

Electronic Safety and Security Design and Construction Standard

1. General

- A. Owners shall be involved in the planning and design of all electronic safety and security projects.
- B. Buildings shall be equipped with access control and video surveillance.
- C. Mississippi State University has standardized on the Genetec Security Center unified security platform as the required access control and video management product for the campus. All installed access control and video management systems shall be based on the Genetec Security Center unified security platform.
- D. The contractor shall be required to customize the ACS per the requirements of the project. The contractor shall be responsible for coordinating with the Mississippi State University Life Safety Division for programming all ACS features and functions.
- E. Programming of ACS features and functions shall be conducted by a Genetec Licensed integrator.
- F. All hardware must be home run to the ACS panel. No hardware shall be physically connected to perform a task outside of the ACS panel, but should be programmatically connected unless otherwise approved.
- G. Renovations and additions will be reviewed to determine if existing electronic safety and security systems (Total Card access and/ or video surveillance) should be changed to Genetec Security Center unified security platform.
- H. All licensing for device connections on Genetec Security Center unified security platform (access and video) will be purchased per RFP 17-16.

2. Related Work

- A. Division 08 – Door Hardware
- B. Division 14 – General Elevator Requirements

3. Definitions

- A. Monitored: Utilizes door position switch, latch bolt monitor, and/or request to exit devices.
- B. Controlled: Any monitored opening that utilizes electronic locking.

4. Access Control Function Definitions

- A. ACS – Access Control System
- B. AEO – Acceptable exit only: Request to exit, latchbolt monitoring, door position contacts.
- C. ALPR – License Plate Recognition
- D. BRDR – Biometric reader, acceptable entrance: Biometric reader (fingerprint, hand geometry), electrically unlocking hardware, request to exit, latchbolt monitoring, door position contacts.
- E. CSA – Client Software Application
- F. DCO – Door contact only: Door position contact.
- G. DGM – Dynamic Graphical Maps
- H. DRDR – Dual card reader entrance: Dual card reader (card in/ card out), electrically unlocking hardware, latchbolt monitoring, door position contact. Pushbutton override on safe side.
- I. EEO – Emergency exit only: Latchbolt monitoring, door position contacts.

- J. EES – Emergency exit with sounder: Latchbolt monitoring, door position contacts, locally audible piezo sounder connected to access control system.
- K. PEAE – Programmable entrance, acceptable exit: Electrically unlocking hardware, request to exit, latchbolt monitoring, door position contacts.
- L. RDR - Single card reader entrance, acceptable exit: Single proximity reader, electrically unlocking hardware, request to exit, latchbolt monitoring, door position contacts.
- M. SDK – Software Development Kit
- N. SMA - Software Maintenance Agreement
- O. SSM – Server Software Module
- P. UI – User interface
- Q. USP – Unified Security Platform
- R. USW – Unified Web Client
- S. VMS – Video Management System

5. Building/ Space Security Level Definitions

- A. Definitions are provided to establish minimum security requirements.
- B. The level of security required will be dependent on the function of the facility and of specific space within the building.
- C. Individual spaces within a building may have differing Security Levels. All spaces shall be reviewed with the Owner.
 - i. Level 1: Low Risk – All campus buildings and facilities, not otherwise defined below.
 - 1. Spaces are accessible during normal working hours and locked after hours.
 - 2. Exterior doors have alarms that register in the software and trigger an associated camera.
 - 3. Exterior doors will have self-closers.
 - 4. Scheduled exterior doors shall have electronic locks.
 - 5. Occupants are responsible for locking/ unlocking of interior doors.
 - 6. Install video surveillance cameras in the following locations:
 - a. All exterior openings
 - b. Coverage of entire loading dock, if applicable.
 - ii. Level 2: Moderate Risk – Buildings, or spaces within building or facilities in which information of a confidential nature is stored or otherwise maintained. This category includes, but not limited to, human resource file rooms, student record rooms or others regulated by privacy acts and areas for proprietary research or sensitive operational information.
 - 1. All items in Level 1, plus self-closers on interior doors.
 - 2. Spaces are locked when unoccupied.
 - 3. Provide video surveillance cameras to storage rooms.
 - iii. Level 3: Substantial Risk – Areas, buildings or other spaces known to be , or logically assumed to be , targeted for destruction, disruption or vandalism by individuals or groups, as well as areas of specific safety concern to students, faculty, visitors, or staff. These areas include, but not limited to, the College of Veterinary Medicine, buildings which house controlled substances and student dormitories.

