1. **GENERAL – For UGA Athens Campuses Only**
   A. Related sections:
      i. 00 73 01 – Approved Sole Source / Sole Brand
      ii. 01 77 00 – Project Closeout
      iii. 08 71 00 – Door Hardware
      iv. 27 00 00 – General Communications Requirements
   B. All new Access Control Systems (ACS) are required to use the approved sole brand system identified below under Part 2. PRODUCTS.
   C. For this section “Contractor” shall also mean “ACS subcontractor” unless specifically noted otherwise.
   D. 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 direct connection between the ACS field panel and a campus network switch.
   E. 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.
   F. Server / Database Programming: To maintain security and accuracy, the UGA contracts with a third party vendor 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 new or renovated ACS installations
      i. The FMD manages the agreement between the UGA and the ACS third party programming and maintenance vendor.
      ii. Any ACS programming required as part of a new construction or modifications to an existing building with ACS, are required to be performed by the UGA programming and maintenance vendor.
      iii. Unless they are the UGA programming and maintenance vendor, the subcontractor that installs or modifies ACS in a building is not authorized to make the associated database programming changes.
      iv. For project delivery methods in which the Contractor is a Construction Manager, Design-Builder, or General Contractor (the ACS installation subcontractor is not acting as prime):
         1. **The Contractor must contract directly with the UGA current programming and maintenance vendor. The Contractor is not allowed to have an ACS installation subcontractor contract with the UGA current programming and maintenance vendor for the programming.**
         2. **The Contractor shall include in their Bid or Cost of the Work the cost for the Contractor to retain the services of the UGA programming and maintenance vendor to perform all required ACS programming to make the new facility or renovation ACS fully operational.**
v. For project delivery method in which the ACS installation subcontractor is the prime Contractor (is directly contracted with the Owner):
   1. The ACS installation subcontractor is not allowed to contract with the UGA current programming and maintenance vendor for the programming. In this situation, the UGA will contract directly with the UGA current programming and maintenance vendor for the programming.

G. Any variance request approvals related to Access Control shall be signed by both the Project Manager and FMD IT.

H. 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.

I. 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.

J. 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.

K. 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

L. 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.

M. 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.

N. The Contractor shall only use the existing web interface provided by FMD IT as a system interface for End-Users.

O. 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.

P. 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
         1. The following devices must be installed with supervised wiring:
            a. Request to Exit
            b. Door Position Switch
            c. Motion Sensor
            d. Panic/Duress Button
            e. Glass Break Sensor
         2. All door installation shall require the use of no less than a request to exit device and a door position switch device.
         3. All door hardware shall be fail secure.
         4. Doors that require power shall use electric hinges or power transfer devices and door loops shall not be used.
         5. 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
          1. Equal to HES Assa Abloy or Von Duprin
          2. Electric strikes can be surface or flush mounted.
      iii. Locks:
          1. All doors must mechanically relock after removing a key used to unlock or open the door.
      iv. Door Position Switch
          1. Internal door position switches should be used where the door and location allows.
          2. Door position switches shall be equal to GE Sentrol magnetic contact or sensor.
      v. Request to Exit
1. Request to exit devices shall be internal to the door where the door and location allows.
2. Mechanical crash bar or turn handle request to exit devices must be used where the door and location allows.

vi. Motion Detector
1. Shall be equal to Tri-tech motion detectors.
2. Shall use at least the three following technologies:
   a. Passive Infrared
   b. Microwave
   c. 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
   1. Shall be equal to the following Hoffman enclosures:
      a. A42N3009
      b. A36N24ALP
      c. A36N30ALP
      d. A30N24ALP
      e. 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
   1. Batteries must include labeling that specifies the device that is powered or backed up by the battery and the installation date of the battery.
   2. 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 the installing contractor 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:
        1. Contractor
        2. Design Professional
        3. Project Manager
        4. FMD ACS Project Manager
        5. FMD Hardware Technician
        6. FMD Software Technician
        7. 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:
        1. General Door Tests
           a. Doors have been rekeyed.
b. Doors open and close without mechanical problems.
c. Doors lock and unlock mechanically for ingress and egress.

2. Card Reader Door Tests
   a. Door locks, unlocks, and secures from the ACS manually and with a schedule.
   b. Door locks, unlocks, and secures when using a card that is granted access.
   c. Door does not lock or unlock when using a card that is not granted access.
   d. 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.
   e. After a valid card swipe that unlocks the door, if the door is opened it must lock immediately following being opened.
   f. Door alarms when forced open and resets when the door is closed.
   g. Door alarms when held open longer than the door ajar time and resets when the door is closed.

3. Door Position Switch/
   a. Value is ‘off’ when the door is closed or contact is closed.
   b. Value is ‘on’ when the door is open or contact is opened.
   c. 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.

4. Request To Exit Tests
   a. Value is ‘off’ when the request to exit is not triggered
   b. Value is ‘on’ when the request to exit is triggered.

5. Contact Tests
   a. Value is ‘off’ when the contact is closed.
   b. Value is ‘on’ when the contact is opened.
   c. Contact alarms when the contact is broken and resets when the contact is made.

6. Motion Sensor Tests
   a. Value is ‘off’ when the motion sensor is not triggered
   b. Value is ‘on’ when the sensor is triggered.
   c. Motion sensor alarms when its respective space is configured in a manner that should cause an alarm and resets when the motion sensor resets.

7. Tamper Switch Tests
   a. Value is ‘off’ when the tamper switch is not triggered
   b. Value is ‘on’ when the tamper switch is triggered.
   c. Tamper switch alarms when the enclosure or object is opened or removed and resets when the enclosure is closed or object is returned.

8. Duress/Panic Button Tests
   a. Value is ‘off’ when the duress/panic button is not triggered
   b. Value is ‘on’ when the duress/panic button is triggered.
c. Duress/panic button alarms when the button is pressed and resets when the button is reset.

9. Glass Break Tests
   a. Value is ‘off’ when the glass break is not triggered
   b. Sensitivity is set so that the value does not turn ‘on’ under normal building operation.

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

11. Push Button Tests
    a. Value is ‘off’ when the push button is not triggered
    b. Value is ‘on’ when the push button is triggered.

12. ADA Door Tests
    a. When the exterior push button is triggered while the door is locked the door remains locked and the door operator is not triggered.
    b. 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.
    c. 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.
    d. 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.

13. Battery Tests
    a. 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.

14. ACS Controller Tests
    a. All internal batteries are connected.
    b. 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.
    c. After the self-initialization the controller is fully functional with no external interaction.

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

16. 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
      1. A copy of all installation drawings shall be delivered to Project Manager for distribution at the completion of the job. See section 01 78 00 Closeout Submittals.
      2. The drawings shall include but not be limited to:
         a. 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.
         b. 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.
         c. Riser diagrams for the ACS panel shall be included and labeled with the ACS aliases for all of devices contained within.
         d. 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
      1. 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.
      2. The documentation shall include but no be limited to:
         a. IP address, IP Gateway, IP Netmask, and device MAC information of the ACS panel installed.
         b. Punch-down and network hardware port numbers that the ACS devices connect to.
         c. Manufacturer’s documentation for all installed devices.
         d. 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.