



28 13 00
SECURITY AND ACCESS CONTROL

1. GENERAL – For UGA Athens Campus Only

- A. Related sections:
 - i. 00 73 01 – Approved Sole Source / Sole Brand
 - ii. 01 41 26.06 – Dining Services
 - iii. 01 77 00 – Project Closeout
 - iv. 08 71 00 – Door Hardware
 - v. 27 00 00 – General Communications Requirements
- B. The UGA Campus in Athens, Georgia has standardized the Genetec Access Control System as the required access control product for the campus. All installed access control systems (ACS) shall be based on the Genetec Access Control system.
- C. The Security Contractor shall provide and coordinate all conduit, raceways, and box system requirements for the Security & Access Control System.
- D. The security contractor must be a certified Genetec Synergis installer and have completed formal, documented training through UGA Access Control Group prior to being awarded a contract to perform work on UGA's campus. All programming must be completed by the contractor at the direction of UGA Access Control group. The security contractor must provide a valid Genetec training certificate prior to installation. Sub-contracting of Genetec equipment installation is not permitted.
- E. The contractor shall be required to customize the ACS per the requirements of the job. The contractor shall be responsible for coordinating with the user group in programming all ACS features and functions.
- F. Students, faculty, and staff can obtain UGA identification cards that shall serve as an ACS credential from the UGA Card Office. These cards can have electronic information embedded and can interface with the ACS. Credentials shall match industry standard ABA and Wiegand formats to communicate with the ACS.
- G. For any work on Biosafety locations, the Contractor, through the Project Manager, shall coordinate with FMD and the UGA Office of the Vice President for Research Office of Biosafety.
- H. The Contractor that performs work on projects including Biosafety level spaces must be authorized by and complete credentials as required by the UGA Office of Vice President for Research Office of Biosafety.
- I. The Design Professional and/or Contractor shall request IP addresses related to the ACS installation through the Project Manager who will request them from FMD Information Technology.
- J. 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 rather be programmatically connected after being home run to the ACS panel unless otherwise approved.
- K. The contractor shall provide all documentation and shall perform all duties involved in obtaining work permits as required to complete the Project. All permitting shall be within the associated city or jurisdiction.
- L. The access control installer shall not subcontract the access control installation.
- M. Quality Assurance



- i. Industry Referenced Standards. The following specifications and standards are incorporated into and become a part of this Specification by reference.
 - a. FCC compliance
 - b. UL compliance
 - c. NEC compliance

2. PRODUCTS

A. Acceptable Products

- i. Acceptable door hardware can be found under Section 08 71 00 Door Hardware.
- ii. Magnetic locking systems are not allowed. In some instances they may be required due to facility requirements in which case an approved variance signed both the Project Manager and FMD is required.
- iii. All exterior, not located inside the building, hardware must be exterior rated and installed as per the manufacturer's specifications and instructions regarding exterior installation.
- iv. Readers must support at least OSDP v2 and OSDP Secure Channel as defined in IEC 60839-11-5.

*Revised
Aug 2025*

B. Card Readers

- i. The ACS System shall support a variety of card readers that shall encompass a wide functional range.
- ii. Supported Readers as required for each job are as follows:
 - a. Wavelynx Ethos readers with UGA Custom Security Keys.
- iii. Readers shall be black in color and shall be weather-proof.

C. Cards

- i. All access control cards are existing.

D. Doors

- i. All security door hardware shall be fail secure unless otherwise required to meet building, fire, or other code.
- ii. All doors shall require the use of at least request to exit and door position switch devices.
- iii. Doors that require power shall use electric hinges or power transfer devices. Door loops shall not be used unless specified for the job.
- iv. Acceptable door hardware can be found under Section 08 71 00 Door Hardware.

E. Door Strikes

- i. Rutherford, HES Assa Abloy or Von Duprin door strikes shall be used. The following are acceptable models:
- ii. Rutherford F2164 (failed locked) / 2364 (failed unlocked) series
- iii. Von Duprin 6100, 6200, 6300 series
- iv. HES Assa Abloy 9600 series
- v. Electric strikes can be surface or flush mounted.

F. Genetec 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, relay pulse times, and alarm point shunt times shall be loaded into the controller's memory. The multiple reader access control panel shall support OSDP, Wiegand, magnetic stripe, proximity, keypads, barcode, vehicle ID, barium ferrite and

*Revised
Aug 2025*



biometric devices. The panel shall provide programmable communications ports, Power supply with backup, TVSS, etc. The System Intelligent Controller shall be connected to the LAN and receive and transmit data to / from the Network File Server and Client Workstations.

- ii. Genetec Synergis Cloud Link module shall contain 2 GB of DDR3 DRAM, 16 GB on-board SSD, two Gigabit Ethernet ports and four RS-485 communication ports. Cloud Link module to be provided with battery back-up, and surge suppression.
- iii. Battery back-up shall be required inside 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 OSDP, Wiegand, magnetic stripe, proximity, keypads, barcode, vehicle ID, barium ferrite and biometric devices. The panel shall provide programmable communications ports, Power supply with backup, TVSS, etc. 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 LP1502 module shall contain 16 MB RAM, two reader ports, eight supervised inputs and four Form C output relays. The module shall provide capacity for up to 240,000 cardholders and 50,000 transactions. The module shall communicate to downstream READER INTERFACE MODULES via RS-485 communication bus.
- iii. Battery back-up required inside 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 readers and Central System equipment specified herein. The module shall be mounted in metal enclosure with ample space to accommodate equipment necessary for amount of readers specified and for 20% future 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. The module shall communicate to the Mercury Intelligent Controller via RS-485 communication bus.
- iii. Battery back-up shall be required inside each panel. Battery should be sized for one hour of constant operation.

I. DC Power Supply

- i. Provide low voltage power supply units associated with Local Interface Units and Door Control Panels, and as required to provide 12 and 24 volt regulated, filtered D.C. power for locking controls, D.C. locks, signal devices, and readers. Output power shall be 24 volt D.C. with ampere rating not less than 150% of load imposed on power supply under most severe conditions of load. D.C. output shall be fused. Output voltage shall be regulated within plus or minus 5% from no load to full load. Power supply shall be UL listed.

Revised
Aug 2025



- ii. Provide low voltage power supply units as required to provide
 - iii. 5 volt regulated, filtered D.C. power for magnetic stripe card readers. Output power shall be 5 volt D.C. with ampere rating not less than 150% of load imposed on power supply under most severe conditions of load. D.C. output shall be fused. Output voltage shall be regulated within plus or minus 5% from no load to full load. Power supply shall be UL listed.
 - iv. Battery back-up shall be required inside each power supply panel.
 - v. Battery should be sized for one hour of constant operation.
- J. Field Hardware Power Supplies
 - i. Auxiliary power supplies for doors or other field devices that require power outside of that provided by the access control system shall be located as close to the door or field device they are providing power for as possible. Power supplies shall be installed no more than 20 feet from the device they are providing power for.
- K. Door Position Switch Contacts
 - i. Overhead Doors - 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. A wide operation gap distance of up to three inches shall be required to prevent false alarms caused by door movement or damaged and loose fitting doors.
 - a. Door contacts shall be GE / Sentrol 2200 series, GRI equivalent, or approved equal.
 - ii. Surface Mount - Door contacts shall be provided with supervised loop and shall have a flexible armored cable with total encapsulation to protect against moisture.
 - a. Door contact for surface mount swing door locations shall be GE / Sentrol 2700 series, GRI equivalent, or approved equal.
 - b. Door contacts for recessed mounted swing or sliding door locations shall be GE / Sentrol 1078, GRI equivalent, or approved equal.
 - iii. Door contact shall have anodized aluminum finish, with stainless steel flexible cable.
 - iv. Door contacts shall be UL Listed and be warrantied for two years.
- L. Request-to-Exit Devices
 - i. Door hardware shall provide free egress.
 - ii. Request-to-exit (REX) devices shall be used to shunt DPS alarm only, and shall not unlock door hardware.
 - iii. REX devices shall be internal to door where the door and location allows
 - iv. Motion REX (PIR) devices shall have wide angle, long range lenses (adjustable) to detect motion of personnel desiring to exit through the door. Coordinate exact field mounting location to provide best operation of (PIR) type (REX) device. (PIR) device shall operate at 9.0 to 16.0 VDC and have form-C output contacts rated at minimum 24 VDC / 0.5 amps. Bosch DS series or approved equal.
 - v. Motion Request to exit devices shall be Bosch DS150i, DS160, or approved equal.



