Design Standard

Electronic Security Systems

This standard was created on February 27th, 2024. Future changes and updates will be marked with an underline. Please refer to Part 4 of this standard for full revision history.

PART 1 - GENERAL

1.1 NOTICE OF CONFIDENTIALITY

A. Security system work is critical to the security of Texas A&M University. Plans, specifications and other documentary material and information about the security system are confidential information and shall remain secure and confidential. Confidential information shall not be deliberately or inadvertently disclosed to anyone other than the Contractor's personnel and subcontractors who require disclosure to perform their portion of the work. Track confidential information and ensure that copies are accounted for and properly destroyed when no longer needed to perform the work.

1.2 PURPOSE

A. Establish design criteria, define activities, identify stakeholders and assign responsibilities as they relate to the installation of electronic access control systems for the TAMU College Station campus. This standard is intended for Facilities Planning and Construction (FP&C) projects, SSC Services for Education (SSC) projects, Campus Planning Design and Construction (CPDC) projects and the TAMU Keyless Administration Team shop.

1.3 OVERVIEW

A. The electronic safety and security systems for TAMU buildings and facilities are managed and maintained by the Keyless Administration Team (day to day operations) and Campus IT (backbone and communications). The primary function of these security systems is to protect the campus population and assets. The University Police Department (UPD) will monitor and respond to all approved security alarms that are a part of this campus security system. The hardware and installation requirements listed in this guide must be in full compliance in order to obtain infrastructure maintenance support by the Keyless Administration Team, Technology Services and alarm monitoring by UPD.

B. Prior to commencing work in an existing building contact Building Access and Security (979-2845-1207, facse@tamu.edu) to notify him of location, activities, and start/finish times of necessary work.

1.4 ELECTRONIC SECURITY SUPPORTED AT TAMU COLLEGE STATION

A. Card Access Control. This system replaces the typical mechanical key-controlled door lock with a door locking system that uses an access card (physical card or mobile credential) as the access credential. This provides added features including:

1. Monitor and document building access activities.
2. Student/staff ID functions as the access card.
3. Tailored access privileges for each user.
4. Card user access privileges can be deleted or modified without retrieving the issued access
5. Automatic card deactivation when a student, visitor or employee role becomes inactive.

6. Individual University Departments control their facility access-controlled doors via a web interface.

7. Cancellation of all privileges in case of lost or stolen card

8. Locking or unlocking doors performed by automatic schedule or manually via software.

B. Each system may include: an electric door-locking mechanism, card reader located adjacent the door, door status sensor, door prop alarm and a request to exit device. Typical system configuration is card or schedule-controlled entry with free exiting. To access the controlled area, users must present their cards to the card reader located near the door. The door will unlock momentarily and relock. If the door is held open or propped, a local warning buzzer will sound to remind the user to close the door before an alarm message is transmitted to the UPD. Card access can also be used to control elevator functions.

C. Emergency Delay Exit Door. The emergency delay exit door system operates as a fire code compliant (NFPA 101) emergency exit door but will not open until a 15 second delay period has expired after an exit attempt has been initiated. Local siren sounds immediately to alert local staff of attempt to exit and police receive message with location and specific alarm information. A local fire alarm triggers the immediate release of the door(s). Local controls or programmable time schedules can be used to override this security function. Typical installations include back or side code required exits to labs, exterior building emergency exit doors and stairwell doors. These systems may also be used with card readers in interior egress applications; however, these interior applications should be provided on a limited basis only to secure areas accessed through egress doors.

1.5 SOFTWARE LICENSES

A. The Installing Vendor shall provide each license as required by the ACSMS manufacturer for this project.

1. Access Control System Integration licenses for each IP Enabled Access Control lock to function and operate as an extension of the Access Control System. Capable of supporting alarms and events as noted by the Access Control System manufacturer.

2. Provide quantities as required.

1.6 REFERENCES – (LATEST PUBLISHED VERSION AT DATE OF CONTRACT DOCUMENTS)

A. Americans with Disabilities Act (ADA)

B. Crime Prevention Through Environmental Design (CPTED)

C. NFPA 70 – National Electric Code (NEC)


E. NFPA 730 – Guide for Premises Security

F. NFPA 731 – Standard for the Installation of Electronic Premises Security

G. Underwriter’s Laboratories (UL) Applicable Standards
H. NECA 1 – Standard Practice of Good Workmanship in Electrical Contracting
I. Telecommunications Industry Association (TIA) Applicable Standards
J. Institute of Electrical and Electronics Engineers (IEEE) Applicable Standards
K. Texas A&M University Design Standards
L. Texas A&M University System Facility Design Guidelines
M. Occupational Health and Safety Act (OSHA)
N. Texas Accessibility Standards (TAS)
O. International Building Code (IBC)

1.7 SECURITY SYSTEM VENDORS
A. Software – Avigilon
B. Access Control - Avigilon
C. Card Readers – HID
D. Video Management System - Avigilon

1.8 QUALITY ASSURANCE
A. Contractor Qualifications
   1. Each Bid must include information that clearly indicates that Bidder meets each of the following minimum qualification requirements:
      a. Bidder must have experience installing Avigilon systems and be a certified integrator
      b. Bidder must have minimum five years of experience supplying equipment and performing services similar in size and scope to those required for this project.
      c. Bidder must have an office in the College Station area within 100 miles of the University.
   2. A single security systems integration contractor shall provide the work specified in this guide and have a minimum of five years’ experience in the fabrication, assembly and installation of systems of similar complexity as specified herein.
   3. The security contractor shall work directly for the GC and not as a subcontractor under another trade.
   4. The security contractor shall maintain a service facility and organization with staffing capable of providing comprehensive maintenance and service for the specified systems within a 100-mile radius of The Texas A&M College Station campus.
   5. The security contractor shall have local in-house engineering and project management capabilities consistent with the requirements of the project. Provide a team managed by a project manager and field supervisor responsible for submittals, installation, scheduling, manpower, testing, record documents, etc. The field supervisor shall be on-site during all work activities to ensure quality, compliance with contract documents and coordination with other trades.
6. The contractor shall maintain a spare parts inventory necessary to resolve component failures of the system. Spare part inventory shall include the following:
   a. Control boards
   b. Card readers
   c. Power supplies
   d. Door position switches
   e. Door management units

B. Integrator Qualifications
   1. Installer Qualifications: Installers, verifiably authorized and in good standing with the primary product manufacturers, with a minimum 5 years’ experience installing integrated access control hardware similar in material, design, and scope to that indicated for this Project and whose work has resulted in construction with a proven record of successful in-service performance.
      a. Factory Training: Installation and service technicians are to be competent factory trained and certified personnel capable of maintaining the system.
   2. Integrated IP-Enabled access control products that comply with current University standards are required to be supplied and installed only through designated “Authorized Channel Partner” (ACP), “Certified Integrator” (CI) and “Preferred Installer” (PI) accounts

C. Documentation to include with Bid Proposal
   1. Proof of security contractor licenses from the Texas Department of Public Safety’s Private Security Bureau for both the firm and employees working on-site.
   2. Proof of on-site personnel manufacturer certifications, training and licenses as required to purchase, install, modify, and service the specified systems.
   3. Provide a list of three projects within the last five years that utilize the specified systems. For each project, provide a name, location, description, date of completion, contact name and contact phone number.
   4. Maintain factory trained and certified technicians. Certified technicians shall install and terminate security riser closet equipment including DGPs, terminal cabinets, and power supplies and shall supervise installation, commissioning, and maintenance of the work. All installing personnel shall be licensed as required by local and/or state jurisdictions. The contractor shall maintain certification information for each technician at all times and shall provide certifications to the general contractor, security consultant and TAMU Project Manager for verification and record.
   5. If the contractor has been involved with any litigation or criminal action with a client or government agency within the past five years, provide full details and status of each occurrence.
   6. Specification Compliance
      a. Provide a specification compliance statement indicating compliance or deviation for each item in the specification. The statement shall be comprised of a list of all numbered paragraphs that appear in this Specification.
      b. Indicate compliance of the proposed equipment and/or services by the word “Comply” following each paragraph number.
      c. Indicate an exception to the requirement by the word “Exception” following the applicable paragraph number.
d. Should the proposed equipment and/or services not entirely comply with the requirements specified, but ultimately achieve the intent, the Bidder shall indicate the clarification to the requirement with the word "Clarification" followed by a full explanation of the extent of compliance for the applicable equipment and/or services proposed.

e. Instances where there is no indication of compliance or exception shall be considered non-compliant.

f. This compliance statement is critical for proposal evaluation. Failure to submit may result in the disqualification of the proposal.

1.9 SUBMITTALS

A. Produce submittal drawings using the latest version of AutoCAD. Printed drawings shall be at least half size drawing that are suitable to show in readable detail all elements of the project, including any text or symbols.

B. Provide submittals within 30 days of contract award.

C. Prior to installation the submittals shall be reviewed and approved by the security consultant and TAMU Facility Access & Security leader.

D. Submittals shall include:

1. Equipment schedules necessary to identify products that will be provided for the project. Schedules shall include description, manufacturer, model, and quantity for each product.

2. Manufacturers’ product data sheets for all components of the security system provided by the project. These product data sheets should provide descriptive literature, illustrations, installation instructions, information on compliance with applicable standards, dimensions, model number, electrical characteristics, support requirements, connection requirements and all applicable information to verify compliance with specifications. Where more than one part number is listed on a manufacturer’s data sheet, highlight the applicable information.

3. Floor plans necessary to identify specific device locations, cable routes and quantities, cable types, riser locations, and references to installation details and diagrams.

4. Floor plans should also indicate electronic door hardware type and voltage for each door when these devices are controlled by the security system. This can be accomplished with symbols or keyed notes.

