall have its own dedicated 120V hardwired circuit

2.3.6.3 All outlets wired to individual 20A breakers, with the panel clearly labeled "SECURITY" and room number.

2.3.6.4 Panels with readers shall provide backup power and connect to building generator power if available.

2.3.7 Cable Management And Conduit

2.3.7.1 Shall adhere to Division 26.1.6's wiring requirements. Access control wiring shall have own pathway and shall not share pathway with any other low voltage wiring or cabling.

2.3.8 Room Environment

2.3.8.1 Spaces need to be able to contain all necessary equipment and code-required clearance, with space for future expansion of a minimum of one additional control panel.

2.3.8.2 Room must maintain temperature and humidity within manufacturer's recommendations for PACS and security electronics.

2.3.9 Physical Room Layout

2.3.9.1 Room must be centrally located to serve all planned areas; maximum allowable run from the furthest PACS reader to the control panel is 300 feet.

2.3.9.2 If any reader or controlled opening would exceed 300', a second physical access control closet is required.

2.3.9.3 Access to the physical access control closet must NOT require passing through secure/unrelated spaces (e.g. offices or storage rooms).

2.3.9.4 See Division 28, Section 2.3.13 for location to TR requirement.

2.3.10 Security And Access Control

2.3.10.1 Door to physical access control closet must be solid-core or steel, swing outward, with electronic access tied to the building PACS.

2.3.10.2 Key override using Physical Security Office (PSO) Approved Master Key.

2.3.11 Installation

2.3.11.1 All cable terminations, mounting, and equipment installation must follow manufacturer specifications and industry best practice (NECA 1, NFPA, UL).

2.3.11.2 Coordinate physical layout and panel positioning with the Physical Security Office

2.3.11.3 Grounding must meet requirements for security electronics including NEC and UL 294 for Access Control Systems. Access Control Panels, Enclosures, and Equipment shall be provided with a dedicated equipment grounding conductor, sized per NEC. Access Control Panels shall have a main ground bus bar connected to the building ground system with a minimum #6 ground conduction wire.

2.3.11.4 Document all terminations: Each PACS panel and junction to be clearly labeled and match floor plan/Electronic Security As-Built.

2.3.12 Documentation And Identification

2.3.12.1 Permanently label all PACS panels, control units, and cable terminations.

2.3.12.2 Each label shall include the room number, panel number, and function.

2.3.12.3 Provide digital and printed map of all panel and reader locations, and cable paths. Labels shall be with laminate, no permanent or paint marker is acceptable.

2.3.12.4 All conduit runs, panel connections, and power circuits to be marked/identified for emergency response.

2.3.13 In alignment with Section 27110.2.K of Division 26.19, for new construction and major renovation, Telecommunications Rooms (TR) shall have physical access control readers.

2.3.13.1 The TR and Physical Access Control Closet should be adjacent to each other and share a wall between them.

2.3.14 The integrated access control panel shall provide at least the following capacities

2.3.14.1 Readers/door sensors - 128

2.3.14.2 Credential Capacity – 64,000

2.3.14.3 Configure Alarm Conditions/Alarm Points - 128

2.3.14.4 Access Levels - Unlimited

2.3.14.5 Time Zones - 8

2.3.14.6 Password Levels - 2

2.3.14.7 Card Issue Levels - 8

2.3.14.8 Reports – 5

2.3.14.9 Connectivity to physical panic buttons for integration

2.3.15 The system shall be capable of storing at least 64,000 credentials per access control panel

2.3.16 The system shall be capable of storing card transactions in a single log location based on the free space availability of the server or servers configured for the purpose

2.3.17 A user definable limit shall cause the operator interface to warn the operator when the number of transactions in the file has exceeded that limit

2.3.18 The access control panel shall integrate with surveillance system (Avigilon) and where cameras and readers/sensors are present together, integrate on a one-to-one basis with a bi-directional integration between Avigilon VMS and the Centralized Physical Access Control Solution, adhering to modern ONVIF protocol standards.

2.3.19 The entire database of the physical access control system shall be definable at an Operator Workstation or secured cloud-based web portal

2.3.20 The operator interface shall allow the operator to perform commands including, but not limited to, the following

2.3.20.1 Override All Doors or group of doors to unlocked or locked-down state by administrator command.

2.3.20.2 Release Overrides for individual doors at per-reader/door basis

2.3.20.3 Command reader to alter status to enable access where prior state was locked-down

2.3.20.4 Command reader to alter status to locked-down where prior state was enable access

2.3.20.5 Command reader to temporarily unlock an individual door or group of doors

2.3.20.6 Configure/Silence Local Alarm Conditions for individual door or group of doors

2.3.21 System operators shall, from the operator interface, be able to manually unlock controlled doors for a variable time period, or program an event to automatically unlock and lock doors during a particular time period

2.3.22 Reports

2.3.22.1 Shall be generated automatically or manually, and directed to network devices, printers, or file storage

2.3.22.2 At minimum, the system shall allow the operator to easily obtain the following

2.3.22.2.1 List of all cardholders/credentialed users

2.3.22.2.2 List of all transactions currently available in any access group or sub-group of credential users or readers

2.3.22.2.3 Reports shall also allow constraining to any specific reader or reader group in a given time-frame.

2.3.23 The system shall provide on-line query generation which can be used to obtain specific information from the above logs based on user defined parameters. These queries, once defined, may be stored and used again when needed

2.3.24 The system shall be provided complete with all equipment and documentation necessary to allow an operator to independently perform the following additional functions

2.3.24.1 Add/Delete/Modify Access Control Panels

2.3.24.2 Add/Delete/Modify Readers

2.3.24.3 Add/Delete/Modify Cardholder User Data

2.3.25 Graphical programming shall be used to define processes whereby other FMS functions may be controlled by a valid Credential transaction

2.3.26 At least 1024 cardholder/credential groups shall be definable per access control panel connected

2.3.27 The Access Control Panel shall communicate with the Readers of the system, if connection is lost, reader shall maintain functionality with last known approved credentialed users.