- vi. 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. Motion Detector Devices
 - i. Shall be equal to Tri-tech motion detectors.
 - ii. Shall use at least the three following technologies:
 - a. Passive Infrared
 - b. Microwave
 - c. Digital Signal Processing
- N. Panels and Enclosures
 - i. Tamper switches must be installed on all panels and enclosures
 - ii. Physical panel box type shall be equal to the following Life Safety FlexPower MCLASS™ Integrated Mercury power systems.
 - iii. A standardized key must be used for all panels and enclosures. Project Manager shall coordinate with FMD IT to obtain specification.
- O. Copper System Wiring
 - i. Card reader connection cable shall be shielded twisted-pair OSDP cabling as defined in IEC 60839-11-5. Wiegand cabling shall not be used. Cable must meet minimum NEC requirements for Class 2 wiring.
 - ii. Power wiring for electrified door hardware shall not be smaller than No. 22 THWN or XHHW.
 - iii. All wiring systems shall use stranded copper conductors. Terminations can be made to crimp type screw lug.
 - iv. All wiring systems shall be color-coded so that each conductor for individual lock set is of a distinctive color.
 - v. All wiring shall be in accordance with the manufacturers' written recommendations.
 - vi. All cabling / wiring shall be submitted in a detailed spreadsheet including cut sheets and samples to the Owner prior to any installation.
 - vii. All conductors within junction boxes, pull boxes, and equipment cabinets shall be grouped and laced with nylon tie straps with identification tab, for individual lock sets.
 - viii. All signal and low voltage wire to be plenum rated.
 - ix. All security wiring shall be supervised. This includes monitoring of all inputs.
- P. Transient Voltage Surge Suppression
 - 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 installed at each end and locations where conductors enter or exit a building.
 - ii. Fuses shall not be used for surge protection.
 - iii. Surge suppression devices shall meet the following standards / publications:
 - a. UL 497B
 - b. UL 1449 (must meet 330 Volt suppression rating)
 - c. IEEE Category B impulse and ring wave tests

Revised
Aug 2025



- iv. Acceptable Manufacturers: Northern Technologies, Inc., EDCO, or equal. Product shall be warranted against defect for a period of not less than five (5) years.
- v. All power connections, including 24 VDC and 24 VAC power supplies and direct wired or plug-in 120 VAC power connections, for all systems and components specified herein, shall be equipped with surge suppression devices. Devices shall be bonded to building grounding system in accordance with Article 250 of the National Electric Code.
- vi. Grounding:
 - a. Provide a dedicated, separate No. 6 AWG copper conductor from building grounding system to all security equipment rooms, security equipment cabinets, and control rooms.
 - b. Connect all lightning protection devices and security equipment non-current carrying metal parts to grounding conductor in accordance with Article 250 of the National Electric Code.
 - c. Provide ground bus bar in each equipment room and control room with dedicated ground conductor to each cabinet, enclosure, pull / junction box and all equipment.
- vii. Ground Resistance Measurement:
- viii. Each signal ground system
 - a. D.C. resistance shall be measured between any point on the signal ground bus and the earth ground. An instrument designed specifically to measure the resistance of a point to each earth ground shall be used. The systems subcontractor shall measure ground resistance in accordance with the procedure as outlined by the test equipment manufacturer. Instrument shall be Biddle earth resistance test instrument, or approved equal.

3. EXECUTION

A. Submittals

- i. Product Data: 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 conduits. For each IP Networked device cable label names, patch down room numbers, patch down cable names, patch down port numbers, and switch port numbers must be provided.
- ii. Test Plan: Contractor shall submit a test plan that defines the tests required to ensure that the system meets technical, operational, and performance specifications, 15 days prior to the proposed test date. Owner / User must approve the test plan before the start of any testing. The test plan shall identify the capabilities and functions to be tested, and include detailed instructions for the setup and execution of each test and procedure for evaluation and documentation of the results.



- iii. Manufacturer Certification: Submit a letter from the manufacturer's representative stating the proposed system being submitted for review are in accordance with the recommendations of the manufacturer.
- B. It is the responsibility of the contractor to meet with the appropriate UGA Facilities representative to compare the placement and installation of proper devices with the drawings and specifications. A 100% device by device test will be conducted by the vendor under the supervision of the owner's representative. Punch lists will be developed at that time and furnished to the contractor. All punch list items must be corrected and verified prior to acceptance of the system.
- C. Closeout Submittals
 - i. At the time of final inspection, provide four (4) sets of complete data on ACS equipment used in this Project. This data shall be in 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 certification from system manufacturers that systems are installed in accordance with manufacturer's recommendations and are functioning correctly at the time of final inspection.
 - v. Submit as-built drawings to show conduit layout and wiring for all systems. Contractor to submit four (4) sets of hard copy As-Built drawings and submit electronic files in .dwg and .pdf formats electronically with the owner.
 - vi. Submit corrected point-to-point drawings for all systems with color code to show the actual as-built conditions.
 - vii. Contractor to submit all finalized programming settings, including schedules, user database, etc.
 - viii. Note IP switch port numbers and locations (room number) assigned to the security system. This is a requirement for every IP device.
 - ix. For additional closeout submittals, refer to Section 01 78 00 Closeout Submittals
 - x. Contact the UGA Access Control Team at accesscontrol@uga.edu or 706-542-7551 to obtain Record Drawing Requirements.
- D. System Requirements
 - i. The University of Georgia security and access control systems shall be connected to the dedicated General Building Genetec server but shall operate autonomously from other campus buildings. Tasks such as defining access groups, time zones, generating reports, creating maps, etc. shall be programmed specific to each space.
 - ii. All access control panels must be installed in a building network closet.
 - iii. As per Genetec standard all systems must be installed with one master Cloud Link module which controls Mercury EP1502 modules over the network. The Mercury EP1502 modules then control Mercury MR modules over a RS-485 bus. All field panels must be connected back to the Cloud Link over the network using an EP1502 module. No RS-485 busses should leave the panel enclosures.
 - iv. All field equipment including but not limited to card readers and input buttons must be mounted in compliance with all codes and regulations.