5. Camera systems should include Avigilon system design tool showing camera location and pixels per ft.

6. Device termination details necessary to ensure consistent installation by all personnel and subcontractors.

7. Control panel termination details and schedules necessary to ensure that installation personnel and subcontractors properly connect devices to the DGP, power supplies, transition equipment, and other head end equipment.

8. Complete installation drawings including system block and functional diagrams of all systems and subsystems. Terminal point to point wiring diagrams for each type of device including correct terminal or connector pin designations.

9. Power supply points listing with devices and maximum loads to prevent overloading.
10. Riser diagram showing routes between floors or other areas that are not easily identified on the floor plans.

11. Detailed elevation drawings showing DGP and associated panel layouts.

1.10 OPERATION AND MAINTENANCE MANUAL

A. Submit one electronic copy of the security O&M Manual to TAMU Keyless Administration Team at the conclusion of the project. The security O&M Manual shall conform to the following:

1. Name, address, and phone number of nearest representative of each project contractor and sub-contractor.

2. Table of contents

3. Tabbed sections including:
   a. Theory of operation, design philosophy, specific functions
   b. System block diagram
   c. List of system associated mechanical locking keys with key codes and tamper resistant hardware types
   d. Equipment list, including a brief description, model, and the total number of each item used in the project.
   e. Rack and wall elevation layouts
   g. Maintenance requirements for equipment, inspections and preventative maintenance schedules.
   h. As-built drawings for each floor. Each drawing shall show: cable type and identifier, actual cable routing pathway, device number and device input/output number.

1.11 SIGNAGE

CONSTRUCTION SCHEDULE

A. The completion of the security system is heavily dependent on work by other trades. To ensure coordination with these other trades the security contractor will be responsible for providing a detailed construction schedule.

B. The schedule shall include all relevant security activities, estimated completion dates, duration of each activity and predecessor activities by other trades that impact security activities.

C. The security contractor shall provide a preliminary schedule for all security work. Schedule shall conform to requirements listed in paragraph B above. Throughout the installation the security contractor shall provide written updates at least once every two weeks to the general contractor, consultant and TAMU Project Manager. This schedule will allow the GC and owner to verify progress and identify any issues early on that will impact the overall construction schedule.

1.12 WARRANTY

A. The contractor shall warranty the completed work to be free of defects in workmanship and materials for a period of one year from the date of system acceptance.

B. If the workmanship or materials are found to be defective or not in accordance with the contract documents during the warranty period, the contractor shall make corrections promptly with factory certified technicians at no cost to the owner. All labor and materials shall be provided by the contractor.
C. The contractor shall provide the Keyless Administration Team and Campus IT with a 7 days per week 24 hours per day phone number that will respond to warranty service calls. A technician is required to be on-site within 8 hours of placing the warranty service call and the repair shall be completed within 24 hours of site arrival.

D. The contractor shall provide loaner equipment for any device that cannot be repaired in the field. Loaner equipment shall be functionally and technically equivalent to the replaced item.

E. Immediately following a warranty service request, the contractor shall provide written notice to Campus IT and the general contractor confirming that a factory certified technician is being dispatched to the site with a schedule for repair. Include the technician’s name and contact information.

F. After warranty service work is completed, the contractor shall provide written notice to Campus IT providing details on the service work completed, cause of trouble and any other outstanding issues with a timeline on correcting them.

G. The Owner reserves the right to expand or add to the system during the warranty period using firms other than the contractor for such expansion without affecting the contractor’s responsibilities, provided that the expansion is done by a firm which is an authorized dealer or agent for the equipment or system being expanded. Contractor shall not be responsible for maintenance of equipment installed by other firms.

PART 2 - PRODUCTS

2.1 GENERAL

A. All products and materials shall be new and approved in the pre-installation submittals.

B. Exterior devices shall be sealed and protected against weather conditions including heat, cold, moisture, dust, and sand.

2.2 BUILDING ACCESS CONTROL SYSTEM (BACS)

A. System Description

1. Provide Security panels, HID Signo series card readers, and alarm input and output devices connected to the campus Avigilon security management system. HID readers shall be custom readers with TAMU encryption.

2. Provide power to locks and connect the locks to a DGP auxiliary relay to provide for card reader or BACS control of doors.

3. Card Reader Controlled Doors

   a. Card reader-controlled doors shall include:

      1) Card Reader.
      2) Double pole, double throw (DPDT) magnetic door position switch for each door leaf.
      3) 24 VDC electric locking mechanism with integral request to exit (REX) switch.

   b. Typical Configuration

      1) Wire normally closed REX switch output to the REX input.
      2) The Door shall automatically relock after the door opens after a valid card read access.
5. Card Reader Controlled Doors with Automatic Door Operators
   a. Configure doors with automatic door operators as follows:
      1) Free Exit Side Push Plate
         a) The push plate shall function at all times.
         b) When pressed, the door operator push plate shall:
            i. Signal the interface controller to unlock the door and provide closed REX signal to the DGP.
            ii. Signal the door operator to open the door.
      2) Card Reader Unlock Mode
         a) The door shall be unlocked.
         b) The card reader-controlled side door operator push plate shall be enabled.
         c) When pressed, the door operator push plate shall signal the door operator to open the door.
      3) Card Reader Locked Mode
         a) The door shall be locked.
         b) The card reader-controlled side door operator push plate shall be disabled.
         c) Upon a valid card read, the DGP shall provide a signal to the interface controller to:
            i. Unlock the door.
            ii. Enable the card reader-controlled side door operator push plate.

6. Access Controlled Doors without a Card Reader
   a. Emergency exit only doors
      1) Emergency exit only doors shall include:
         a) Double pole double throw (DPDT) magnetic door position switch for each door leaf.
         b) Door Management Unit (DMU)
      2) Anytime this door is opened the DMU will sound immediately, and an alarm will be sent to UPD.
   b. Exit doors with request to exit switches:
      1) Exit doors with request to exit switches shall include:
         a) Double pole double throw (DPDT) magnetic door position switch for each door leaf.
         b) Request to exit switch integral to door hardware
      2) Anytime this door is opened without a request to exit signal, an alarm will be sent to UPD.
      3) Remote Sounder activation if the door is held open longer than an adjustable time after a valid access. Coordinate exact times for each door with Campus IT.

7. Card Reader Controlled Elevators
a. Provide card reader in elevator car panel and associated digital output relay control of elevator floor select buttons. Individual digital output relays are needed for each floor select button in each elevator equipped with a card reader. Provide cabling from access control panel to elevator demarc panel. Provide individual control for each floor select button for each elevator door.

b. When an elevator is in the card reader control mode, the floor select buttons shall be disabled. The passenger shall be required to hold their access card up to a card reader mounted in the elevator return panel. Upon a valid card read, the BACS shall enable the floor select buttons the passenger is authorized to access. The passenger shall then push the desired select button. Once the passenger has pushed the button, the elevator control system will illuminate the button and send the elevator to the selected floor and open the selected door.

c. When the elevator is in normal mode, floor select buttons shall be enabled.

d. Card readers shall be in override anytime the elevator is in fire service mode.

e. If elevator DGP fails the elevator will enter secure mode.

f. If elevator independent key switch goes to fire override switch mode an alarm will be generated to UPD.

g. Elevator contractor to provide the following. Verify this information with TAMU Elevator Services and the elevator specifications:

1) Infrastructure for Card Reader in each elevator shall require six (6) 2-conductor 20AWG stranded, low voltage cable with an overall braided shield and drain wire. These items shall be run from the elevator controller to the elevator car top. Provide an excess loop of six (6) feet long on each end. The excess cable loop shall be neatly bundled and located in a 6" x 6" x 4" Deep "J" box on the elevator car top. Provide an 18" x 24" x 6" deep hinged lockable "J" box in the elevator machine room as a Demarc for Card Reader wiring. Provide screw terminal strips for wiring connections. Clearly label both boxes “Elevator Card Reader Future Use”.

2) Removable blank for Card Reader. The area where the future card reader will be installed in the Car Panel shall be self-contained and isolated from the Elevator wiring within the car panel. The card reader shall be installed using a cover panel to be removed and replaced from the finish side of the car panel using tamperproof screws. The height of this reader shall be in compliance with all ADA and TAS requirements. Card reader shall be bypassed anytime the Elevator is in Fire Service Mode.

8. Card Reader Controlled Elevator Hall Call Buttons

a. Provide a card reader adjacent to the elevator hall call button. When the elevator is in card reader control mode, the hall call button shall be disabled. Upon a valid card read, the BACS shall enable the hall call button and the user shall be able to select the button for access.

b. When the elevator is in normal mode, hall call buttons shall be enabled.

c. Card readers shall be in override mode anytime the elevator is in fire service mode.

9. Integrated IP-Enabled Access Control Devices

a. IP Enabled Power-over-Ethernet (PoE) Integrated Card Reader Mortise Lock: IP enabled, PoE ANSI/BHMA A156.13 Grade 1 mortise lockset with integrated proximity card reader, request-to-exit, latch bolt and deadbolt monitoring, and door position signaling in one complete unit. Motor driven locking/unlocking control of the lever handle trim, 3/4” deadlocking anti-friction latch, and 1” case-hardened steel deadbolt (optional). Lock is U.L listed and labeled for use on up to 3-hour fire rated openings. Available with or without keyed high security cylinder override.
1) Completely intelligent and integrated locking unit with Ethernet power and communication connection capability directly from the locking unit back to the central system host server without additional access control interfaces or components (excluding PoE switches and Mid-Span devices) via an existing or newly installed TCP/IP network.

2) Open architecture design supports wired integration with third party access control systems applications via software development kit (SDK). Real-time software accessible alarms for forced door, unknown card and door held open, with inside lever handle (request-to-exit), auxiliary latchbolt, deadbolt, and door position (open/closed status) monitoring.

