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 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. Approved access Control equipment and systems conforming to this section of the specifications manufactured by Genetec, Mercury, and HID will be acceptable.
      ii. Acceptable door hardware can be found under Section 08 71 00 Door Hardware.
      iii. 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.
      iv. 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.
   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. HID Dorado WP644B model or equal
         b. HID RP40 series or equal
      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. 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 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 System 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 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 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 EP1502 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.

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 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 or approved equal.
      b. Door contacts for recessed mounted swing or sliding door locations shall be GE / Sentrol 1078 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 of a type specified by the manufacturer of the ACS System. 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

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 close out 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.

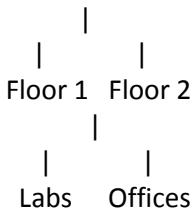
c. The integrator shall use the copy configuration tool to create new alarms. New alarms must be created by copying all of the configurations from the 'Empty Alarm Template' alarm.
d. Any configuration changes from the default 'Empty Alarm Template' alarm must be coordinated with the UGA Access Control 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 following 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 displays 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 additional 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. The integrator is responsible for configuring doors that are required for the installation.
c. 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.
d. Any configuration changes on the door properties tab from the default 'Door Template' alarm must be coordinated with the UGA Access Control Project Manager.
e. The integrator shall set all relevant hardware points under the hardware tab.
f. 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.
g. 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.
h. 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.
i. 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

j. 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. The integrator is responsible for configuring elevators that are required for the installation. This includes floor information, access rules, schedules, and advanced data
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. 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.
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 13 00.01
SECURITY AND ACCESS CONTROL – LEGACY SYSTEM

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
      vi. 28 13 00 – Security and Access Control
   B. All new Access Control Systems (ACS) are required to use the approved sole brand system identified in Section 28 13 00 Electronic Access Control and Intrusion Detection.
   C. This section shall only apply to work on existing installations of the legacy Andover Controls 'Andover Continuum' access control system in cases approved by the UGA Access Control Team (accesscontrol@uga.edu or 706-542-7551). The sole source provider of the Andover Continuum access control system is Operational Security Systems, Inc. (404-352-0025).
   D. For this section "Contractor" shall also mean "ACS subcontractor" unless specifically noted otherwise.
   E. The ACS consists of card readers, biometric readers, keypad readers, intrusion detection sensors, and electric door hardware that are connected to an ACS field panel. The field panel is typically located in a building telecom room (TR) or designated building network location such as an MDF or IDF. The ACS panel is connected to an existing server over the UGA network. This typically requires a direction connection between the ACS field panel and a campus network switch.
   F. Students, faculty, and staff can obtain UGA identification cards that shall serve as an ACS credential. These cards can have electronic information embedded and include magnetic swipe cards or proximity field cards that can interface with the ACS. All magnetic swipe cards, proximity cards, and biometrics shall use industry standard ABA and Wiegand formats to communicate with the ACS.
   G. Server / Database Programming: To maintain security and accuracy, the UGA contracts with Operational Security Systems, Inc. (OSS) to program and provide support for the ACS. Only this vendor is allowed access to the ACS server / database for programming and support information related to ACS installations covered under this section.
      i. The FMD manages the agreement between the UGA and OSS.
      ii. Any ACS programming required as part of work covered under this section are required to be performed by OSS.
      iii. For project delivery methods in which the Contractor is a Construction Manager, Design-Builder, or General Contractor:
         a. The Contractor must contract directly with OSS. The Contractor is not allowed to have an ACS installation subcontractor contract with OSS.
         b. The Contractor shall include in their Bid or Cost of the Work the cost for the Contractor to retain the services of OSS to perform all required ACS programming to make the new facility or renovation ACS fully operational.

H. Any variance request approvals related to Access Control shall be signed by both the Project Manager and FMD IT.
I. Any work on a new or renovated ACS must be completed by a Contractor certified by the ACS manufacturer and the Contractor shall have been in business for at least three years.
J. 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.
K. 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.
L. During the design phase, if any of the following are being considered, the Design Professional and / or Contractor, through the Project Manager, shall coordinate with FMD and the UGA programming and maintenance vendor to ensure functionality with the ACS:
    i. Biometric technology
    ii. Glass Breaks
    iii. Elevator
    iv. Automatic ADA Door Openers
    v. Motion Sensors
    vi. Duress / Panic Buttons
M. The Design Professional and Contractor shall refer to Division 27 00 00 General Communications Requirements of the Standards for all network cabling required to interface with the ACS.
N. 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.
O. The Contractor shall only use the existing web interface provided by FMD IT as a system interface for End-Users.
P. 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 after being home run to the ACS panel.
    i) Example – A push button for a door with a door operator should not connect directly to the door operator to open the door. Both the push button and operator connections must be home run to the ACS panel. Once at the panel the software must be configured to allow the door operator to open when the button is pressed based on the lock state of the door.
Q. Refer to 27 00 00 General Communications Requirements.
    i. Cables shall not be spliced and must be continuous from the field hardware device to the respective ACS panel.
    ii. All cables must be labeled on each end specifying the device type and a specific device identifier.
    iii. All manufacturers' specifications must be followed when joining wiring with all connecting hardware such as wire nuts.