- v. The Contractor shall only use the existing web interface provided by FMD IT as a system interface for End-Users.
- E. Wiring Systems
 - i. All wiring must be installed in conduit unless otherwise agreed upon with the UGA Project Manager.
 - ii. Protect all communication and data equipment against surge induced on all control, sensor and data cables.
 - iii. All cables and conductors which serve as control, sensor, or data conductors shall have surge protection circuits installed at each end that meet the IEEE 472 surge withstand capability test and the electrical transient tests established in UL365.
 - iv. Fuses shall not be used for surge protection.
 - v. The work under this section of the specifications includes the installation of all wiring for the electric door hardware. The installation of the door hardware and the actual connections to the electric hardware and the access control system shall be done under this section of the specifications. It is the responsibility of the Security Contractor to coordinate all electrical requirements and connections of the electrified hardware and to coordinate with & communicate to UGA all work to be done by UGA. Provide necessary instruction in writing.
 - vi. All security wiring shall be labeled at the head end, any separating junction, and at the field device.
 - vii. All security wiring shall be supervised. This includes monitoring of all inputs. Specifications for wire supervision can be requested from the Project Manager.
 - viii. The contractor is responsible for running networking cable between each networked device and to each networking closet as required for device communication. Before plugging into a switch networking cable must be punched into a patch panel. All access control related patch cables must be red. Campus networking requirements can be found under Section 27 00 00 General Communications Requirements.
- F. Testing
 - i. Testing requirements apply to all construction.
 - ii. All door hardware shall be tested prior to inspections. Where door hardware installations are impacted by existing doors or hollow metal frames, contractor shall immediately notify UGA representative and provide, in writing, information on existing deficiency and corrective measure required to allow the completion of the Project.
 - iii. Materials and documentation to be furnished under this specification are subject to inspections and tests. All components shall be terminated prior to testing.
 - iv. Equipment and systems will not be accepted until the required inspections and tests have been made, demonstrating that the access control system conforms to the specified requirements, and that the required equipment, systems, and documentation have been provided.
 - v. Issues log must be turned over at 10 month and 1 year mark. Include all service events conducted to date.
- G. Training



- i. The Contractor shall include in the base Contract all costs required to train operation and maintenance personnel in the use and maintenance of systems provided under this section of the specifications. Training sessions shall be conducted by instructors certified in writing by the manufacturer of the specific system.
 - ii. University of Georgia Facilities shall be staffed by unique UGA personnel, which shall be cross reference to the UGA master database. The contractor shall be responsible for configuring personnel in the Genetec system to use the Project's location.
 - iii. Sessions shall be conducted for not less than two hour periods during normal working hours, i.e., Monday through Friday, 8:00 AM to 5:00 PM. Training session schedules shall conform to the requirements of UGA Facilities; therefore such schedules shall be submitted to UGA for approval not less than two weeks prior to the training session. At UGA's discretion, provisions shall be made to allow owner personnel to participate in final system check out of all systems.
 - iv. Time to be included in base Contracts for specific systems shall be as follows:
 - a. ACS System entirely - 4 hour
- H. Genetec Software Design Requirements
 - i. General
 - a. The contractor responsible for programming the Genetec system is herein referred to as 'integrator'
 - b. The integrator will under no circumstances change any entities or configurations from another integrator without direct permission from the UGA Access Control Project Manager.
 - c. The integrator does not have delete or remove permission for any entities in the system. The removal of any entity in the system must be coordinated with the UGA Access Control Project Manager.
 - d. The integrator shall make no changes to any entities listed as 'Templates'.
 - e. All change requests must be given to the UGA Access Control Project Manager in writing.
 - ii. Partitions
 - a. The integrator is not able or responsible for entering new partitions into the Genetec system.
 - b. If additional partitions are needed the integrator must coordinate this with the UGA Access Control Project Manager.
 - c. The integrator is required to put all entities created by the integrator into the correct partition(s). Partitions will be provided for each location the integrator is responsible for. An additional unique partition is included for each integrator that can be used for testing purposes by that integrator.
 - d. The integrator will not put any entity in the 'Root' partition.
 - iii. Access Control Units
 - a. Set the name of the access control unit to the name of the building or location it is providing security for. Campus maps and UGA building



names can be found here,

<http://www.architects.uga.edu/maps/current>.

- b. Set the building number in the custom field tab. Building numbers can also be found here, <http://www.architects.uga.edu/maps/current>.
 - c. Set the integrator custom field with the name of the installing integrator. Use the full company name and the same name for all similar fields.
 - d. Update the Cloud Link and all downstream hardware to the latest supported firmware revision unless otherwise coordinate with the UGA Access Control Project Manager.
 - e. Initialize and configure the Cloud Link and all downstream hardware.
 - f. IP information will be provided by the UGA Access Control Project Manager.
 - g. Once all downstream devices are configured, rename all objects under the 'Peripherals' tab with the following format:
 - h. Building name - Corresponding Entity name - Peripheral Type (REX, DPS, Lock, etc.) - Interface Board Details - Peripheral name
 - 1) Ex: Building A - Door 1 - REX - EP1502 1 - MR52 2 - Input 1
 - 2) Ex: Building A - EP1052 1
 - 3) Ex: Building A - Unused - EP1502 1 - Input 1
 - i. Set the correct Time Zone and location information under Location.
 - j. All access control units must have their passwords changed from the manufacturer defaults. This must be coordinated with the UGA Access Control Project Manager.
- iv. Cardholders
 - a. The integrator is not able or responsible for entering new cardholders into the Genetec system.
 - b. If adding new cardholders is required for the installation they must be coordinated through the UGA Access Control Project Manager.
 - c. The installation may require the integrator to add access rules or modify other fields for existing cardholders.
 - v. Cardholder Groups
 - a. The integrator is responsible for creating any cardholder groups that are required for the installation.
 - b. The integrator is responsible for adding any cardholders to cardholder groups that are required for the installation.
 - c. The installation may require the integrator to add access rules or modify other fields for existing cardholder groups.
 - d. Cardholder groups shall be used for granting access for cardholders to areas / doors
 - e. Cardholder group names must follow this format:
 - f. UGA Building Name / Department Name Relevant Group Information
 - 1) Ex: UGA Building A Custodial Supervisors
 - 2) Ex: UGA Department B Staff
 - vi. Credentials



- a. The integrator is neither able nor responsible for entering new credentials into the Genetec system.
 - b. If adding new credentials is required for the installation they must be coordinated through the UGA Access Control Project Manager.
- vii. Access Rules
 - a. The integrator is responsible for creating any access rules as required for the installation.
 - b. The integrator is responsible for attaching and configuring access rules to the relevant entities as necessary such as schedules, cardholder groups, doors, elevator, and areas.
 - c. Access Rules shall not be attached directly to cardholders. Access Rules shall only be attached to cardholder groups and then those groups attached to specific cardholders.
 - d. Access rule names must follow this format:
 - 1) UGA Building Name / Department Name Relevant Access Rule Information
 - i) Ex: UGA Building A
 - ii) Ex: UGA Building A Shop
- viii. General Settings
 - a. The integrator shall make no changes to any options under the System Task->General Settings Tab with the exception of Actions.
 - b. Any needed changes here such as custom fields, custom events, etc. must be coordinated through the UGA Access Control Project Manager.
- ix. Actions
 - a. The integrator is responsible for creating and configuring any Event to Actions that are required for the installation, such as alarms.
- x. Roles
 - a. The integrator shall make no changes to any roles under the System Task->Roles Tab.
 - b. Any needed changes here must be coordinated through the UGA Access Control Project Manager
- xi. Schedules
 - a. The integrator is responsible for creating any schedules that are required for the installation.
 - b. The integrator is responsible for attaching and configuring schedules to the relevant entities as necessary such as access rules, doors, and areas.
 - c. For each schedule intended the integrator must create two schedules.
 - d. One schedule must be a 'Weekly' schedule following the name format:
 - 1) UGA Building Name / Department Name Relevant Schedule Information
 - i) Ex: UGA Building A Unlock Weekly Schedule
 - ii) Ex: UGA Building A Shop Alarm Weekly Schedule
 - e. One schedule must be a 'Specific' schedule following the name format:
 - 1) UGA Building Name / Department Name Relevant Schedule Information
 - i) Ex: UGA Building A Unlock Exception Schedule