3) 2,400 users and 10,000 event transaction history (audit trail). Distributed intelligence allows standalone operation in absence of network communication allowing for system operational redundancy.

4) Energy Efficient Design: Provide lock bodies which have a holding current draw of 15mA maximum and can operate on either 12 or 24 volts. Locks are to be field configurable for fail safe or fail secure operation.

5) Supports HID 125 kHz proximity formats up to 39 bits, including Corporate 1000. Dual credentialing available with keypad option.

6) Power and communication from one Ethernet (category 5e or higher) cable. Compliant with 802.3af specifications requiring 12.95 watts for Power over Ethernet.

7) Supports real-time system lockdown capabilities. Inside lever retracts latch bolt and deadbolt simultaneously.

8) High security mechanical key provides emergency override retraction of latch bolt without need for electronic activation.

B. Hardware and Software Requirements

1. Access Control Manager Software

   a. Access Control Software
      1) Operating System: Secure embedded Linux OS.
      2) Includes the option to integrate with Active Directory.
      3) Includes a HTML browser-based client.
      4) Includes Avigilon Unity Access mobile app, formerly ACM Expedite, to allow operators to manage access to facilities from a mobile environment.
      5) Allows for the unification with Avigilon Unity Video, formerly Avigilon Control Center (ACC).
      6) Includes the ability to record on alarm.
      7) Includes Multi-factor Authentication for additional logon security.
      8) Includes enhanced map icons for improved sharpness, scalability and visibility on any background.
      9) Includes multiple search options.

   b. Access Control Software Capacities
      1) Intelligent Controllers: 512 per appliance allowing geographic independence from appliance via IP communication.
      2) Access Control System Appliances Supported: Up to 100 using replication.
      3) Events Stored: Up to 150,000,000.
      4) Events Stored: Up to 75,000,000.
         • Sub-panels: Up to 32 per intelligent controller.
      5) Doors: Up to 64 per intelligent controller.
      6) PIN Length: Between 2 and 8 digits.
      7) Card Formats: Up to 128 per appliance.
      8) Time Schedules: 255 per intelligent controller.
9) Holidays: 255 per intelligent controller.
10) Identity and Operator Database: Up to 500,000.
11) Client Connections: Up to 50.

c. Access Control Software Collaborations
1) Database Collaborations and Integrations: provide access control software capable of integration with the following industry standard third-party databases:
   a) Bidirectional:
      ▪ Structured Query Language (SQL) Server.
      ▪ Oracle Relational Database Management System (RDBMS).
      ▪ Comma Separated Value (CSV).
      ▪ REST API Integration.
   b) Push Only:
      ▪ Extensible Markup Language (XML) for Event Push.
2) Visitor Management Integration:
   a) HID Global Easy Lobby
   b) Alert Enterprise Guardian
   c) Savance EIOBoard
3) Custom Integrations:
   a) Destination Dispatch
   b) Custom Integrations using RestAPI
4) Video Integrations:
   a) Avigilon Control Center
   b) Milestone XProtect
   c) Tyco ExacqVision

d. Access Control Software Interface
1) Web-Based Access Support: Provide access control software with browser-based access to system applications including support for industry standard desktop and mobile web browsers.
2) Tabbed User Interface: System supports the following functionality in a tabbed view:
   a) Monitor events, alarms, and hardware status in real time.
   b) Verify identities in real time.
   c) Search historical events and alarms.
3) Events and Alarms: Provide a system that allows administrators the ability to create, configure, and prioritize events and alarms and communicate information about the generation of the event or alarm to the operator with guidance for responding to the event or alarm. Events will support two levels: system level events affect all objects in the system; field level events affect only the object they are configured on.
4) Access Groups: Provide a system that allows administrators the ability to create groups of card readers and schedules such that card readers can allow or restrict access to areas based on schedules.
5) Identity Records: Provide a system with integrated identity management, allowing imports of data from supported databases. Each identity supports access control based on groups and roles as well as individual overrides. Include functionality to customize identity and token forms in base software. Provide identity records capable of management and synchronization between multiple sites.
6) Roles: Support a role-based permission method allowing one or more roles to be assigned to identities to determine physical and logical access.
7) Anti-Passback: Provide access control software capable of designating areas to require a card to enter and exit the area before it is used to enter the area again.
Soft and Hard Area APB: Tracks each badge that enters a specific area and defines which areas the badge may access next.

Door-Based APB: Tracks each badge that enters and does not allow the same badge to enter twice in a row until after the APB time limit is reached.

Token-Based, Timed APB: Tracks each badge that has accessed a door. After the badge has accessed one door, it must access a second door or wait until the APB time limit is reached before it may access the first door again.

Timed Area APB: Time based hard area APB. When the time limit expires, the hard area APB becomes a soft area APB.

Hard Door APB: Tracks each badge that enters a door and does not allow the same badge to enter twice in a row.

Soft Door APB: Tracks each badge that enters a door and generates a warning transaction if the same badge is used at the same door twice in a row.

8) Badging: provide a tool to support the creation of custom badge layouts including the following content:
   a) Static Information: Badge size, background color, text strings, and graphics common to every badge.
   b) Dynamic Information: Text fields and images from the identities database unique to each badge.

9) Enrollment: Provide integrated identity management and enrollment functionality as part of the core system functionality.

10) Macros: Provide a system capable of linking one or more events to macros such that a single event may execute up to 30 macros. System must support a minimum of 255 macros per intelligent field controller.

11) Device Template Configuration: Provide an access control system that supports templates to automatically populate standard parameter fields in groups for new or existing doors, wires, readers, and input/output devices.

12) Encryption: Provide access control system that supports the following encryption methods:
   a) TLS 1.2: Require TLS encryption between the access control system and Mercury controller.
   b) Custom Certificates: Require self-signed or certified authority certificates to harden access control systems. Certificates will authenticate Mercury panels to the access control system.
   c) FIPS 140-2: Require access control server to utilize FIPS 140-2 compliant ciphers only.
   d) FIPS 201-2: Require large-encoded card formats for FIPS 201-2 certified pivClass readers.

13) Custom Device Mappings: Administrators may assign a unique group of alarm attributes to specific device-alarm combinations to override global settings of generic attributes.

14) Dashboard: Allow creation of a dashboard for real-time status and actions of hardware components on a single screen that can also filter by name, status, appliance, or group.
   a) Hardware Status:
      Panels: Communication, power, tamper, and battery.
      Sub-panels: Communication, power, and tamper.
      Inputs: Inactive, active, trouble, and masked.
      Outputs: Off, on, and trouble.
      Doors: Communication, tamper, battery, unlocked, help, masked, and forced.
      Appliances: RAM, program, database, CPU load, and port status.
   b) Monitor:
      Panels: Device status, security status, name, model, firmware, IP address, MAC address, cards in use, and last communication.
      Sub-panels: Device status, name, panel, type, port, address, and firmware.
      Inputs: Device status, input name, subpanel, EOL resistance, and address.
      Outputs: Device status, output name, subpanel, schedule, and address.
Power Supplies: Power supply name, installed status, status, and logs.
Access Control Doors: Status, name, panel, door state, door mode, and override status.

c) Manipulate Access Control Doors:
   Door actions: Grant, restore, unlock, locks no access, disable.
   Door mode: Card only, card and PIN, card or PIN, PIN only, facility code only.
   Door Forced: Mask forced, unmasked forced.
   Door Held: Masked held, unmasked held.
   Installed: Install, uninstall.

15) Map Interface: Provide interface for creating customizable layouts including floorplans, reader locations, and buttons that can trigger actions.
   a) Actions: Card readers indicate alarm via icon and allow for card only, card and pin, card or pin, pin only, facility code only, disable, unlock, lock, grant, restore, mask held, unmask held, and trace actions.
   b) Occupancy/Mustering: Maps will provide real-time occupancy of a defined area.
   c) Programmable Buttons: Maps will provide mapping of buttons and text to perform actions.

16) Verification Interface: Provide web-browser-enabled connection to access control software allowing a user to review information about card holders entering or exiting up to four (4) doors in real time. Information to include badge photo, transaction time, and date via any device with a compatible browser.

17) Virtual Verification Station: Provide web-browser-enabled connection to the access control software to allow a user to visually confirm the identity and authorization of a person attempting entry to a controller area via a mobile device such as a tablet or smartphone.

18) Intrusion Interface: Provide interface to see real-time status of linked Intrusion Panels.
   a) Display Intrusion Panels with following status:
      Communication, Battery, Power, Tamper, Phone Line.
   b) Display and Interact with Configured Areas.
      Status, Area Name, Panel Name.
      Silence, Disarm, Master, and Perimeter.
   c) Display and Interact with Intrusion Points.
      Status, Point, and Area.
      Bypass and Un-bypass.
   d) Display and Interact with Intrusion Output.
      Status, Outpoint, Panel.
      Activate and Deactivate.
   e) Access Control Software Reporting: Generate, filter, edit, and customize system reports including the automated generation and distribution of customized reports in PDF and CSV formats.

   e. Access Control Software Video Integrations
      1) Video Management System Unification: Provide the following features in video the management system when used in conjunction with access control software.
         a) Link cameras and doors on a single screen.
         b) Search video by card swipe using identity search.
         c) Grant door access.
         d) Monitor live door swipes with video for identity verification.
         e) Display video and alarm information in the video management client.
      2) Access Control System: Provide following features in access control software when used in conjunction with a video management system.
         a) Link cameras and doors to specific events.
         b) Notifications for events include live video and recording of events from before and after in the web browser interface.

f. Access Control Software Administration
1) Backup: Provide access control software capable of backing up via USB drive, local appliance, windows network share, or secure copy protocol.

2) Database Replication: Replicate database from 1 to 100 appliances for distributed identity control.