1. All items in Level 2, plus electronic locks/readers and self-closers on selected interior doors, card access on elevators to restrict floors, cameras to monitor secure spaces, and emergency lockdown buttons on large capacity rooms.
 2. Door alarms may also be local, audible alarms.
 3. Provide video surveillance cameras in adjacent parking lots, walkways and stairwells.
 - iv. Level 4: High Risk – Areas used for storage or utilization of hazardous chemicals or materials, and laboratories known to or intended to house potentially dangerous biological agents (BSL 3 and above). Buildings and spaces have restricted access.
 1. All items in Level 3, plus intrusion detection system, card reader on main door to exit.
 2. Elevators and stairwells shall be capable of limiting access.
 3. Some areas may require 2-factor authentication (card + pin, biometric + card or pin) to enter.
 4. Provide video surveillance cameras for monitoring hazardous materials and/or biological safety cabinets and laboratory storage areas.
6. Site Security
 - A. Structural barriers such as bollards and fencing shall be installed at the primary and secondary entrances to prevent vehicular approaches and intrusion.
 - B. Landscaping shall be selected and placed such that opportunities for concealment are minimized.
7. Video Surveillance
 - A. Video surveillance equipment shall be compatible with Genetec Security Center unified security platform.
 - B. Video surveillance cameras shall have sufficient resolution and be located such that recognizable images of individuals are captured by the Genetec Security Center system.
 - C. Provide dedicated electrical circuit(s) on the emergency or back-up power system for the Genetec Security Center system.
 - D. Video surveillance equipment shall be compatible with Genetec Security Center 5.6 unified security platform. A supported device list can be found at <https://www.genetec.com/solutions/resources/supported-device-list>.
 - E. Video surveillance cameras shall be fixed unless otherwise noted.
 - F. Video surveillance cameras shall be hard-wired, Ethernet connected devices utilizing TCP/IP communication protocol.
 - G. All system wiring for video surveillance cameras shall be **grey**, plenum rated CAT6 or greater for all camera distances up to 90 meters from the nearest distribution frame with cable shielding following the camera manufacturer's installation guidelines. Lengths exceeding 90 meters will require fiber optic cable with encoders and decoders, as required.
8. Openings, General
 - A. When the entry door into a space has access control functionality, all other doors into that space shall be electronically monitored.

- B. Openings with multiple doors shall have a single reader controlling a single opening. Access control readers shall control only one opening.
 - C. For double-leaf doors, a keyed removable mullion shall be provided.
 - D. Any opening with a reader shall have keyed override. The key for the override will be on a separate keying system for access control doors. This key will be "restricted" for release.
 - E. Door operator actuator shall only be active when door is electronically unlocked.
9. Openings, Exterior
- A. All exterior doors shall be controlled or monitored.
 - B. All exterior doors will have video surveillance cameras.
 - C. Exterior doors which are not hinged, such as sliding doors, overhead coiling or similar openings shall be monitored, less latchbolt monitor.
 - D. Main entrances shall be monitored and controlled by card reader(s). Where an automatic door operator is installed, that door shall be equipped with a card reader.
10. Opening, Interior
- A. Main entrances into auditorium shall be controlled by readers.
 - B. ITS rooms shall be controlled by readers.
 - C. Transformer vaults, electrical rooms and mechanical rooms shall be controlled by readers.
 - D. Lab spaces to be controlled by readers will be determined by the level of security required. Evaluation will be conducted by the Electronic Safety and Security Committee.
 - E. Openings into classrooms will be evaluated by the Electronic Safety and Security Committee requirements for auto-lock and auto-unlock features through the access control system. These electronically controlled spaces shall have an emergency locking pushbutton located near the lectern. A single pushbutton should operate all doors in the space.
11. Interior spaces
- A. Camera placement will be determined on a project basis.
12. Building Miscellaneous Security
- A. Roof hatches shall be locked at all times from the inside and electronically monitored through the access control system.
 - B. All windows within 6' of grade plane shall open 6" maximum.
13. System Description
- A. The University has standardized on a unified security platform manufactured by Genetec. Specifically, the system is Security Center which is comprised of IP video surveillance and access control.
 - B. A room or rooms with sufficient wall space for future expansion shall be identified for the installation of unified security platform equipment including database units, door control units, racks and power supplies. The preference is for all equipment to be co-located in ITS communication room(s) or datacenters that is centrally located in the building. The room may be located up to 250' from an opening.