ii) Ex: UGA Building A Shop Alarm Exception Schedule

- xii. Scheduled Tasks
 - a. The integrator is responsible for creating any scheduled tasks that are required for the installation.
 - b. The integrator is responsible for configuring any scheduled tasks that are required for the installation
- xiii. Macros
 - a. The integrator is not able to create new macros into the Genetec system.
 - b. If macros are required for an installation, the integrator will be responsible for testing those macros outside of the UGA Production Genetec system. Once testing is complete, the macros must be delivered to the UGA Access Control Project Manager for testing by UGA before being created and configured in the system by UGA.
 - c. All changes for macros must follow the process mentioned in Macros Subsection B.
- xiv. Output Behaviors
 - a. The integrator is responsible for creating any output behaviors that are required for the installation.
 - b. The integrator is responsible for configuring any output behaviors that are required for the installation.
 - c. The default output behaviors, such as Normal, Active, Periodic, and Pulse, may be used by the integrator but not modified.
- xv. Reports
 - a. The integrator is responsible for creating any reports that are required for the installation.
 - b. The integrator is responsible for configuring any reports that are required for the installation. This may include automation such as running the reports with a scheduled task or e-mailing the reports to a user or user group.
- xvi. Users
 - a. The integrator is neither able nor responsible for entering new users into the Genetec system.
 - b. If adding new users is required for the installation this must be coordinated through the UGA Access Control Project Manager.
- xvii. User Groups
 - a. The integrator is neither able nor responsible for entering new user groups into the Genetec system.
 - b. If adding new user groups is required for the installation this must be coordinated through the UGA Access Control Project Manager.
- xviii. Alarms
 - a. The integrator is responsible for creating all alarms that are required for the installation.
 - b. The integrator is responsible for configuring all alarms that are required for the installation.



- c. The integrator shall use the copy configuration tool to create new alarms. New alarms must be created by copying all of the configurations from the 'Empty Alarm Template' alarm.
- d. Any configuration changes from the default 'Empty Alarm Template' alarm must be coordinated with the UGA Access Control Project Manager.
- e. For all installations the following alarms must be created for relevant entities:
 - 1) Door Forced Alarms
 - 2) Door Held Open Alarms
 - 3) Input / Zone Alarms
 - i) Ex: Glass Break, Motion Sensor, etc.
 - 4) Each alarm must have its corresponding entities attached in 'Attached Entities' section.
 - i) Ex: Door 1 at Building A must have a door forced alarm and a door held open alarm created and Door 1 must be added under the 'Attached Entities' Section.
 - 5) Alarm names must follow the name format:
 - i) UGA Building Name Entity Name Alarm Type
 - a) Ex: UGA Building A Door 1 Door Forced Alarm
 - b) Ex: UGA Building B Room 238 Door Held Open Alarm
 - c) Ex: UGA Building C Hallway 1 North Glass Break Alarm

xix. Maps

- a. The integrator is responsible for creating maps for all areas included in their installation. The integrator shall use basic floorplan maps, use an appropriate map size for the area, and crop / remove any extraneous information from the map as necessary.
- b. The integrator is responsible for configuring maps for all areas included in their installation.
- c. All maps must be readable. At all zoom levels maps must display solid and clearly defined lines and walls along with legible text from the imported map source.
- d. Configuration must include:
 - 1) A readable text field noting the name of the building and area
 - i) Ex: Building A - Floor 1
 - ii) Ex: Building B - North
 - 2) The addition of all doors and inputs to the map.
 - 3) A compass rose must be included and correctly positioned on the map.
- e. For multi-area, multi-floor, multi-building, or any combination therein the map must contain links to all corresponding areas. This must be accomplished through the usage of text boxes placed on the map in such a way as to not impede the viewing of any points on the maps.
- f. Zone inputs must be represented on the maps as input entities.



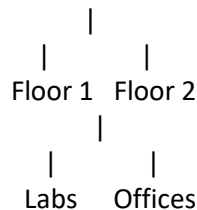
- g. If a single map can encompass multiple areas it can be set on the parent area of the multiple areas.

- 1) Ex: A small building with a single floor is split into two areas on either side of the building. A single map can be used on the building area to represent both child areas.

xx. Areas

- a. The integrator is responsible for creating new areas that are required for the installation.
- b. The integrator is responsible for configuring areas that are required for the installation.
- c. If the integrator needs a new partition for a new area this must be coordinated through the UGA Access Control Project Manager
- d. The integrator shall set all relevant access rules for the area
- e. Area naming formats must follow a tree structure with the building or location as the root.

- 1) Ex: Building A



xxi. Doors

- a. The integrator is responsible for creating new doors that are required for the installation.
- b. All doors shall have their Card Readers programmed in OSDP mode and Secure Channel mode with encryption must be configured and enabled. Card readers shall not be programmed in Wiegand mode.
- c. The integrator is responsible for configuring doors that are required for the installation.
- d. The integrator shall use the copy configuration tool to create new doors. New doors must be created by copying all of the configurations from the 'Door Template' door under the Root->Templates area.
- e. Any configuration changes on the door properties tab from the default 'Door Template' alarm must be coordinated with the UGA Access Control Project Manager.
- f. The integrator shall set all relevant hardware points under the hardware tab.
- g. The integrator shall set all relevant access rules for the door. The preferred use of access rules would be to inherit them from a parent area.
- h. The integrator shall set all relevant schedules for the door. This must include both a 'Weekly' and 'Specific' schedule as mentioned in the schedules section.

*Revised
Aug 2025*



- i. The integrator must set the integrator custom field with the name of the installing integrator. Use the full company name and the same name for all similar fields.
 - j. Door names must follow the name format:
 - 1) Building Name EXT / INT Door Name
 - i) Ex: Building A EXT Door 1
 - ii) Ex: Building B INT Door 238
 - k. Door descriptions must include information relevant to the purpose of the room or provide additional information helpful for locating the door.
 - 1) Ex: Exterior Stairwell Northwest Corner
 - 2) Interior Lab Near Northwest Stairwell
- xxii. Elevators
- a. The integrator is responsible for creating new elevators that are required for the installation.
 - b. All elevators shall have their Card Readers programmed in OSDP mode and Secure Channel mode with encryption must be configured and enabled. Card readers shall not be programmed in Wiegand mode.
 - c. The integrator is responsible for configuring elevators that are required for the installation. This includes floor information, access rules, schedules, and advanced data.
 - d. The integrator must set the integrator custom field with the name of the installing integrator. Use the full company name and the same name for all similar fields.
 - e. Elevator names must follow the name format:
 - 1) Building Name Elevator Name
 - i) Ex: Building A Main Elevator
 - ii) Ex: Building B Service Elevator
- xxiii. Zones
- a. The integrator is responsible for creating new zones that are required for the installation.
 - b. The integrator is responsible for configuring zones that are required for the installation. This includes properties, arming, and cameras.
 - c. The integrator must set the integrator custom field with the name of the installing integrator. Use the full company name and the same name for all similar fields.
 - d. The integrator shall use only hardware zones. If a virtual zone is required for the installation its creation and configuration must be coordinated through the UGA Access Control Project Manager.
- xxiv. Video Units
- a. The integrator is responsible for creating new video units that are required for the installation.
 - b. The integrator is responsible for configuring video units that are required for the installation.