3) Failover and Redundancy: Provide access control software that supports switching to a backup system automatically in the event of a fatal failure without loss of monitoring or hardware control.
   a) Provide failover technology supporting LDAP data replication.
   b) Provide failover technology supporting either a 1:1 or N:1 architecture.

4) Updates: Provide access control software capable of automatically updating the following:
   a) Operating System: Version, service packs, and security vulnerabilities.
   b) Field Devices: Firmware versions.

5) Upgrade Functionality: Provide access control software capable of automatically upgrading software licensing.

g. Accessory Software Schedule

1) Reader Licensing:
   a) Additional Readers: AC-SW-LIC-16RCU-6-P; perpetual, adds 16 reader software licenses to any appliance to expand door capacity up to the appliance’s maximum capacity.

2) Badging Application Software Licenses:
   a) Badging Application: AC-SW-LIC-BDGE-6-P; perpetual, one per appliance.

3) Video Integration Licenses:
   a) Exacq: AC-SW-LIC-EXACQ-6-P; perpetual, one per appliance.
   b) Milestone: AC-SW-LIC-MILEST-6-P; perpetual, one per appliance.

4) Intrusion Integration Licenses:
   a) Bosch: AC-SW-LIC-BOSCHINTR-1PANEL-6-P; perpetual, per panel, one per appliance.
   b) Bosch: AC-SW-LIC-BOSCHINTR-10PANEL-6-P; perpetual, for 10 panels, one per appliance.

5) Verify Integration Licenses:
   a) Verify: AC-SW-LIC-AVO-VER-5VS-6-P; perpetual, for five virtual stations, one per appliance.
   b) Verify: AC-SW-LIC-AVO-VER-16VS-6-P; perpetual, for sixteen virtual stations, one per appliance.

6) Biometric Integration Licenses:
   a) VIRDI: AC-SW-LIC-VIRDI-BIO-6-P; perpetual, for Virdi Biometric readers, one per appliance.

7) Redundancy and Failover Software Licenses:
   a) Replication: AC-SW-LIC-REP-6-P; for multi-appliance replication, one per appliance.
   b) Auto Failover: AC-SW-LIC-AF-6-P; hot standby auto failover software license, one per appliance.
   c) Partitioning: AC-SW-LIC-PART-6-P; for additional partitions, one per appliance.

8) IT Collaboration Software Licenses:
   a) Microsoft SQL: AC-SW-LIC-SQL-6-P; from Microsoft SQL Server 2000 forward, one per appliance.
   b) Oracle: AC-SW-LIC-ORCL-6-P; from Oracle DB 9i Server forward, one per appliance.
   c) LDAP Directory: AC-SW-LIC-LDAP-6-P; for Microsoft Active Directory or other, one per appliance.
   d) XML: AC-SW-LIC-XML-6-P; for XML events, one per appliance.
   e) REST: AC-SW-LIC-REST-6-P; perpetual, for unlocking REST-based API for custom integrations, one per appliance.
2. Access Control Hardware (Card Readers)
   a. Reader shall support BLE, NFC based mobile credentials
   b. Reader shall include Apple's Enhanced Contactless Polling (ECP) to support credentials in Apple Wallet
   c. Reader shall include a lifetime limited warranty.
   d. Reader shall support DESFire and SEOS based credentials.
   e. Reader manager application shall have IP65 outdoor rating
   f. Reader shall support both mullion and wall mount options.
   g. Reader shall include intelligent power mode to reduce building energy consumption.
   h. Reader shall have GreenCircle verification
   i. Controller shall have open architecture that is IP-enabled
   j. Reader shall be HID Signo Series or approved equal
   k. Reader shall support MIFARE DESFire technology to allow Aggie Card integration

3. Video Control Software
   a. Software shall provide an overview of events across all cameras in the site
      1) Analytic events, face and license plate watch list matches, UAD events, UMD events, motion events, alarms
      2) Shall include operator ability to triage most important events
   b. Software shall incorporate AI-powered facial recognition technology
      1) Populate watch lists by uploading images from recorded video
      2) Query for watch list entries
      3) Receive alerts for potential watch list matches
      4) Create alarms that trigger when an individual on the watch list is detected
   c. Software shall incorporate AI search engine
      1) Ability to sort through recorded video to locate a person or vehicle of interest across an entire site
      2) Ability to search for person or vehicle of interest by entering physical description, by uploading a photo, or by finding an example on recorded video
   d. Software shall enable analytic events and alarms to be viewed and searched through a user interface
      1) Real-time events and forensic capabilities detect and notify operators of scene changes and rules violations
   e. Unusual Activity and Unusual Motion Detection (UAD & UMD)
   f. ACM-ACC interoperability
      1) Identity verification enables users to see ACM system credentials dynamically displayed with ACC camera views
      2) Identity search enables users to visually verify access events and initiate an appearance search across the entire site for the same person
   g. Software shall be Avigilon Unity 8 or newer and shall be preinstalled on Avigilon recorders and appliances
      1) Avigilon HD Video Appliances, Network Video Recorders (NVRs), NVR Workstations, ACC ES Recorders, ACC-ES Analytics Appliances, ACC-ES 8-Port Appliances, H4ES camera line
      2) ACC stand-alone software shall be installed as appropriate

4. Camera Requirements
   a. Camera requirements shall be based on minimum pixels per foot (DORI system – Detection, Observation, Recognition, Identification)
   b. DORI minimum standards
      1) Building Entry – Identification (80 PPF)
      2) Building Exit – Recognition (40 PPF)
3) Elevator Lobby (Viewing Elevator Doors) – Recognition (40 PPF)
4) Stairwell Access Doors (Entering Floor) – Recognition (40 PPF)
5) Entry Lobby – Observation (30 PPF)
6) Faculty Office Suite Entry Doors – Identification (80 PPF)
7) Faculty Office Suite Lobby – Recognition (40 PPF)
8) Faculty Office Hallways – Observation (20 PPF)
9) Hallways to Secured Storage or Valuable Asset Areas – Detection (20 PPF)
10) Loading Dock – Recognition (40 PPF)

c. Cameras must support classified object detection analytics
d. Cameras must support Avigilon analytic event configurations
e. Cameras must support unusual activity detection
f. Cameras must support appearance search analytics
g. Cameras must support object detection by sub-types: car, truck, bicycle, motorcycle, bus, person, other
h. Cameras must support tamper detection
i. Cameras must support UL294 Outdoor and Indoor rated, IP65
j. Cameras must support an operating temperature range between -30 degrees F and +140 degrees F and a humidity range of 0% to 95% noncondensing
k. Cameras must comply with Section 889 of the National Defense Authorization Act
l. Cameras installed in exterior locations shall have the ability to switch from Day to Night mode automatically.
m. All cameras shall be connected to Campus VMS
n. All new installations require the use Avigilon cameras and must meet requirements listed above.
o. When upgrading or replacing existing cameras Avigilon cameras are required and must meet requirements listed above
p. Avigilon cameras capable of supporting features and specifications listed in this section.
q. Use of the Avigilon system design tool will be the determining standard for camera image quality requirements.

5. Request to exit (REX)

a. Doors equipped with electrified locksets or crash bars shall have integrated REX switches.
b. REX motion sensors can only be installed with prior approval from Campus IT

6. Door Position Switches

a. Concealed Magnetic Door Position Switch: Provide Sentrol 1076D Series or approved equal door position switches.
b. Surface Mount Door and Hatch Position Switch: Provide Sentrol 2500 Series or approved equal surface mount door position switches.
c. Overhead Door Position Switch: Provide Sentrol 2300 Series or approved equal surface mount door position switches.
d. Provide armored cable from surface mount and overhead switches to the associated junction box to conceal and secure the wire.

7. Delayed Exit Device Controller

a. Provide Securitron Model XDT-24 or approved equal. Locate the controller above the secured side of the door. Provide additional cabinet as required to provide a neat and serviceable installation. Install 2 sounders in the ceiling above the secured side of the door.
b. Signage requirement for exit only delayed egress door. Signs should be mounted above the crash bar and have a red background with white letters that are 1” tall with a
1/8” stroke width (NFPA 101 requirement). Campus IT and EHS shall approve sign language upon request prior to installation.

8. End of line (EOL) Resistor Terminations
   a. Field (Device) End
      1) Provide GRI 6644T Standard Series Parallel Resistor Packs with 2 – 1K 1/8 watt 5% carbon film with 2 blue and 2 black 12-inch leads.
      2) Locate EOL Resistor Terminators at the end of the cable being supervised and within device housings. All Exceptions must be approved by Campus IT prior to installation.
   b. Panel End
      1) Resistors will not be installed at the panel without written authorization by the TAMU project manager.
      2) Provide appropriate screw heads for each application (e.g. countersunk heads for recessed cover plate screws, flat head screws for standard junction box covers, etc.).

9. Power Supplies
   a. Provide LSP or approved equal UL Listed Class II power supplies for BACS equipment and electric locking devices.
   b. Some electronic locking hardware require a 120VAC power supply at the door. In these instances, the door hardware installation contractor shall be responsible for furnishing and installing the locking hardware manufacturer’s recommended power supply. Verify with TAMU Project Manager and security consultant to determine if a remote power supply is required.
   c. Power supplies shall provide the following:
      1) Each battery shall be permanently labeled with the date of manufacturer and date of installation (month & year). The date of installation is the month & year that the battery was placed in the power supply and began charging.
      2) A battery charger to maintain the battery.
      3) Low battery and power fail contacts to monitor the status of the input power and the battery. Connect each power supply low battery and power fail alarm as a separate alarm input into DGP.
      4) Key lockable wall mount metal enclosure with tamper switch. Coordinate keying requirements with TAMU Project Manager.
      5) *Sealed gel battery backup to provide four hours of continuous operation during power failure.* Provide batteries as required to provide specified battery backup time for a fully loaded power supply, regardless of the connected load.
   d. Additional DGP Power Supply Requirements
      1) The DGP power supply provide power only to DGP’s and shall not provide power for locks or any other low voltage device.
   e. Additional Electric Locking Mechanism Power Supply Requirements
      1) 24 VDC output.
      2) Provide (1) lock power supply per DGP.
      3) Fail secure electric locking mechanisms shall remain locked during power failure and fire alarm conditions.
      4) Connect fail safe locking devices in accordance with applicable life safety codes to unlock automatically under the following conditions:
a) Loss of power to the power supply.
b) Failure of the power supply.
c) Fire alarm activation if required by EHS.