2.3.28 Failure of a Reader shall be detected and reported to the system in real time.

2.3.29 When a card or other credential is read at a reader, the card number and issue level are sent to the control panel. If the reader is equipped with a keypad, an at least 4-digit PIN may be entered and verified at the reader. PIN devices shall not be the sole method of access for any door. The controller, which shall be programmed to control access by both location and time periods, shall verify all information and immediately grant or deny access and record the transaction including date, time and location. If access is granted, the controller shall send a signal to the appropriate reader to activate the door lock. If access is denied, the transaction will be recorded identifying the reason.

2.3.30 The system shall be capable of supporting Magnetic Stripe card, Near Field Communication (NFC), Bluetooth (BT), and Mobile Credentials each with Custom Key provided by LSU where applicable. Each reader must be compatible and support integration with biometric authentication (BioStar). The system shall be designed to maintain access control through two levels of degradation. The control panel shall continue to provide, using its local database, a full level of access control upon loss of communications with the Physical Access Controls Management System. Upon loss of

communications with the control panel, the readers shall continue to control access using verification of the facility code in the Credential and, if used, a PIN entry.

2.3.31 The system shall be able to designate certain readers to control only entry or exit, and shall require a cardholder/credentialed user using a card at an entry reader to subsequently use it at an exit reader before again entering the secured area. This shall prevent “passing back” a card to an unauthorized second user

2.3.32 Individual cards/credentials may be programmed for special privileges to override access level and time zone parameters

2.3.33 The controller shall provide an interface which permits data to be collected on site via USB connection.

2.3.34 In the event of a power loss, a backup battery shall provide full controller operation for up to eight hours, and memory retention of at least 24 hours. Other requirements are specified in Division 26.12.

2.3.35 Physical credentials shall be able to be programmed into the solution individually; additions, deletions, and changes shall be completed in real time, such as for visitors and guest users.

2.3.36 Alarm Conditions may be programmed by the operator for suppression during specific time periods. The controller shall provide an output for annunciation of alarms

2.3.37 The control panel shall provide a buffer to store at least 1024 historical transactions per control panel if communication is lost with the Physical Access Controls Management System. Panel should continue operation if connection between it and the solution/system is lost in offline model.

2.3.38 The readers shall consist of mechanisms to read magnetic stripe, NFC, Bluetooth, and Mobile Credentials, each with Custom Key support. All new-install readers shall support EV1, EV2, EV3. All readers shall support the disabling of magnetic stripe support as required by LSU. No authentication or other credential shall be permitted without approval through the PSO.

2.3.39 The reader shall control the electric door lock, visual access indicators, access and shunt timers, and an auxiliary access input for integrations required for proper functionality of all connected hardware.

2.3.40 The reader shall monitor door status as referenced in 1.10

2.3.41 All readers shall provide a visual and audible indicator for granted and denied access, and tamper detection capability

2.3.42 Readers shall be surface or flush mounted. Outdoor readers shall be supplied with special weather-resistant housings. Where required, readers shall be configured with integral 16-position keypads. All readers shall meet ADA height and access requirements, where required, integrate with ADA door openers

2.3.43 Readers with 16-position keypads shall be able to verify PIN codes even during loss of communications with the control panel. If the readers lose communications with control panel, they shall be able to determine authorized access based on the facility code and PIN, if used, which shall be verified at the reader

2.3.44 Readers that are capable of proper operation without the need of standoffs when mounted to walls containing substantial amounts of metal construction shall be available.

2.3.45 At the system owner’s request, the manufacturer shall provide NFC cardstock compatible with the readers, panels, and physical access control solution utilized, programmed to operate under LSU Custom Key environment

2.3.46 Standard cards shall be available with minimal printing and permanently marked with respective card number and reference code. Magnetic Stripe card, Near Field Communication (NFC), Bluetooth (BT), and Mobile Credentials each with Custom Key provided by LSU is to be used

2.3.47 All Card Access Control parts shall comply with the following

2.3.47.1 For exterior and egress pathway doors, electrified crash bars are the standard hardware method for card access doors and must be compatible with access system and wiring

harness. Request to Exit (REX) sensor shall be integrated within the electrified crash bar itself, rather than on an external motion detector. Configurable alarm conditions for local alarm shall include statuses referenced in 1.10, with signal to control panel is standard.

2.3.47.2 For new construction and major renovations, core through door, electrified hinge loop, and conduit to the reader shall be standard. Magnetic Lock: No magnetic locks are to be used. If an exception is granted by the PSO and the Louisiana Office of State Fire Marshal, the magnetically locked door shall not be the sole method of egress from the secured location.

2.3.47.3 Crash Bar and Cable: Provide double pole, double throw with release button

2.3.47.4 Door contacts - Provide door status contacts that mount to surface of door and frame.

2.3.47.5 Provide 4" x 4" button for egress where called for with low-profile operator where ADA access is required, complete with integration to door hardware.

2.3.47.6 Power Supply - Provide 12/24-volt, UL Listed, power supplies with independent load switches and battery backup

2.3.48 Warranties

2.3.48.1 Manufacturers' standard warranties to cover defects in materials and workmanship

2.3.48.1.1 Warranty period to begin at date of substantial completion and shall not be less than one year for any part.

2.3.48.1.2 Copies of all warranties shall be provided to LSU at completion of the project.