*Revised
Aug 2025*



- c. The integrator must set the integrator custom field with the name of the installing integrator. Use the full company name and the same name for all similar fields.
- d. All video units must use SSL or other secure communication protocols. Any exceptions must be coordinated with the UGA Access Control Project Manager.
- e. All video units must have their passwords changed from the manufacturer defaults. This must be coordinated with the UGA Access Control Project Manager.
- f. All video units must have their firmware updated to the latest version. Any exceptions must be coordinated with the UGA Access Control Project Manager.
- g. IP information will be provided by the UGA Access Control Project Manager.
- h. Video unit names must follow the name format:
 - 1) Building Name Camera Function Description
 - i) Ex: Building A North Parking Lot
 - ii) Ex: Building B Main Stairwell First Floor

xxv. Cameras

- a. The integrator is responsible for creating new cameras that are required for the installation.
- b. The integrator is responsible for configuring cameras that are required for the installation.
- c. The integrator must set the integrator custom field with the name of the installing integrator. Use the full company name and the same name for all similar fields.
- d. Camera names must follow the name format:
 - 1) UGA Building Name Camera Function Description
 - i) Ex: Building A North Parking Lot
 - ii) Ex: Building B Main Stairwell First Floor
- e. If multiple cameras come from the same video unit the names must include information to denote which camera they are and how they relate to the video unit. The description must also include information on how locate each camera
 - 1) Ex:
 - i) Name: Building A North Parking Lot Camera 1
 - ii) Description: Camera on pole next Main Street

xxvi. Monitor Groups

- a. The integrator is responsible for creating new monitor that are required for the installation.
- b. The integrator is responsible for configuring monitor groups that are required for the installation.

xxvii. Plugins

- a. The integrator is not responsible for creating or configuring and shall neither create nor configure plugins unless explicitly stated in the



installation requirements. The creation or configuration of any plugins must be coordinate with the UGA Access Control Project Manager.

I. Warranty

- i. The contractor shall warrant the ACS for one year from date of receiving substantial completion from the Owner / User against defects in equipment or workmanship. Failed equipment shall be replaced by the contractor at no cost to the owner. Owner's personnel may perform initial trouble investigation but replacement of failed equipment and escalated problem support will be handled by the contractor.
- ii. A 10 month warranty inspection must be scheduled and performed by the contractor. This inspection shall include a full site walkthrough and testing of each access controlled point.
- iii. Issues log must be turned over at 10 month and 1 year mark. Include all service events conducted to date.



28 20 00
VIDEO SURVEILLANCE SYSTEM

1. GENERAL

A. General Requirements

i. Related Sections:

- a. 00 73 01 – Approved Sole Source / Sole Brand
- b. 01 77 00 – Project Closeout
- c. 27 00 00 – General Communications Requirements
- d. 28 13 00 – Security and Access Control
- e. UGA Physical Access Control and Video Security Systems Policy

- ii. UGA has standardized on the Genetec Security Center Omnicast IP Video Surveillance System as the required video surveillance management system product for UGA. All installed Video Management Systems (VMS) on UGA properties within Athens-Clarke County are required to be the Genetec Security Center Omnicast IP Video Surveillance System.
- iii. While the use of the UGA Genetec system is available outside of the Athens-Clarke County area, standardization of the Genetec Security Center VMS is not required outside the Athens-Clarke County area. All security camera systems shall comply with this and any other applicable policies, standards, and laws.
- iv. The definition of contractor shall vary based on the size and nature of the project. Examples include for new building construction projects, the General Contractor shall be responsible for the video surveillance systems, for singular system renovation projects, the security contractor or electrical contractor may be responsible for the video surveillance systems. For this standard, “contractor” shall refer to the party responsible for the installation and programming of the video surveillance system
- v. The contractor shall coordinate with the requirements of the UGA Physical Access Control and Video Security Systems Policy (contact UGA PM or download from the UGA Policy Portal website: policy.uga.edu/policy-library/) and Division 28, Section 28 13 00 Security & Access Control System from the UGA Design & Construction Supplemental General Requirements & Standards.
- vi. All Video Surveillance systems must comply with the requirements of the UGA EITS High Bandwidth Consumption Systems Policy (contact UGA PM or download from the UGA EITS policy website: eits.uga.edu/access_and_security/infosec/pols_regs/policies/).
- vii. The contractor shall provide and coordinate all conduit, raceways, and box system requirements for the Video Surveillance System or use pathways provided by others as defined in their contract.
- viii. The contractor must be a certified Genetec Security Center Omnicast installer and have completed formal, documented training through Genetec. All programming must be completed by the contractor at the direction of UGA FMD Access Control group. The contractor must provide a current and valid Genetec training certificate prior to installation.
- ix. The contractor shall be required to program the video surveillance system per the requirements of the job. The contractor shall be responsible for



- coordinating with the user group in programming all camera system features and functions directly or through an already established communication channel through their GC and/or FMD or UGA PM.
- x. For any work on Biosafety locations, the contractor, through the Project Manager, shall coordinate with FMD and the UGA Office of the Vice President for Research Office of Biosafety. The contractor that performs work on projects including Biosafety level spaces must be authorized by and complete credentials as required by the UGA Office of Vice President for Research Office of Biosafety.
 - xi. The contractor shall directly or through an already established communication channel through their GC and/or FMD or UGA PM request IP addresses related to the video surveillance system installation from FMD Access Control
 - xii. All video surveillance cabling must be in compliance with UGA Division 27 00 00 standards. Cabling must be home run to the closest telecom room that allows compliance with the TIA/EIA 90-meter rule.
 - xiii. Every project will be different and will provide a specific responsibility breakdown between General Contractors, Contractors, and Sub-Contractors. The responsibilities of all parties involved in a project to be provided to UGA shall include but not be limited to the following:
 - a. Shop drawings on all video surveillance systems and equipment.
 - b. Installation of all new video surveillance systems and equipment as documented in the drawings and specifications
 - c. Wire and wiring termination for all video surveillance and control systems and equipment.
 - d. Testing and check-out of all video surveillance systems and equipment.
 - e. Warranty for all video surveillance systems and equipment
 - f. As-Built drawings along with operations and maintenance documentation for the complete video surveillance system.
 - xiv. All installations shall require a physical observation walk-through from the UGA FMD Access Control Group. UGA FMD Access Control, or their consultant, shall issue construction observations that shall be corrected prior to the project reaching completion.
 - xv. The contractor or their General Contractor as appropriate for each project shall provide all documentation and shall perform all duties involved in obtaining work permits as required to complete the Project. All permitting shall be within the associated city or jurisdiction.
 - xvi. All Video Surveillance System designs shall be reviewed and approved by the UGA Access Control Committee or their delegates.
 - xvii. Security cameras shall be required at the following locations:
 - a. All exterior entries and exits.
 - 1) A camera shall be mounted on the outside of the building to watch the immediate surrounding exterior area
 - 2) A camera shall be mounted on the inside of the building to focus on the opening and persons using the opening.
 - b. All floor transitions such as stairwells and elevator lobbies.



- 1) A camera shall be mounted in or outside of a stairwell in such a way to be able to monitor all persons entering and exiting the stairwell to each floor.
- 2) A camera shall be mounted in each elevator vestibule to be able to monitor all persons entering and exiting the elevator to each floor.
- c. All alarmed doors and other devices such as duress/panic buttons.
 - 1) A camera shall be mounted near and with a clear view of all devices and doors that alarm to the UGA Police Department.
- d. All areas of refuge where a communication interface is required.
- e. Other locations as determined as appropriate by the department in coordination with the Access Control committee or their delegates.
- xviii. Camera resolution or selection shall be as follows. This section uses the DORI (Detection, Observation, Recognition, and Identification) standards as defined in IEC 62676-4:2014 guidelines or the most recent version.
 - a. Inside buildings, the intent is to locate cameras to allow personnel Identification (DORI) as individuals enter a building or transition between floors. Camera selection should support minimum resolution of 75 pixels per foot or 40 pixels per individual face.
 - b. Outside of buildings, cameras should be located to observe general activity around UGA buildings or select pedestrian walkways. Camera selection should strive to support Recognition (DORI) at 40 pixels per foot or 20 pixels per individual face.
- xix. All video security footage must be stored for a minimum of 30 days. 60 days shall be the preferred retention period. Video security footage should not be stored for longer than 90 days unless required by policy or applicable law. Video retention must comply with USG (University System of Georgia) 'Security Surveillance Records' records retention standards (0472-13-029A, B, and C).
- B. Quality Assurance
 - i. Specifications, Standards and Codes
 - a. All work shall be in accordance with the following (Check with state and local authorities for specific editions which may apply):
 - 1) The National Electrical Code (NFPA 70) with any applicable State Amendments (current adopted edition)
 - 2) The International Building Code with Amendments (current adopted edition)
 - 3) The Life Safety Code (NFPA 101) – (current adopted edition)
 - 4) The National Electrical Safety Code (ANSI C-2) - (current adopted edition)
 - 5) Americans with Disabilities Act (ADA) - (current adopted edition)
 - 6) Local city and county ordinances governing electrical work - (current adopted edition)
 - 7) BICSI TDM Installation Standards - (current adopted edition)
- C. Installer's Qualifications