5) Provide power distribution boards with independently fused output relays and fire alarm control panel interface.

f. Additional Device Power Supply Requirements

1) Provide device power supplies for other security system devices requiring power (e.g. card readers, local alarms, motion sensors, etc.)
2) Provide power distribution boards with independently fused outputs.

C. System Interfaces

1. Electric Locking Mechanisms

a. The security consultant and door hardware consultant shall coordinate all door hardware, door and door frame design. The door hardware consultant shall be responsible for specifying all access control door hardware based on security consultant input and ensure consistency with project hardware (see 08 71 00). The security consultant shall verify all specified door hardware is appropriate for the security application. In addition, the security consultant must specify the sequence of operations for each access-controlled opening and define termination requirements for the security contractor.

b. TAMU preferred electronic lock manufacturers:

1) Electrified Exit Device
   a) Sargent (Assa Abloy)
   b) Von Duprin (Allegion)

2) Mortise Locks
   a) Sargent (Assa Abloy)
   b) Schlage (Allegion)

3) Magnetic Locks
   a) Locknetics (Allegion)
   b) Rutherford Controls (RCI)

4) Self-managed Locks
   a. Sargent (Assa Abloy)

5) Cylindrical Locks are prohibited
6) No electric strikes unless approved by Building Access and Security.
7) Lock Cylinder
   a) Schlage Primus FSIC core (Allegion)

2. Elevator Control System

a. The security consultant shall verify the elevator security requirements with Building Access and Security and coordinate with the elevator consultant to ensure the appropriate system
interfaces are in place.

3. Fire Alarm and Life Safety
   b. The security consultant shall coordinate the access control system design with the life safety consultant to ensure compliance with applicable codes and requirements. This includes, but is not limited to, the fire alarm interface, fail safe/secure locking mechanisms, and delayed egress.

2.3 NETWORK AND SIGNAGE REQUIREMENTS

A. Network Requirements
   1. Bandwidth consumption: Off campus sites or sites not in compliance with minimum network standards shall consult with networking prior to installation of cameras. For installations of 50 or more cameras, or when building camera count reaches that amount, TAMU IT shall be consulted for proper networking architecture compliance.
   2. POE switches are recommended to be used in direct consultation with TAMU IT networking (shall adhere to minimum network standards).
   3. Network based cameras and recording systems may only be connected to the network, in consultation with networking. Portal accessing the network shall be approved by TAMU IT.
   4. Cable numbers shall be mapped to their corresponding switch ports.
   5. Identification device descriptions are required for port descriptions.
   6. Black patch cables, appropriately labeled, should be used in network/data/IDF closets.

B. Signage Requirements
   1. Signage for video and CCTV locations required at main entrances to areas with video security, such as building entrances and elevator landing areas. The signage language should say: “This Area Subject to Video Surveillance”.
      a. Sign size to be 3 ½” X 11”,
      b. Signs will be placed so the bottom of the sign is 60” above finished floor (i.e. Just above the light switch level).
      c. Signs will be placed in locations where they can readily be seen by someone entering the space. Guidance for signage placement is as follows:
         1) Immediately inside or outside the entrance door to the building lobby or other building entrances.
         2) Above the elevator call buttons in the elevator lobby.
         3) On walls and not on doors.

2.4 WIRE AND CABLE

A. Description
   1. Provide wire and cable infrastructure for all security system components.
   2. In addition to requirements of this section, ALL New construction and renovations shall comply with the requirements of the TAMU Network Installation Design Standards.
   3. In addition to requirements of this section, all existing buildings shall comply with the requirements of Appendix E – TAMU Camera & Keyless Wiring Installation Standards (existing buildings)

B. Minimum Requirements
1. Conductors and cable shall be UL listed for its intended application and shall meet all national, state, and local code requirements for its application.

2. Conductors and cable shall meet individual security system manufacturer specifications.

3. Provide shielded conductors and cable as required by the manufacturer or as required to provide for interference-free signals.

4. Color coding shall be accomplished by using solidly colored insulation. Grounding conductors, where insulated, shall be colored solid green or identified with green color as required by NEC.

5. Increase conductor sizes on cables as required to be consistent with circuit current ratings, length of wire runs, and manufacturers’ recommendations.

6. Composite cables are not an acceptable alternative.

7. Due to wire run distance, electronic locks may require a larger gauge wire or remote power supply to work properly. Contractor will be responsible for determining distance, power supply, and wire gauge requirement. Confirm requirements with TAMU IT.

8. Patch Cables
   a. Provide pre-manufactured patch cables (cable, connectors, boots, etc.) as required to connect security systems to voice and data communication outlets.
   b. Patch cables shall be certified for their specific use to meet or exceed applicable industry specifications (e.g., TIA, ETL, UL, CSA).
   c. Provide cable lengths as necessary to neatly route cables through cable management systems and other cable organization systems.
   d. Provide connectors as required for proper termination. Provide boots for connectors where applicable to prevent snagging.
   e. Provide category 5e patch cables as required for the connections of security equipment. Confirm category 5e cabling specifications and requirements with Building Access and Security.
   f. Provide cable jacket colors as follows:
      1) Blue for data cables.
      2) White for voice cables.
      3) White for security cables except for direct burial cables.

C. Minimum Conductor and Cable Types and Sizes.

1. Security contractor shall verify maximum distances and wire gauge.

2. Low Voltage Power Cable
   a. 18 AWG (4 conductors minimum per locking device), stranded, insulated, and jacketed.

3. Card Reader Cable
   a. Banana cable for card readers shall consist of four different groups:
      Six 22 AWG conductors (shielded),
      Four 22 AWG conductors,
      Four 18 AWG conductors
      Two 22 AWG conductors.
4. Keypad Cable
   a. 20 AWG (4 conductors minimum), stranded, insulated, and jacketed.
5. Alarm Point Monitoring Cable
   a. 20 AWG (4 conductors minimum per input or alarm point), stranded, insulated, shielded, and jacketed.
6. Siren, Speaker, and Control Point Cable
   a. 18 AWG, (4 conductor minimum) stranded, insulated, and jacketed.

PART 3 - EXECUTION

3.1 COORDINATION

A. Security contractor shall be required to coordinate installation activities with the following divisions or groups:
   1. Door hardware, doors and door frames.
   2. Electrical power and pathways.
   3. Telecom voice and data cabling and outlets.
   5. Elevator demarc panel, traveling cables and elevator car card reader enclosure by contractor.
   6. IP and phone number assignment.

B. Meetings
   1. All meetings shall be documented to include attendees, meeting topics, resolution to each topic, and action items with resolution date and responsible party. These meeting minutes shall be distributed to all attendees, consultant, contractor, TAMU Project Management and TAMU IT within 2 business days.
   2. Project Kickoff Meeting
      a. The intent of this meeting is to:
         1) Introduce the TAMU representatives, security consultant and construction teams dedicated to security agenda only.
         2) Identify communication channels and process.
         3) Establish expectations and review milestones.
         4) Review the project scope and requirements.
         5) Establish schedule for provision and review of submittals.
         6) Answer questions and resolve any issues.
   3. Pre-Installation Meeting
      a. The intent of this meeting is to:
1) Review the construction schedule and key milestones.
2) Coordinate requirements and schedules of other trades related to the security system.
3) Review issues and/or problems as necessary.

4. Integrated Access Control Door Hardware and Electrical Coordination: Coordinate the layout and installation of scheduled integrated access control door hardware, and related access control equipment, with required connections to source power junction boxes, power supplies, detection and monitoring hardware and fire alarm system.
   a. Door Hardware Interface: The access control system to interface and be connected to electrified and integrated access control door hardware as described under Division 08 Sections "Door Hardware" or "Access Control Door Hardware". Coordinate the installation and configuration of electrified door hardware being monitored or controlled with the controls, software and access control hardware specified in this Section.

5. Meetings with Other Trades
   a. The intent of these meetings is to coordinate requirements with other trades as required to:
      1) Review the details for each interface.
      2) Ensure that each trade understands requirements for the interface with the security system.
      3) Verify interface responsibilities and close any gaps in scope of work.
      4) Resolve issues as required.
   b. The initial coordination meeting shall involve all trades related to the security system. Additional meetings will be scheduled as necessary for additional coordination.
   c. The general contractor will be responsible for scheduling coordination meetings.

3.2 INSTALLATION

A. General
   1. Coordinate equipment installation requirements with other trades prior to installation.
   2. After installation, protect equipment to prevent damage during the construction period. Close openings in conduits and boxes to prevent the entrance of foreign materials.
   3. Make equipment connections in accordance with the approved submittal drawings and manufacturer specifications.
   4. Seal exterior devices to protect against weather conditions including heat, cold, moisture, dust, and sand.

B. Equipment
   1. Field-verify specific equipment locations to provide the best fit and function. Verify locations with the Architect as necessary.
   2. Install equipment in accordance with manufacturer specifications.
   3. Install equipment to allow adequate clearance for testing and maintenance.
   4. Locate end of line resistors within the device housing.
5. Provide tamper resistant screws and fasteners for equipment located in accessible and/or public areas.