- C. Coordination with Owners and Design Professional to identify doors that shall have electronic monitoring, locks, cameras and any other security equipment.
- D. All buildings shall be designed to allow the capability of being locked down individually from all others.
- E. For new and major renovations, as a minimum: all exterior doors shall be monitored/ alarmed and main entrances shall have electronic locks/ alarms and proximity readers. The Design Professional shall review the condition of existing doors and hardware for compliance with applicable codes and advise the owner of necessary/recommended replacement or upgrades.
- F. All electronically locked/monitored exterior doors shall have a camera installed.
- G. Departmental requests for additional access control doors and cameras shall be on a case-by-case basis.

14. Products

- A. Acceptable Products:
 - i. Approved access control equipment and systems manufactured by Genetec, Mercury Security and HID which conform to this section of the specifications will be acceptable.
 - ii. Magnetic locking systems are not allowed. In some instances, magnetic locking systems may be required due to facility requirements in which case an approved variance is required. All life safety codes will apply to magnetic locking systems.
 - iii. For all exterior doors, not located inside the building, hardware must be exterior rated and installed per manufacturer's specifications and instructions.
 - iv. All cameras to be installed must be on Genetec Security Center supported hardware list.
 - v. All cameras to be installed on the exterior must be exterior rated.
- B. Card Readers:
 - i. The ACS shall support a variety of card readers that shall encompass a wide range of functions.
 - ii. Supported readers:
 - 1. Mullion: HID multiclass SE RP15 or equal
 - 2. Standard: HID multiclass SE RP40 or equal
 - 3. PIN required: HID multiclass RPK 40 or equal
 - 4. Biometric: Suprema BioEntry W or equal
 - iii. Readers shall be black. Readers for exterior use shall be weatherproof.
- C. Cards:
 - i. All access cards are existing.
- D. Doors:
 - i. All electronic access control door hardware shall be fail secure unless otherwise required to meet building, fire, or other code.
 - ii. All electronically controlled doors shall require the use of request to exit, door position switch and latchbolt monitor.
 - iii. Doors that require power shall use power transfer device. Door loops shall not be used unless specified for the job.
- E. Door Strikes:
 - i. Rutherford, HES Assa Abloy, or Von Duprin door strikes are acceptable.

- ii. Electronic strike can be surface or flush mounted.
- F. System Intelligent Controller:
 - i. The system intelligent controller shall operate and control access to multiple doors as a total standalone unit with full distributed database and with no dependency on the central system. All valid card numbers, time zones and relay functions shall be loaded into the controller's memory. The multiple reader access control panel shall support wiegand, magnetic stripe, proximity, keypads, barcode, vehicle ID, barium ferrite and biometric devices. The panel shall provide programmable communications ports and power supply with battery backup. The intelligent controller shall be connected to the LAN and receive and transmit data to/from the network file server and client workstations.
 - ii. The Synergis Cloud Link module shall contain 2GB of DDR3 RAM, 16GB on-board SSD, two Gigabit Ethernet ports and four RS485 communications ports. Cloud Link module is to be provided with battery back-up and surge suppression.
 - iii. Battery backup is required in each panel. Battery should be sized for one hour of constant operation.
- G. Mercury-based Intelligent Controller
 - i. The Mercury Intelligent Controller shall communicate between the System Intelligent Controller and the 2 Reader Interface Module. The device shall support Wiegand, magnetic stripe, proximity, keypads, barcode, vehicle ID, barium ferrite and biometric devices. The panel shall provide programmable communications ports and power supply with back-up. The Mercury Intelligent Controller shall be connected to the LAN and receive and transmit data to/from the network file server and client workstations.
 - ii. Mercury EP1502 module shall contain 16MB of RAM, two reader ports, eight supervised inputs and four Form C output relays. The controller shall provide capacity for 240,000 cardholders and 50,000 transactions.
 - iii. The intelligent controller shall communicate with reader interface modules via RS-485 communication bus.
 - iv. Battery backup is required in each panel. Battery should be sized for one hour of constant operation.
- H. Mercury-based 2 Reader Interface Module:
 - i. The 2 reader interface module shall be the microprocessor based interface device between the card readers and the ACS central system. The module shall be compatible with the card readers and ACS equipment specified. The module shall be mounted in metal enclosure with ample space to accommodate equipment necessary for the amount of readers specified and for 20% growth. Metal enclosure may also house power supply for door hardware where specified.
 - ii. Mercury MR52 module shall contain two reader ports, eight general purpose inputs and six Form C output relays.
 - iii. The module shall communicate to the Mercury intelligent controller via RS-485 communications bus.
 - iv. Battery backup shall be required inside each panel. Battery shall be sized for one hour of constant operation.
- I. DC Power Supply