- i. Contractor with at least 3 years of successful application, installation, and testing experience on specified systems and equipment. All supervisors and installers assigned to the installation of this system or any of its components shall have factory certification from each equipment manufacturer that they are qualified to install and test the provided products. General electric trade staff shall not be used for the installation of the video surveillance system and associated hardware. All installers assigned to the installation of this system or any of its components shall have a minimum of 3 years' experience in the installation of the specified equipment. Sub-contracting of Genetec equipment installation is not permitted.
 - ii. The video surveillance equipment must be provided by a Genetec certified provider.
- D. Submittals
 - i. Pre-Construction Shop Drawings: 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 showing device locations, vertical riser diagrams, equipment rack details, elevation drawings of equipment racks, sizes and type of all cables and conduits.
 - ii. Test Plan: Contractor shall submit a test plan which defines the tests required to ensure that the system meets technical, operational, and performance specifications, 30 days prior to the proposed test date. The test plan must be approved before the start of any testing. The test plan shall identify the capabilities and functions to be tested and include detailed instructions for the setup and execution of each test and procedures for evaluation and documentation of the results.
 - iii. Manufacturer Certification: Submit a letter from the manufacturer's representative stating the proposed systems being submitted for review are in accordance with the recommendations of the manufacturer.
 - iv. It is the responsibility of the contractor to meet with the appropriate UGA representative to compare the placement and installation of proper devices with the drawings and specifications. A 100% device-by-device test will be conducted by the vendor under the supervision of a UGA representative. Punch lists will be developed at that time by the UGA representative and furnished to the contractor. All punch list items must be corrected and verified prior to acceptance of the system.
- E. Drawings
 - i. The Drawings indicate the arrangement of video surveillance equipment. Coordinate installation of equipment with the structural, mechanical and electrical equipment and access thereto.
 - ii. Raceway home runs as shown on the video surveillance drawings shall be installed as shown on the Drawings, and as required by the associated equipment manufacturers.
- F. Record Drawings



- i. At the time of final inspection, provide an electronic file of complete data on Electronic Security equipment used in this project. This data shall include all approved product submittals and 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. Maintenance and operating instructions on all systems.
- iv. Certification from system manufacturers that systems are installed in accordance with manufacturer's recommendations and are functioning correctly at the time of final inspection.
- v. As-built drawings to show conduit layout and wiring for all systems. Contractor to submit electronic copy of As-Built drawings and submit electronic files in AutoCAD (most current version) and PDF formats.
- vi. As-builts to also include corrected point-to-point drawings for all systems with color code to show the actual as-built conditions

G. Warranty

- i. The contractor shall warrant the Video Surveillance System for one year from date of receiving substantial completion from the FMD / User against defects in equipment or workmanship. Failed equipment shall be replaced by the contractor at no cost to UGA. FMD's personnel may perform initial trouble investigation, but replacement of failed equipment and escalated problem support will be handled by the contractor.
- ii. The Contractor shall submit a Warranty Letter as part of the closeout documentation (as-built drawings and Operating Manuals). The Warranty Letter shall state the date on which the warranty starts and the duration of the warranty (in months or years). The letter shall also provide contact information for warranty and service calls. Any special instructions for warranty and service calls must be described.
- iii. A 10-month warranty inspection must be scheduled and performed by the contractor. This inspection shall include a full site walkthrough and testing of each electronic security device.

2. PRODUCTS

A. Products – Video Surveillance General

- i. All cameras shall be U.L. listed and shall be the standard product of one manufacturer complying with not less than the specifications contained herein. Installation of each camera shall include mounting brackets and/or camera housings fully compatible with the camera provided and as required by Security Surveillance System camera schedule.
- ii. All exterior camera locations wired with copper cabling systems and mounted beyond a protected building, shall be provided with Transient Voltage Surge Suppression (TVSS) located within 6FT of the protected device and provided with sufficient ground connection. In addition, TVSS device shall be installed in telecom room in front of network hardware for the protection of telecom room equipment. TVSS shall be rated for Ethernet POE Surge Protection.
- iii. All camera installations shall be securely attached to the mounting surface. Use lead shields on solid masonry, toggle bolts for hollow masonry, and machine



- bolts for steel. All anchoring devices shall be rated to support not less than five times the total equipment weight. Reference mounting details in contract documents.
- iv. It shall be the responsibility of the contractor to ensure all IP addressable devices conform to required IT standards for UGA (https://eits.uga.edu/access_and_security/infosec/pols_regs/policies/) and USG (https://www.usg.edu/information_technology_services/it_handbook/). Security and data protection including things such as the removal of “default” keys/passwords, installation of all current security updates, and responsible record keeping of all IP address, MAC address, security protocol, user ID and passwords. Contractor shall be required to fully coordinate with the UGA FMD Access Control group.
 - v. All exterior camera housings to be provided as matte black per when mounted on red & dark brick surfaces. Provide white/off-white housings on precast, concrete, & stucco surfaces. Coordinate with mounting surface color/conditions. Contractor to follow manufacturer instructions for painting to ensure camera warranty is not voided when manufacturer-colored housings are not available. Preference is to provide colored housings from manufacturer. All painting by the contractor will require 1-year contractor warranty from date of substantial completion and must not void the manufacturer warranty.
 - vi. Additional camera installation requirements:
 - a. All cameras shall be dome-type. Bullet housings shall be avoided unless specifically required by the project.
 - b. Corner mount cameras are not preferred for UGA projects.
 - c. All requirements for mounting on historical structures shall be coordinated and approved by Office of University Architects (OUA).
 - d. General aesthetics shall be prioritized in the installation of all cameras. Coordinate with UGA project manager.
 - e. Cameras shall not be left installed until they are fully operational. Installed cameras shall be covered with screening until fully operational.
- B. Low Light Indoor/Outdoor Day/Night Fixed, 2 Megapixel Cameras
- i. Basis of design is the Axis P3265-LV(E) (or current/modern equivalent) security dome style camera with a I-Pro, Hanwha, or Bosch approved equal. Reference Axis part number for preferred features.
 - ii. All cameras, in this category, shall be equipped with variable focal lenses.
 - iii. When mounted in exterior spaces, the camera shall be outdoor ready with housing that is IK10 vandal resistant.
 - iv. Contractor to reference feature requirements mandated by the installation requirements.
 - v. It shall be the contractor’s responsibility to ensure that the latest supported version of firmware that is compatible with the Video Management System is downloaded to all cameras prior to Final Inspection.
- C. Low Light Indoor/Outdoor Day/Night Fixed, 5 Megapixel Cameras
- i. Basis of design is the Axis P3267-LV(E) (or current/modern equivalent) security dome style camera with a I-Pro, Hanwha, or Bosch approved equal. Reference Axis part number for preferred features.