6. Remove dirt, packaging, wiring scraps, and other debris from equipment, boxes, cabinets and work areas at the end of each workday.

7. Wherever possible, remove contractor and manufacturer equipment logos from security field devices.

8. Final approved wire identification sheet submitted to Building Access and Security will be placed in a clear plastic sleeve mounted on the inside door of the termination can and intrusion panel for future reference.

9. Accessibility Coordination
   a. When mounting card readers or other devices that require accessibility coordinate with the architect and other trades to ensure ADA requirements are being met.
   b. Doors with both a card reader and automatic door operator push plate should have both of these devices placed next to each other.
   c. On the pull side of a single door, place the card reader on the latch side of the opening. On the pull side of double doors, place the card reader on the right side which is generally the path of travel.
   d. Card readers should generally be mounted 48” from an inside corner and 42” above finished floor.
   e. On the pull side of a door, card readers should be mounted 48” from the door jamb so that a wheelchair would be clear of the swing of the door.

10. All power transfer hinges or other devices that provide a wiring path from the door to the frame shall be serviceable without having to remove the door.

11. Integrated access control products, campus locks, and IP enabled products are required to be installed by "Authorized Channel Partner" (ACP), "Certified Integrator" (CI) or “Preferred Installer” (PI) program.

12. Final connect the system control switches (integrated access control door hardware, remote readers, keypads, display terminals, biometrics), and monitoring, and signaling equipment to the related Controller devices at each opening to properly operate the electrified door and access control hardware according to system operational narratives.

3.3 CONDUIT, BOXES AND RACEWAYS

A. Conduit shall be a minimum of ¾ inch (flex is not allowed). Junction boxes shall be a minimum of 8x8x4, pull boxes, wire troughs, and wire ways dedicated to security will be provided by electrical contractor. Provide additional conduit necessary to complete the installation.

B. Provide conduit between power sources provided under a separate section and security system low voltage power supplies.

C. Provide conduit from interface terminal cabinets to security pull boxes.

D. Carefully install conduit, properly and adequately support conduit as required to comply with the requirements specified herein and as required by the NEC, and provide a neat, workmanlike installation. Support horizontal conduit runs with clamps, pipe straps, special brackets, or heavy iron ties secured to building structure.

E. Lay out and install conduit runs to avoid proximity to hot pipes. In no case shall a conduit be run within three inches of such pipes, except where crossings are unavoidable, and then the
conduit shall be kept at least two inches from the covering of the pipe crossed.

F. Provide fire stops where conduits penetrate fire rated walls and/or floors.

G. Provide tamper resistant screws or fasteners for junction boxes located in accessible and/or public areas.

3.4 WIRING TECHNIQUES

A. Wire installation is not specifically detailed in the Contract Documents. Determine conductor requirements for each device in accordance with the Contract Documents and manufacturer requirements.

B. Install cable in accordance with Security System manufacturer requirements and NEC.

C. Color code and terminate conductors consistently as follows:
   1. Red for positive and black for negative DC power leads.
   2. White for positive and green for negative alarm loop conductors.

D. Run wiring within conduit or exposed within walls, neatly above accessible ceilings, and in riser closets.

E. Arrange cables within access panels to allow for removal of the access panel and access to equipment within the panel. Arrangement shall also be in a neat and workmanlike manner. Building Access and Security shall hold the final, authoritative opinion on what constitutes a neat and workmanlike manner. Failure to meet Building Access and Security’s expectations in this matter shall result in Security Contractor to redress cabling/installation to Security Operations’ satisfaction, at no additional cost to the project.

F. Neatly route cables parallel or perpendicular to building lines.

G. Provide J hooks and other cable support systems (spaced at regular intervals) within accessible ceiling spaces. Fasten cables to the cable support systems and provide strain relief to protect cables and ensure compliance with required cable bends.

H. Cabling shall be at least 18” from power lines of 2 KVA or less, at least 3’ from fluorescent lighting and power lines between 2 and 5 KVA and at least 2’ from transformers and motors.

I. Run cables at least six inches from the communications cable plant, intercom wires, input/output wires, and siren wires.

J. Route wire and cable as required to prevent interference and signal contamination of both Security System cable and cable associated with other systems. Coordinate the routing of wire and cable requiring isolation from power, radio frequency (RF), telephone, etc.

K. Provide sleeves and code compliant fireproofing techniques for all penetrations of fire rated partitions, masonry walls, and slabs, where the penetrations are made by or used for installation camera and keyless access systems.

L. Separate high voltage (120 VAC and above) cables from low voltage cables within enclosures to comply with NEC requirements.

M. Fasten approved wire management hardware (bridle rings, j-hooks, etc.) to the building structure and/or cable tray at least every 10 feet where not in conduit. Do not lay or fasten cables to electrical conduits, light fixtures, piping, mechanical equipment, or ceiling grids.

N. Run wire and cable continuous from device location to the final point of termination. No mid-run
Cable splices will be allowed except where cables transition from one type to another (e.g. underground cable to plenum cable). Provide the following where cable transitions are required:

1. Provide labeled terminal strips inside lockable cabinets at cable transition locations and document locations in the submittals.
2. Label terminal cabinets and document labels in record documentation.
3. Provide the same number of conductors and insulator colors for each cable type from the security device to the DGP location.
4. Where shielded cable is required, the shield shall also be spliced.

O. Visually inspect wire and cable for faulty insulation prior to installation.

P. Provide bushings, grommets, and strain relief material where necessary to prevent abrasion of wire and excess tension on wire and cable.

Q. Component Connections
   1. Exposed conductors are not acceptable.
   2. Wire nuts shall not be an acceptable means of connecting wire cable.

R. Neatly install and terminate wire and cable within Control panel's, power distribution cabinets and other security enclosures. Pull cables tight, remove slack, and route in such a way as to allow direct, unimpeded access to the equipment within the enclosure. Allow no more than 1/16 inch of exposed tinned wire on all terminal strips.

S. Bundle and tie wire and cable with Velcro hook & loop type or similar cable ties. Tie wrap type fasteners shall not be acceptable.

T. Where applicable provide heat-shrink to insulate wire connections. The use of electrical tape shall not be acceptable.

U. Cover exposed high voltage (120 VAC and above) power terminations within Control panel's, power distribution cabinets and other security enclosures.

V. When electric locking mechanisms or power transfer hinges come with factory terminated connectors, the contractor shall consult with Building Access and Security prior to removal. Under no circumstances will the contractor be allowed to cut these connectors off without consulting Building Access and Security.
3.5 POWER REQUIREMENTS

A. 120 VAC emergency power dedicated circuit, appropriately sized to security will be provided by the electrical contractor.

B. Connect to AC power and provide UL listed power supplies and transformers to distribute low voltage power to the system components as required.

3.6 GROUNDING

A. Ground all equipment and cables in accordance with manufacturer requirements and instructions.

B. Ground cable shields and drain wires as follows:
   1. From the field devices, terminate shield drain wires to the terminal cabinet ground bar.
   2. Bond the terminal cabinet and Control panel cabinet ground bars to the Control panel ground bar with a minimum 12 AWG solid conductor green grounding wire.
   3. Do not terminate shields and drain wires between the terminal cabinet and Control panel.

C. If device requires specific grounding location it shall be tested and certified in writing by the Electrical Contractor.

3.7 LABELED FRAMES AND DOORS

A. In no instance shall any fire-rated labeled door or frame be drilled, cut, penetrated, or modified in any way.

B. The Contractor shall be responsible for replacing any labeled door or frame that is modified without written approval from the manufacturer.

3.8 LABELING

A. All labels shall be based on final TAMU door and room numbering scheme approved by TAMU Facilities Analytics and Mapping (FAM). Building Access and Security shall be consulted on labeling prior to installation.

B. All cables need to be labeled alike at both ends.

C. Permanently mark all terminals. Terminal and cable markings shall agree with markings shown on as-built drawing.

D. Label each camera with the number shown on final security system program sheet that has been approved by Building Access and Security.

E. Neatly coil and secure spare conductors in the ceiling, device back box or panel wire way. Neatly bundle and tag conductors.

F. Label equipment including, but not be limited to control panel’s (label to denote control panel address), power supplies, and termination cabinets. Coordinate names, fonts, styles, and devices to be labeled with Building Access and Security prior to labeling. Provide computer-generated labels; handwritten labels shall not be accepted.

G. Identify power circuits and breaker locations within each power supply cabinet. This shall include any remote power supplies.
H. Label Materials

1. Conductor and Cable Labeling
   a. Provide T&B Shrink-Kon Type HVM or equal labels.
   b. Labels shall be computer or machine generated and fastened to conductors/cables. Hand-written labels shall not be accepted.

I. Label wires and cables as follows:

1. Mark all wire and cable in common at both ends.
2. Install markers to be a readable font size from left to right or top to bottom. Locate labels near termination points.
3. Install labels when wire and cables are installed.
4. Labeling shall agree with record documentation.

J. Control Panels, Power Supplies and Termination Cabinets

1. All Control Panels and Intrusion DMP XR550m control panels will be assigned a unique account number by TAMU IT after the contractor submittals have been reviewed. Labels on each control panel shall read: “ACCT: XXXX. XXXX represents a 4 digit account number.

2. Each termination cabinet associated with a Control Panels shall have a label that reads: “Control Panels XXXX TERMINATION”. XXXX represents a 4-digit account number.

3. Each power supply associated with a Control Panels or Intrusion shall have a label that reads: “DGP XXXX YYYY PS”. YYYY represents the type of equipment being powered. For example, “Control Panels 1234 LOCK PS” represents the lock power supply for DGP #1234.