- i. Provide low voltage power supply units associated with the interface modules and door control panels and as required to provide 12 and 24 volt regulated, filtered DC power for locking controls, DC locks, signal devices and readers. Output power shall be 12 or 24 volts DC with ampere rating not less than 150% of load imposed on the power supply under most load conditions. DC output shall be fused. Output voltage shall be regulated within plus or minus 5% from no load to full load. Power supplies shall be UL Listed.
 - ii. Battery backup shall be required inside each power supply enclosure. Battery shall be sized for one hour of constant operation.
- J. Field Hardware Power Supplies
 - i. Auxiliary power supplies for doors or other field that require power outside of that provided by the ACS shall be located as close as possible, but no more than 20 feet from the door or field device that is being powered.
- K. Door Position Switch (DPS):
 - i. Door position switches shall be recessed mounted. $\frac{3}{4}$ " door position switches will be required for all steel/ metal doors.
 - 1. Sentrol 1078 series or equal
 - ii. Where surface mount switch is required, door position switch shall be provided with a supervision loop and shall have flexible armored cable.
 - 1. Sentrol 2700 series or equal
 - iii. Overhead door contacts shall be provided with armored cable and be surface mounted. The floor mount units shall be constructed with a low-profile heavy cast aluminum housing. The reed switch assembly shall be fully encased in polyurethane potting material to prevent damage due to moisture or humidity.
 - 1. Sentrol 2200 series or equal
 - iv. Door position switches shall be UL Listed and warranted for two years.
- L. Request to Exit Devices (REX):
 - i. Door hardware shall provide free egress.
 - ii. Request to Exit devices shall be used to shunt DPS alarm only and shall not unlock the door hardware.
 - iii. REX devices shall be internal to door where the door and location allows.
 - iv. Motion REX (PIR) devices shall have a wide angle, long range lense to detect motion of personnel exiting through the door. Coordinate exact field mounting location to provide best operation of PIR type Rex device. PIR REX device shall operate at 9.0 to 16.0 VDC and have Form C output contacts rated at minimum 24 VDC / 0.5 amps.
 - 1. Bosch DS series or equal
 - v. When REX is provided in door hardware, REX signal must be sent prior to door physically unlocking. REX signal should be sent on initial operation of level handle on panic bar.
- M. Panels and Enclosures:
 - i. Physical panel box type shall be equal to the Life Safety FlexPower MClass Integrated Mercury Power system or Altronix Trove2M series.
 - ii. Tamper switches must be installed on all panels and enclosures.
 - iii. A standardized key must be used for all panels and enclosures.
- N. Cabling:

- i. Tappan Spec. # H916021C or equal for most installations.
- ii. Power wiring for electrified door hardware shall meet manufacturer's specifications.
- iii. All wiring systems shall use stranded copper conductors.
- iv. All wiring shall be in accordance with the manufacturers written recommendations.
- v. All cabling will be continuous from control equipment to door hardware. No splicing is permitted.
- vi. All signal and low voltage wiring shall be plenum rated.
- vii. All security wiring shall be supervised. This includes the monitoring of all inputs.
- viii. All cabling shall be labeled on both ends with identification tabs that use nylon tie straps.
- ix. All Ethernet cabling related to the ACS shall be **white** plenum rated CAT6 or better.
- x. All Ethernet cabling related to the video surveillance shall be **grey** plenum rated CAT6 or better.

O. Transient Voltage Surge Protection:

- i. Protect all equipment against surges induced on all control, video and power cables. All copper cables and conductors which serve as 120v power, control or video conductors shall have surge protection circuits where conductors enter or exit a building.
- ii. Fuses shall not be used for surge protection.
- iii. Surge protection devices shall meet the following:
 1. UL497B
 2. UL1449 (must meet 330v suppression rating)
 3. IEEE Category B impulse and ring waves tests
- iv. Acceptable manufacturers: Northern Technologies, Inc, EDCO, or equal. Products shall be warranted against defects for a period of not less than five (5) years.
- v. Surge protection devices shall be bonded to building grounding system in accordance with NEC Article 250.
- vi. Grounding:
 1. Provide a dedicated, separate No. 6 AWG copper conductor from building grounding system to all security equipment rooms, security equipment cabinets and control rooms.
 2. Connect all lightning protection devices and security equipment non-current carrying metal parts to grounding conductor in accordance with NEC Article 250.
 3. Provide ground bus bar in each equipment room and control room with dedicated ground conductor to each cabinet and enclosure.