- ii. All cameras, in this category, shall be equipped with variable focal lenses.
 - iii. When mounted in exterior spaces, the camera shall be outdoor ready with housing that is IK10 vandal resistant.
 - iv. Contractor to reference feature requirements mandated by the installation requirements.
 - v. It shall be the contractor's responsibility to ensure that the latest supported version of firmware that is compatible with the Video Management System is downloaded to all cameras prior to Final Inspection
- D. Low Light Indoor/Outdoor Day/Night Fixed, 8 Megapixel Cameras
- i. Basis of design is the Axis P3268-LV(E) (or current/modern equivalent) security dome style camera with a I-Pro, Hanwha, or Bosch approved equal. Reference Axis part number for preferred features.
 - ii. All cameras, in this category, shall be equipped with variable focal lenses.
 - iii. When mounted in exterior spaces, the camera shall be outdoor ready with housing that is IK10 vandal resistant.
 - iv. Contractor to reference feature requirements mandated by the installation requirements.
 - v. It shall be the contractor's responsibility to ensure that the latest supported version of firmware that is compatible with the Video Management System is downloaded to all cameras prior to Final Inspection.
- E. Multi-Sensor Multi-Directional Camera
- i. Basis of design is the Axis P3719-PLE, 15MP (or current/modern equivalent) multi-directional camera with IR providing 360-degree coverage with a I-Pro, Hanwha, or Bosch approved equal. Reference Axis part number for preferred features.
 - ii. All cameras, in this category, shall be equipped with variable focal lenses.
 - iii. When mounted in exterior spaces, the camera shall be outdoor ready with housing that is IK10 vandal resistant.
 - iv. Contractor to reference feature requirements mandated by the installation requirements.
 - v. It shall be the contractor's responsibility to ensure that the latest supported version of firmware that is compatible with the Video Management System is downloaded to all cameras prior to Final Inspection.
- F. Multi-Sensor Multi-Directional Camera
- i. Basis of design is the Axis P3719-PLE, 15MP (or current/modern equivalent) multi-directional camera with IR providing 360-degree coverage with a I-Pro, Hanwha, or Bosch approved equal. Reference Axis part number for preferred features.
 - ii. All cameras, in this category, shall be equipped with variable focal lenses.
 - iii. When mounted in exterior spaces, the camera shall be outdoor ready with housing that is IK10 vandal resistant.
 - iv. Contractor to reference feature requirements mandated by the installation requirements.
 - v. It shall be the contractor's responsibility to ensure that the latest supported version of firmware that is compatible with the Video Management System is downloaded to all cameras prior to Final Inspection.



G. Fish-Eye 12MP Mini Dome Camera

- i. Basis of design is the Axis M3058-PLVE, 12MP (or current/modern equivalent) Mini dome camera with 360-degree coverage with a I-Pro, Hanwha, or Bosch approved equal. Reference Axis part number for preferred features.
- ii. When mounted in exterior spaces, the camera shall be outdoor ready with housing that is IK10 vandal resistant.
- iii. Contractor to reference feature requirements mandated by the installation requirements.
- iv. It shall be the contractor's responsibility to ensure that the latest supported version of firmware that is compatible with the Video Management System is downloaded to all cameras prior to Final Inspection.

H. Miscellaneous Cameras

- i. As required by contract drawings, project may require numerous other camera types that will be indicated in drawings or supplemental specifications. These cameras shall be Axis, I-Pro, Hanwha, or Bosch approved camera. Contractor to fully adhere to complete project construction documents.
- ii. All non-standard cameras shall be approved by the UGA Access Control Committee or their delegates.

I. Network Video Management System

- i. The IP video surveillance system (VMS) must be compatible with and integrated to the Access Control System (ACS). The contractor shall be responsible for all programming required for camera / alarm linking.
- ii. The UGA Campus Standard VMS is Genetec Security Center.
- iii. General:
 - a. All video streams supplied from analog cameras or IP cameras shall be digitally encoded in H.264 or H.265 compression formats and recorded in real time.
 - b. Each camera's bit rate, frame rate and resolution will be set independently from other cameras in the system, and altering these settings will not affect the recording and display settings of other cameras.
 - c. Audio and Video storage configuration for the VMS shall either be:
 - 1) Internal or external IDE/SATA/SCSI/iSCSI/FC organized in a RAID configuration of at least RAID 10 or manufacturer equivalent.
 - 2) It shall be possible to include within the overall storage system disks located on external PCs on a LAN or WAN as long as the storage is RAIDed as or uses the manufacturer equivalent as stated above such as:
 - i) Network Attached Servers (NAS) on a LAN or WAN as well as;
 - ii) Storage Area Networks (SAN)
- iv. Archiving
 - a. The Archiver (role) shall use an event and timestamp database for advanced search of audio/video archives. This database shall be a Microsoft SQL Server as per Genetec's compatibility matrix.



- b. The Archiver shall protect archived audio/video files and the system database against network access and non-administrative user access.
- c. The Archiver shall provide a pre-alarm and post-alarm recording option that can be set between one second and 5 minutes on a per camera basis. Confirm with UGA FMD Access Control group on exact settings.
- d. Shall provide the functionality of storing of video and audio streams based on triggering events such as:
 - 1) Digital motion detection
 - 2) Digital input activation
 - 3) Macros
- e. The Archiver shall require video motion detection to be provided by each individual camera.
- f. Multiple video streams shall be available from project cameras. The standard video stream setups are:
 - 1) Live/Remote/Low Resolution
 - i) 5 fps
 - ii) At most, one quarter of camera's maximum resolution
 - iii) High compression
 - 2) Recording/High Resolution
 - i) 15 fps
 - ii) Camera's maximum resolution
 - iii) Medium compression
- g. When video network traffic is sent over the campus or any other network, the Archiver shall communicate using current industry standard encryption for traffic including but not limited to authentication and control and management traffic.
- h. All video network traffic from the Archiver to any client applications shall use current industry standard encryption for all network traffic.
- i. The Archiver shall store the Operating System and video storage on separate disk drives.
- j. The Archiver shall be configured to automatically clean-up video after the retention period defined per the Archiver and each camera to be no less than 30 days.
- v. Hardware and Software Requirements
 - a. Contractor to reference the hardware requirements in the Genetec Security Center System Requirements document for the version of Security Center to be installed.
- J. Video Management Server
 - i. Projects that integrate with a centralized campus security video offering shall not require a local video management server. The cameras in this scenario shall connect over the campus network to a central video management server(s).
 - ii. If the project does not integrate with a centralized campus security video offering, the project shall provide a video management server located in secured Main Telecom Room or IDF to support the IP-Based video management system. This local server and project cameras shall be directly connected to new dedicated security network switches in the Telecom Room.



- iii. The Video Management Server must support the current version of Genetec Security Center that UGA is using. Confirm with UGA FMD Access Control group prior to start of project.
- iv. Server storage capacity shall be sized for 60 days unless otherwise specified by the Project. Storage capacity shall be sized for no less than 30 days in all cases. Cameras shall record at a minimum of 15 frames per second. Recording shall be estimated based on each individual camera scene. Furnish calculations with shop drawings verifying storage sizing is compliant with these specifications.
 - a. For interior cameras that record on motion, minimum recording percentage should be 25% with 50% scene activity.
 - b. For interior cameras that record continuously, minimum recording percentage should be 100% with 50% scene activity.
 - c. For exterior cameras that record on motion, minimum recording percentage should be 75% with 50% scene activity.
 - d. For exterior cameras that record continuously, minimum recording percentage should be 100% with 50% scene activity.
- K. IP Cabling Wiring Requirements
 - i. All IP cabling to conform to UGA General Communication Standards. Reference: All video surveillance cabling must be in compliance with UGA Division 27 00 00 standards.
 - ii. All Video Surveillance System cable shall be colored BLUE.
- L. Copper Patch Cables
 - i. All copper patch cables to conform to UGA General Communication Standards. Reference: All video surveillance cabling must be in compliance with UGA Division 27 00 00 standards.
 - ii. Reference one-line diagrams for patch cable quantities and locations
 - iii. Patch cables shall be approximately 2 meters in length or otherwise sized appropriately for the installation.
 - iv. Patch cord colors shall be as follows:
 - a. Jacket color shall be ORANGE for security cameras.
- M. Patch Panels
 - i. All patch panels to conform to UGA General Communication Standards. Reference: All video surveillance cabling must be in compliance with UGA Division 27 00 00 standards.
- N. Gigabit Poe Ethernet Network Switches
 - i. Provided by UGA EITS. No network switching to be provided or installed by contractor.