K. Control Panels Cables

Accounts: 0001-2000
- Control Panels account
  - 4 digits Board – 1 digit
- Address – 2 digits
- Device – 2 characters
- Input (DI) or output (DO) – 2 characters

Examples:
- [account#]_[board#]_[address#]_[input or output type] [device type] [room or door number]

  0172_2_00_DI
  CR 1.108

L. Intrusion Cables

Accounts: 3001-9999
- Account – 4 digits
- Zone – 3 digits
- Device – 2 characters

Examples:
- [account#]_[zone#]_[input or output type] [device type] [room or door number]
3.10 PROGRESS OBSERVATIONS

A. Security consultant and/or TAMU Project Manager will conduct progress observations during construction to verify construction progress and verify the construction schedule. Coordinate progress observation site visits with the Contractor. Provide Contractor with copies of progress observation reports and other applicable documentation for inclusion in the Commissioning and Closeout Manual.

B. Security contractor shall coordinate appropriate timing of each observation with the general contractor, security consultant and/or TAMU Project Manager as required to meet intended goals.

C. The inspectors will issue reports for each observation to summarize findings and document clarifications noted during the observation and distribute within two (2) business days to contractor, consultant, integrator, security operations and University hardware consultant.

3.11 COMMISSIONING

A. The following activities shall take place to complete the installation of the security system. Documentation of activities, corrective action items and status, and activity completion verification shall be provided to the Contractor for inclusion in the Commissioning and Closeout Manual.

1. Operational Field Testing
   a. Operational Field Testing can be scheduled once the communications cabling contractor has completed the portion of the voice and data network which supports the new security system.
   b. Building Access and Security will review updated system programming forms and make changes as needed.

2. Functional Tests (FT)
   a. Utilize FT checklists created by Building Access and Security.
   b. Contractor shall provide two sets of preliminary as-built drawings to Building Access and Security and the security consultant at least 15 days before the FT process is scheduled to start.
   c. Once operational field-testing procedures have been documented and completed, the final FT walkthrough can begin. The contractor shall demonstrate to Building Access and Security and the security consultant during a full walkthrough inspection that the completed and integrated system complies with the contract documents, initial training is complete, and the system is fully operational.

3. Integrated System Test (IST) 7 days prior to substantial completion.
   a. Consult Building Access and Security on IST
   b. Test critical system interfaces such as fire alarm and elevators.

4. At the conclusion of the project the contractor shall provide an electronic copy, in PDF and AutoCAD format, of the as-built drawings which will be updated and fully reviewed version of the submittals. As-buils shall incorporate all changes to the project including security system design modifications, architectural changes and updated room numbering and be submitted to Building Access and Security prior to substantial completion.

B. Substantial completion requirements:
   1. All keyless access and camera components shall be fully installed and operational.
   Any punch list items as a result of the FT or IST will not interfere with the operation of the security system.
PART 4 – REVISIONS TO DESIGN STANDARD

<table>
<thead>
<tr>
<th>Revision #</th>
<th>Date</th>
<th>Location</th>
<th>Brief Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

END OF SECTION
The following appendices are considered part of this Design Standard:

Appendix A – Camera Installation Guidelines
Appendix B – Wiring and Installation for HID Card Readers
Appendix C – Access Control Checklist
Appendix D – Surveillance Camera Integration Policy
Appendix E – TAMU Camera & Keyless Wiring Standards (Existing Buildings)
Appendix A

Camera Installation

Considerations to Mounting Cameras

Mounting and Aiming Video Analytics Cameras

When installing an Avigilon video analytics camera, follow the listed mounting and aiming recommendations to maximize the camera’s analytics capabilities:

1. The camera should be installed above 9 feet (2.74 m).
2. The camera should tilt downwards no more than 45 degrees.
3. The camera image should be level with the horizon line.
4. The camera should be mounted to a stable surface to minimize the physical movement of the camera after installation.
5. The mounting surface must withstand five times the camera weight.

Inserting Cables through the Sealing Grommet

Unless specified otherwise, you must pull the required cables through the sealing grommet included with the camera when using a cable entry hole. If installing an indoor camera, this step may not be required.

1. Remove the sealing grommet from the camera.
2. Pull the tab on the grommet to open a hole for the Ethernet cable.
3. Push an Ethernet cable through the grommet by one of the following methods:
   a. If the Ethernet cable is uncrimped, push the cable through the grommet.
   b. If the Ethernet cable is already crimped, place the grommet piercing cap on the Ethernet connector then push the cable through the grommet.
4. Push all required cables through the grommet.
   *Note: if pulling multiple cables through the grommet, apply silicone sealant to seal any gaps in the grommet.

Mounting & Aiming

1. To mount the camera, use the Mounting Template and included screws to mount the camera to a suitable surface.
2. Dome Cameras: After the camera is mounted, remove the dome cover with the security Torx wrench and then loosen the pan & tilt set screws to adjust the camera’s view and position. Clean the inside and outside of the dome cover using the provided cleaning cloth.

3. Bullet Cameras: After the camera is mounted loosen the pan and tilt screw at the base of the camera’s bracket with the security Torx wrench to adjust the camera’s view and position.

4. Tighten the pan and tilt lock screws to secure the dome camera’s position.

5. Rotate the azimuth control ring to set the image to the correct angle.

6. In the camera web browser interface or the Avigilon Control Center software, adjust the camera’s Image and Display settings. You can set the zoom position, focus, and change the image rotation.

7. Follow manufactures mounting and installations instruction based on the specific camera model, mounting hardware and location.

Zooming and Focusing the Camera

For dome cameras ensure this procedure is performed after the dome cover is installed, so you can accommodate for the focus shift caused by the dome bubble.

1. In the camera web browser interface or the Avigilon Control Center software, use the camera’s Image and Display settings to zoom and focus the camera.

   a. Use the zoom buttons to zoom the camera in or out.
   b. Click Auto Focus to focus the lens.
   c. Use the focus near and far buttons to manually adjust the focus.

Connecting to the Camera

Initializing a Camera Username and Password - Cameras manufactured after January 1, 2020, do not have a default username or password and will be in a factory default state.

Important: You must create a user with administrator privileges before the camera is operational.

The first user can be created using any of the following methods:

- Camera’s Web Interface: enter the camera’s IP address in a web browser to access the web interface. If the camera is in the factory default state you will be redirected to the Add a new user page to create the first user. For more information, see the Avigilon High Definition H4 and H5 IP Camera Web Interface User Guide.

- Camera Configuration Tool: cameras discovered in the factory default state will be identified by . Select the Admin Users tab to create the first user. For more information, see the Avigilon Camera Configuration Tool User Guide.

- USB Wi-Fi Adapter: when connecting a camera in the factory default state, you will be redirected to the Create Administrator User page to create the first user. For more information, see Motorola Solutions. USB Wi-Fi Adapter System User Guide.

- Avigilon Control Center software version 7.4 or later, or version 6.14.12 or later: when connecting a camera in the factory default state, the client software will ask you to create a new user. For more information, see the Avigilon Control Center Client User Guide.
• Avigilon Cloud Services (ACS) v3.0 or later: when adding a camera you will be asked to create a new user for cameras in the factory default state. For more information, see the Avigilon Cloud Services User Guide.

• Using the USB Wi-Fi Adapter If you have a USB Wi-Fi Adapter (H4-AC-WIFI), attach it to the camera’s micro-USB port (micro-USB to USB adapter required) to access the camera’s mobile web interface. After you connect to the Wi-Fi signal broadcast via the adapter, you can access the mobile web interface from any mobile device using the following address: http://camera.lan

The USB Wi-Fi Adapter creates a Wi-Fi network when it is connected to the camera. Once the Wi-Fi network is active, you can connect and access the camera’s mobile web interface.
1. Connect one end of the micro USB to USB cable to the camera. For more information, see the illustrated instruction manual provided with the USB Wi-Fi Adapter System.
2. Connect the USB Wi-Fi Adapter to the other end of the cable.
3. On your mobile device, access the wifi settings page and connect to the following wifi network: AvigCam-<last 6 digits of the USB Wi-Fi Adapter MAC address> For example: AvigCam-12a4b6
4. If prompted to enter a password, enter: avigilon
5. Access the camera's mobile web interface at camera.lan.
*If you are not automatically prompted to enter the username and password for the mobile web interface, open your web browser and enter http://camera.lan.
*The USB Wi-Fi Adapter automatically redirects you to the correct IP address even if the camera has been assigned a specific IP address.
*Cameras manufactured after January 1, 2020, do not have a default username or password and will be in a factory default state.
**Important: You must create a user with administrator privileges before the camera is operational.

When you are prompted, enter the camera’s administrator username and password.
Depending on the manufacture date of your camera, you will have one of the two options below to log in for the first time:
▪ Cameras manufactured after January 1, 2020: these cameras do no have a default username or password and will be in a factory default state. Login with the username and password that you create when first connecting. For more information, see Creating the Initial User and Logging In.
▪ Cameras manufactured before January 1, 2020: login to the camera using the default username of administrator with no password. It is recommended that you change the password after you first login.
6. The first page you see displays the camera's live video stream. You can adjust the camera's zoom and focus from this page. For more information, see Configuring the Camera.
7. After you finish configuring the camera from the mobile web interface, disconnect the USB Wi-Fi Adapter.