15. Submittals:

A. Product Data:

- i. Submit manufacturer's technical product data, including specifications and installation instructions, for each type of system equipment. Include drawings, which contain complete wiring and schematic diagrams and other details required to demonstrate that the system has been coordinated, and will function properly as a system. Drawings shall include floor plan layouts of devices, components, vertical riser diagrams, equipment rack details, elevation drawings of equipment racks, sizes and types of all cables and

conduit. For each IP networked device, label names, room number, switch port number, and patch port number.

B. Test Plan:

- i. Contractor shall submit a test plan that identifies the tests required to ensure that the system meets technical, operational, and performance specifications. The test plan shall identify the capabilities and functions to be tested, and include detailed instructions for the setup and execution of each test. The test plan shall be submitted 15 days before the start of any testing. Owner/ User must approve the test plan before the start of any testing.

C. Acceptance:

- i. It is the responsibility of the contractor to meet with the Division of Life Safety to compare the placement and installation of proper devices with the drawings and specifications. A 100% device by device test will be conducted with the vendor under the supervision of the Office of Life Safety. All punch list items will be furnished to the contractor and must be corrected and verified prior to acceptance of the system.

D. Closeout Submittals:

- i. At the time of final inspection, provide four (4) sets of complete data on the ACS equipment used in the project. This data shall be bound form and shall include all shop drawings required for this project.
- ii. All record drawings shall include "as-built" system interconnection diagrams with major components identified and number and type of interconnecting conductors.
- iii. Submit maintenance and operating instructions on all systems.
- iv. Submit as-built drawings to show conduit layout and wiring for all systems. Contractor is to submit four (4) sets of hard copy As-built drawings and submit electronic files in dwg and pdf formats electronically with the Office of Life Safety.
- v. Contractor is to submit all finalized programming settings, including schedules, user databases, etc.
- vi. Note IP switch port numbers and locations (room number) assigned to the system. This is a requirement for every IP device.

16. System Requirements:

- A. The access control system shall be connected to the Genetec Security Center server, but shall operate independently from other campus buildings.
- B. Access control system equipment shall be located in ITS rooms.
- C. 120 volt emergency power shall be provided.
- D. All lock power supplies shall be direct wired to a dedicated 120 volt circuit. Properly sized backup batteries shall be installed in the power supplies.
- E. ITS room shall have ¾" fire-rated plywood for mounting access control equipment.
- F. Power over Ethernet (POE) switch for surveillance cameras shall be connected to 120 volt emergency power circuit.
- G. Properly sized uninterruptible power supply (UPS) shall be connected to the POE switch.
- H. All field equipment, including but not limited to, card readers and input buttons must be mounted in compliance with all codes and regulations.

17. Wiring Systems:

- A. All wiring must be installed in conduit unless otherwise agreed upon by the Office of Life Safety.
- B. The work under this section includes the installation of all wiring for electric door hardware. The installation of the door hardware and the actual connections to the electric hardware and the ACS shall be done under this section. It is the responsibility of the Security Contractor to coordinate all electrical requirements and connections of the electrified hardware.
- C. All security wiring shall be labeled at the control equipment and the field device.
- D. All security wiring shall be supervised. This includes monitoring of all inputs.
- E. The contractor is responsible for running all network cable between each networked device and to each networking closet as required for device communication.

18. Testing:

- A. All door hardware shall be tested prior to inspections. Where door hardware installations are impacted by existing doors of hollow metal frames, contractor shall immediately notify Mississippi State University Office of Planning, Design and Construction and provide, in writing, information on existing deficiency and corrective measure required to complete the project.
- B. Equipment and systems will not be accepted until the required inspections and tests have been made demonstrating that the ACS conforms to the specified requirements, and that the required systems, systems and documentation have been provided.

19. Warranty:

- A. The contractor shall warrant the ACS for one year from date of receiving substantial completion from the Owner/ Users against defects in equipment or workmanship. Failed equipment shall be replaced by the contractor at no cost to the Owner. The Office of Life Safety may perform initial troubleshooting, but replacement of failed equipment and escalated problem support will be handled by the contractor.