2. **PRODUCTS**

A. All new access control systems are required to be part of the Andover Controls, Andover Continuum system (Andover). The UGA has sole brand approval for this access control system and no substitutions are allowed.
B. Magnetic locking systems are not allowed. In some instances they may be aesthetically appropriate for some historic facilities in which case an approved variance signed both the Project Manager and FMD is required.
C. Magnetic locking systems that require a "Push to Exit" button are not allowed.
D. 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.
E. Door Hardware
    i. General Door Hardware
        a. The following devices must be installed with supervised wiring:
            1) Request to Exit
            2) Door Position Switch
            3) Motion Sensor
            4) Panic / Duress Button
            5) Glass Break Sensor
        b. All door installation shall require the use of no less than a request to exit device and a door position switch device.
        c. All door hardware shall be fail secure.
        d. Doors that require power shall use electric hinges or power transfer devices and door loops shall not be used.
        e. Auxiliary power supplies for doors or other field devices that require power excluding the ACS panel shall be located as close to the door or field device they are providing power for as possible. The location of the power supply shall not exceed 20 feet from the door or device.
    ii. Door Strike
        a. Equal to HES Assa Abloy or Von Duprin
        b. Electric strikes can be surface or flush mounted.
    iii. Locks:
        a. All doors must mechanically relock after removing a key used to unlock or open the door.
    iv. Door Position Switch
        a. Internal door position switches should be used where the door and location allows.
        b. Door position switches shall be equal to GE Sentrol magnetic contact or sensor.
    v. Request to Exit
        a. Request to exit devices shall be internal to the door where the door and location allows.
        b. Mechanical crash bar or turn handle request to exit devices must be used where the door and location allows.
    vi. Motion Detector
        a. Shall be equal to Tri-tech motion detectors.
        b. Shall use at least the three following technologies:

1) Passive Infrared
2) Microwave
3) Digital Signal Processing

vii. Readers: All magnetic swipe and proximity card readers shall be equal to HID.
viii. Keypads: Shall be equal to HID keypads.
ix. Sliding Doors shall use internal locking mechanisms and internal door position switch.

F. Panels and Enclosures
i. Tamper switches must be installed on all panels and enclosures
ii. Physical panel box type
a. Shall be equal to the following Hoffman enclosures:
1) A42N3009
2) A36N24ALP
3) A36N30ALP
4) A30N24ALP
5) A24N24ALP
iii. A standardized key must be used for all panels and enclosures. Through Project Manager coordinate with FMD IT to obtain specification.
iv. Battery Backups
a. Batteries must include labeling that specifies the device that is powered or backed up by the battery and the installation date of the battery.
b. Must provide battery backups that will last at least 1.5 hours at time of installation with an average lifetime of no less than 3 years.

3. **EXECUTION**

A. Installation Performance Test
i. After an ACS installation is deemed complete by OSS an installation performance test must be coordinated and conducted.
ii. The Contractor shall coordinate with the Project Manager for the following attendees to be present at the performance test:
a. Contractor
b. Design Professional
c. Project Manager
d. FMD ACS Project Manager
e. FMD Hardware Technician
f. FMD Software Technician
g. UGA Public Safety Division Police Department
iii. The installation performance test must include but is not limited to the following tests for all related devices:
a. General Door Tests
1) Doors have been rekeyed.
2) Doors open and close without mechanical problems.
3) Doors lock and unlock mechanically for ingress and egress.
b. Card Reader Door Tests
1) Door locks, unlocks, and secures from the ACS manually and with a schedule.

2) Door locks, unlocks, and secures when using a card that is granted access.
3) Door does not lock or unlock when using a card that is not granted access.
4) After a valid card swipe that unlocks the door, if the door is not opened it must automatically lock back after a predetermined amount of time.
5) After a valid card swipe that unlocks the door, if the door is opened it must lock immediately following being opened.
6) Door alarms when forced open and resets when the door is closed.
7) Door alarms when held open longer than the door ajar time and resets when the door is closed.

c. Door Position Switch /
1) Value is 'off' when the door is closed or contact is closed.
2) Value is 'on' when the door is open or contact is opened.
3) Door position switch alarms when its respective door is opened in a manner that should cause an alarm and resets when the door is closed.

d. Request To Exit Tests
1) Value is 'off' when the request to exit is not triggered
2) Value is 'on' when the request to exit is triggered.