3. EXECUTION

A. Installation

- i. System components shall be installed in accordance with NFPA 70 (current edition), manufacturer's instructions, and as shown. Necessary interconnections, services, and adjustments required for a complete and operable signal distribution system shall be provided. Penetrations in fire-rated construction shall be fire-stopped in accordance with specifications. Conduits and raceways shall be installed in accordance with the National Electric Code (NEC). Cables shall not be installed in the same cable tray, utility pole



compartment, or floor trench compartment with AC power cables. Metal conduits shall not be continuous between buildings. Contractor to provide ground isolation between buildings by breaking continuous copper cabling and metal conduit runs.

- ii. Surge Protection:
 - a. All exterior camera locations wired with copper cabling systems and mounted beyond a protected building, shall be provided with Transient Voltage Surge Suppression (TVSS) located within 6FT of the protected device and provided with sufficient ground connection. In addition, TVSS device shall be installed in telecom room in front of network hardware for the protection of telecom room equipment. TVSS shall be rated for Ethernet POE Surge Protection.
 - b. Protect all video and data equipment from surges induced on all control, power and data cables. All copper cables and conductors which serve as control, power, or data conductors shall have surge protection circuits installed at each end that meet the IEEE 472 surge withstand capability test. Fuses shall not be used for surge protection.
- B. Programming
 - i. All security devices shall be programmed and use naming schemes as stated in the 28 13 00 – Security and Access Control section 3.H Genetec Software Design Requirements section.
- C. Testing Requirements
 - i. General
 - a. All cables and termination hardware shall be 100% tested for defects in installation and to verify cabling system performance under installed conditions according to the requirements of ANSI/TIA/EIA-568-B.1-3, current edition. All pairs/strands of each installed cable shall be tested per UGA Communication Commissioning standards prior to system acceptance. Any defect in the cabling system installation including but not limited to cable, connectors, feed through couplers, patch panels, and connector blocks shall be repaired or replaced in order to ensure 100% useable conductors/strands in all cables installed.
 - ii. Copper Testing
 - a. All twisted-pair copper cable links shall be tested for continuity, pair reversals, shorts, opens and performance as defined in 27 08 00.
 - b. Continuity - Each pair of each installed cable shall be tested using a test unit that shows opens, shorts, polarity and pair-reversals, crossed pairs and split pairs. The test shall be recorded as pass/fail as indicated by the test unit and referenced to the appropriate cable identification number and circuit or pair number. Any faults in the wiring shall be corrected and the cable re-tested prior to final acceptance.
 - c. Length - Each installed cable link shall be tested for installed length using a TDR type device. The cables shall be tested from patch panel to patch panel, block to block, patch panel to outlet or block to outlet as appropriate. The cable length shall conform to the maximum distances set forth in the ANSI/TIA/EIA-568-B.1-3 Standard, current edition. Cable



lengths shall be recorded, referencing the cable identification number and circuit or pair number. For multi-pair cables, the shortest pair length shall be recorded as the length for the cable.

iii. Test Results

- a. Test documentation shall be provided as an electronic file as part of the as-built package. The file shall be titled "Project Test Documentation", the project name, and the date of completion (month and year). The results shall include a record of test frequencies, cable type, conductor pair (or strand) and cable (or outlet) I.D., measurement direction, reference setup, and crew member name(s). The test equipment name, manufacturer, model number, serial number, software version and last calibration date will also be provided at the end of the document. Unless the manufacturer specifies a more frequent calibration cycle, an annual calibration cycle is anticipated on all test equipment used for this installation. The test document shall detail the test method used and the specific settings of the equipment during the test as well as the software version being used in the field test equipment.
- b. The field test equipment shall meet the requirements of ANSI/TIA/EIA-568-B.1-3 (current adopted edition).
- c. When repairs and re-tests are performed, the problem found and corrective action taken shall be noted, and both the failed and passed test data shall be documented.

D. Labeling Requirements

- i. Labeling shall be done in accordance with the recommendations made in the ANSI/TIA/EIA-606 document, current adopted edition, manufacturer's recommendations, and best industry practices.
- ii. All cables, termination hardware, and equipment shall be labeled with machine-generated wrap around labels.
- iii. All labels shall be white or yellow with black text.
- iv. For all horizontal cables, labels are required at the following intervals: 6" from outlet and 12" from termination block/patch panel on each cable. Also provide labeling on front of patch panel and both ends of patch cable. Total of five (5) labels per each camera.
- v. Labeling scheme shall be alphanumeric and match both as-builts and programmed camera names.
- vi. Contractor shall provide, generate, and install all labeling.
- vii. Labels shall be developed and printed using a software program. No hand-written labels are allowed.
- viii. A Label Report shall be turned over to the FMD or OUA PM at the end of the project. The FMD or OUA PM will provide this Label Report to FMD Access Control.



28 31 00
FIRE DETECTION & ALARM

1. GENERAL

- A. Related sections:
 - i. 00 73 01 – Sole Source / Sole Brand
 - ii. 01 91 13 – General Commissioning Requirements
 - iii. 23 00 00 – General Mechanical Requirements (HAVC)
 - iv. 26 00 00 – General Electrical Requirements
 - v. 26 05 33.13 – Conduit for Electrical Systems
- B. In general, a fire alarm riser diagram is a minimum requirement showing the type of smoke detectors in each floor and each room, locations of smoke detectors in the HVAC system, pull stations, horns, strobe lights and control panel(s). A performance specification shall accompany the riser diagram, describing the control panel make- up, features and construction, the zoning requirements, HVAC and elevator (if any) and door holders (if any) interlock descriptions.
- C. The fire alarm shall be programmed so that the silencing of the alarm allows for the visual notifications to remain on and in 'alarm' mode while muting audible alarms.
- D. All fire alarm cable shall be placed within fire alarm conduit which shall be red in color. Any variance regarding this shall be reviewed and specifically approved by the UGA AVP at FMD or OUA.
- E. No fire alarm devices shall be mounted on the exterior of the building; if Design Professional believes that exterior-mounted fire alarm devices are required by code, the Design Professional shall bring this to the attention of the Project Manager for further discussion.
- F. It is UGA's preference that ceiling mounted horns and/or strobes and smoke detectors be utilized wherever possible in lieu of wall-mounted devices.

2. PRODUCTS

- A. Honeywell: 1-877-841-2840, Farenhyt, for new construction projects that are not facilities operated by UGA Housing. For renovation projects that utilize a different brand, the decision to change to Farenhyt or extend the existing system will be made on a case by case basis. This is a sole brand (refer to Section 00 73 01 Sole Source / Sole Brand).
- B. Honeywell: 1-877-841-2840, Notifier for new construction projects that are facilities operated by UGA Housing. For renovation projects that utilize a different brand, the decision to change to Notifier or extend the existing system will be made on a case by case basis. This is a sole brand (refer to Section 00 73 01 Sole Source / Sole Brand).