e. Contact Tests
1) Value is 'off' when the contact is closed.
2) Value is 'on' when the contact is opened.
3) Contact alarms when the contact is broken and resets when the contact is made.

f. Motion Sensor Tests
1) Value is 'off' when the motion sensor is not triggered
2) Value is 'on' when the sensor is triggered.
3) Motion sensor alarms when its respective space is configured in a manner that should cause an alarm and resets when the motion sensor resets.

g. Tamper Switch Tests
1) Value is 'off' when the tamper switch is not triggered
2) Value is 'on' when the tamper switch is triggered.
3) Tamper switch alarms when the enclosure or object is opened or removed and resets when the enclosure is closed or object is returned

h. Duress / Panic Button Tests
1) Value is 'off' when the duress / panic button is not triggered
2) Value is 'on' when the duress / panic button is triggered.
3) Duress / panic button alarms when the button is pressed and resets when the button is reset.

i. Glass Break Tests
1) Value is 'off' when the glass break is not triggered

2) Sensitivity is set so that the value does not turn 'on' under normal building operation.

j. Door Operator Tests
   1) When triggered, if the door is unlocked, the door operator successfully opens the door and closes the door back within expected time-frame.

k. Push Button Tests
   1) Value is 'off' when the push button is not triggered
   2) Value is 'on' when the push button is triggered.

l. ADA Door Tests
   1) When the exterior push button is triggered while the door is locked the door remains locked and the door operator is not triggered.
   2) When the exterior push button is triggered after a valid card swipe that unlocks the door the door operator opens the door and closes the door back within the expected time-frame.
   3) When the interior push button is triggered while the door is locked the door is unlocked, the door operator opens the door, and closes the door within the expected time-frame.
   4) When the interior push button is triggered while the door is unlocked the door operator opens the door and closes the door back within the expected time-frame.

m. Battery Tests
   1) Devices on battery backups should continue to function for the expected amount of time after external power is removed and the devices are operating solely on battery power.

n. ACS Controller Tests
   1) All internal batteries are connected.
   2) Upon total power loss and restoration of a time period no shorter than five minutes the ACS Controller should automatically initialize itself from internal memory.
   3) After the self-initialization the controller is fully functional with no external interaction.

o. All above and non-listed devices must be tested to ensure complete functionality as specified in the installation contract.

p. All above and non-listed devices must be tested to ensure that there is no found case in which the device shows a 'trouble' state.

B. Warranty Inspection
   i. The original installing Contractor is required to perform a warranty inspection on all installations no later than two months before the end of installation warranty.
   ii. This inspection shall be coordinated with the Project Manager and FMD.
   iii. The warranty inspection must follow the test criteria specified in the "Installation Performance Test" above.

C. Closeout Submittals
   i. Drawings

a. A copy of all installation drawings shall be delivered to Project Manager for distribution at the completion of the job. Refer to Section 01 78 00 Closeout Submittals.
b. The drawings shall include but not be limited to:
    1) Wiring diagrams shall be included with locations of wire runs between all devices. The drawing must contain the ACS aliases of the devices the wiring connects. This shall also include network cable installations.
    2) For network cable installations punch-down and port number information must be clearly shown at the location on the drawing that the network cable from the ACS plugs into the campus network equipment.
    3) Riser diagrams for the ACS panel shall be included and labeled with the ACS aliases for all of devices contained within.
    4) Drawings shall include floor plans with the mentioned wiring diagrams and must also include locations of all field and panel devices and any supporting devices such as auxiliary power supplies.

ii. Documentation
a. A copy of all installation documents shall be delivered to the Project Manager to distribute at the completion of the job. These documents will be provided in pdf formats.
b. The documentation shall include but no be limited to:
    1) IP address, IP Gateway, IP Netmask, and device MAC information of the ACS panel installed.
    2) Punch-down and network hardware port numbers that the ACS devices connect to.
    3) Manufacturer's documentation for all installed devices.
    4) All procedural documents for custom development done for the installation. These shall include but not be limited to:
        i) Summary of the development done
        ii) Instruction documentation on how to use the development
        iii) High level overview of all features of the development. This shall be detailed enough that it could be used to support the development.

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. All fire alarm cable not in conduit shall be red in color. Refer to Section 26 05 33.13 Conduit for Electrical Systems. Fire alarm cable is not required to be in conduit unless specifically required by codes (for example, for a smoke evacuation system). Fire alarm cable not in a conduit shall be plenum rated.
   D. **FMD Project Only:** All fire alarm cable shall be placed within in fire alarm conduit which shall be red in color.
2. **PRODUCTS**
   A. Honeywell: 1-877-841-2840, Silent Knight, 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 Silent Knight 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).