Configuring the Camera
Once installed, use one of the following methods to configure the camera:

- If you have the USB Wifi Adapter, you can access the mobile web interface to configure the camera. For more information, see Avigilon USB Wi-Fi Adapter System User Guide.
- If you have installed multiple cameras, you can use the Camera Configuration Tool to configure common settings. For more information, see the Camera Configuration Tool User Guide.
- If the camera is connected to the Avigilon Control Center system, you can use the client software to configure the camera. For more information, see the Avigilon Control Center Client User Guide.
- If the camera is connected to a third-party network management system, you can configure the camera’s specialty features in the camera’s web browser interface. For more information, see the Avigilon High Definition H4 and H5 IP Camera Web Interface User Guide

Notice:
These instructions provide general guidelines related to the installation of surveillance cameras. As such they are not intended to be a comprehensive installation guide. For detailed instructions and specifications refer to the manufacture’s website or printed materials.
All installations must comply with national, state and local building and fire codes. In addition to the guidelines provided in this document the contractor must also adhere to all provisions listed in section 280000 - ELECTRONIC SECURITY of the Texas A&M University universal standards document. Exclusions or omissions in this or other documents do not relieve the contractor from responsibility for following all building, electrical, safety, fire or other codes or industry best practices.
APPENDIX B

WIRING & INSTALLATION FOR CARD READERS

Service Description

Site Survey

Perform physical site survey with system integration contractor, TAMU construction project manager, and building access leader, to confirm

- Number, location and placement of readers, controllers, power supplies and other devices required for a complete building access system based on documented requirements.
- Wire routing, distances, and locations
- Requirements and needs related to the installation
- System integrator will provide Time and Materials Cost Estimate as requested.
- Project manager or Facility Coordinator will provide as much detail as possible including building diagrams and site drawings.

Wiring – Pre-Work Rough In.

Recommended parts for HID Signo reader installation

- Cable, 5-10 conductor (Wiegand or Clock-and-Data), 4 conductor Twisted Pair Over-All Shield and UL approved, Belden 3107A or equivalent (OSDP)
- Certified LPS DC power supply
- Metal junction box
- Security tool HID 04-0001-03 (for anti-tamper screw)
- Mounting hardware
- Reader spacer when mounting on or near metal or metal junction boxes.
- Junction box

Pre-Work Rough-In Activities

1. Verify the work to be performed.
2. Run Cable, 5-10 conductor (Wiegand or Clock-and-Data as specified), 4 conductor Twisted Pair Over-All Shield and UL approved, Belden 3107A or equivalent (OSDP) to reader install location via common methods and procedures. Refer to design document for location.
3. Tag and label all wire run with permanent wire markers according to university design standards.
4. Terminate all cables according to university design standards.
5. For specific wiring instructions & mounting refer to project documents and university design standards.
6. Validate physical continuity of all cables and connectors installed as part of work order.
7. Ensure all installation procedures comply with business, building, fire code regulations and university design standards.
8. All wiring and reader installations must comply with section 280000 - ELECTRONIC SECURITY of the Texas A&M University standards document.
9. All installations must conform with ADA requirements.
HID Signo Reader Installation

- HID Supplied parts
- HID Signo Reader (1)
  - Installation Guide (1)
- Flat head/countersunk 0.138-20 x 1.5" self–tapping screws (2) – for installing the reader directly to a wall (no junction box)
- Flat head/countersunk 0.138-32 x 0.375" machine screws (3) – for Imperial (US) junction box installation (2) and attaching the reader to the mounting plate (1)
- Flat head/countersunk M3.5 x 12mm machine screws (2) – for Metric (EU etc.) junction box installation
- Flat head/countersunk 0.138-32 x 0.375" security screw (1) – alternative anti-tamper screw for attaching the reader to the mounting plate
- 5-pin terminal connectors, terminal strip models only (2)

1. **Mount the mounting plate**

   1. Install the reader on a flat, stable surface. Failure to do so may compromise the IP rating and/or tamper feature. If mounting on or near metal, a spacer is recommended for optimal read performance. Refer to the Readers and Credentials How to Order Guide (PLT-02630) for available options and part numbers.
   2. Use the supplied screws to ensure correct fitting and to avoid damaging the reader or mounting plate. HID is not responsible for damage due to use of unapproved mounting hardware.

      a. Imperial (US): Use supplied flat head/countersunk 0.138-32 x 0.375" screws.
      b. Metric (EU etc.): Use supplied flat head/countersunk M3.5 x 12mm screws.
2. **Wire the reader**

   1. Wire the reader according to the wire scheme below

<table>
<thead>
<tr>
<th>PIGTAIL</th>
<th>TERMINAL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Red</td>
<td>1</td>
<td>+ VDC</td>
</tr>
<tr>
<td>Black</td>
<td>2</td>
<td>Ground (RTN)</td>
</tr>
<tr>
<td>White</td>
<td>3</td>
<td>Wiegand Data 1 / Clock / RS485-*</td>
</tr>
<tr>
<td>Green</td>
<td>4</td>
<td>Wiegand Data 0 / Data / RS485-B*</td>
</tr>
<tr>
<td>Orange</td>
<td>5</td>
<td>LED Input (GRN)</td>
</tr>
<tr>
<td>Yellow</td>
<td>6</td>
<td>Beeper Input</td>
</tr>
<tr>
<td>Blue</td>
<td>7</td>
<td>Hold Input / LED Input (BLUE)*</td>
</tr>
<tr>
<td>Brown</td>
<td>8</td>
<td>LED Input (RED)</td>
</tr>
<tr>
<td>Violet/White</td>
<td>9</td>
<td>Tamper 2 (RLY2)</td>
</tr>
<tr>
<td>Violet</td>
<td>10</td>
<td>Tamper 1 (RLY1)</td>
</tr>
<tr>
<td>Bare</td>
<td></td>
<td>Drain (pigtail models only)</td>
</tr>
</tbody>
</table>

   **Note:** Wiring the reader incorrectly may permanently damage the reader.

   **Note:** Previous iCLASS® readers had reversed RS-485 wiring (P2-7 & P2-6 - A & B). When upgrading to a HID Signo reader, ensure proper connections as defined above.

   **Note:** Data 0 and Data 1 wires for Wiegand may be reused for OSDP. However, standard Wiegand cable may not meet RS485 twisted pair recommendations.

   **Note:** For OSDP cable lengths greater than 200 ft (61 m) or EMF interference, install 120Ω +/- 2Ωresistor across RS-485 termination ends.

   **Note:** For keypad configuration, with the keypad reader operating as 26 bit emulation, enter the facility code followed by # within five seconds of power-up. The facility code must be entered as three digits (i.e., for a facility code of 10 enter 0-1-0-#). If unsuccessful, the reader LED displays solid red. Power-cycle the reader and retry entering the facility code.

   HID Signo readers use facility codes between 1-255, and no default is set. Once a facility code is entered, the reader LED displays violet, then solid red. Then, power-cycle the reader. If there are two short beeps after entering a PIN, the reader facility code is not configured. In this case, power-cycle the reader and retry entering the facility code.

3. **Secure the Reader to the mounting plate**

   1. Hook the top of the reader on the top of the mounting plate.
   2. Align the bottom of the reader with the bottom of the mounting plate.
   3. Secure the reader to the mounting plate using the supplied screw. Security/anti-tamper screw: 0.138-32 x 0.375" screw (supplied)
4. **Power and test the Reader**
   1. Power the reader. The reader will beep and the LED will flash.
   2. Test the reader with a valid Aggie Card. The reader will beep and the LED will flash.

---

**Input Voltage**
- 12V DC

**Communication Lines Cable Lengths**
- Wiegand = 500 ft - 18 AWG (152 m)
- 300 ft - 20 AWG (91 m)
- RS-485 = Max bus length: 4,000 ft - 24 AWG (1,219 m)
- Max length between nodes: 1,640 ft - 24 AWG (500 m)

**Operating Temperature**
- -30° F to 150° F

**Notice:**
These instructions provide general guidelines related to wiring and installation of keyless access systems. As such they are not intended to be a comprehensive installation guide. All installations must comply with national, state and local building and fire codes. In addition to the guidelines provided in this document the contractor must also adhere to all provisions listed in section 280000 - ELECTRONIC SECURITY of the Texas A&M University universal standards document. Exclusions or omissions in this or other documents do not relieve the contractor from responsibility for following all building, electrical, safety, fire or other codes or industry best practices.
## APPENDIX C

### Access Control Checklist

<table>
<thead>
<tr>
<th>Category</th>
<th>Installer</th>
<th>Texas A&amp;M</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installing Wiring, Cameras &amp; Mounts</td>
<td>Yes / No</td>
<td>Yes / No</td>
<td></td>
</tr>
<tr>
<td>Category cable terminated using T568B pin out</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure all camera mounts, cameras, junction boxes, conduit, and wiring are secure and without play, slack, or gaps.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure all cameras, mounts, hardware are secure and tamper resistant</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure all cameras, mounts, and hardware are installed using proper weather proofing techniques</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All wiring is run according to State &amp; local codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wall penetrations and conduit are properly sealed according to NFPA and applicable fire codes</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Tag both ends of wire with permanent numeric wire ID tags</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(handwritten, electrical tape or identification written directly on the wire jacket is not acceptable)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Wiring is to be neatly secured using cable ties or hook &amp; loop fasteners</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensure cables are secured to supports (J/P-hooks, ceiling truss, etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Conceal cables using conduit, Panduit or wall fish where possible/required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All exterior wire runs must be in conduit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>All interior wire runs below 10’ must be in conduit</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Leave properly coiled and dressed service loops at camera location, switch and head end as required</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cabling is at least 18” from power lines of 2 kVA or less</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cabling is at least 3’ from fluorescent lighting &amp; power lines between 2 &amp; 5 kVA</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cabling is at least 2’ from transformers and motors</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cable has been checked for shorts, opens, continuity</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Intermediate or secondary switch locations must be noted on the wire ID chart

Cable has been terminated according to industry and A&M standards using T568B pinout

The Cable length doesn’t exceed the maximum capable distance for cable type

### Cameras

- Adequate Power is provided to power the camera. (Check power cable at camera end to confirm)
- Camera lens used provides the required field of view
- Cameras do not face directly into the sun when installed outdoors or any lighting when installed indoors
- Cameras installed according to manufactures instructions related to temperature, humidity, and environmental conditions
- Cameras do not face reflective surfaces or glass that will reflect IR illuminators back into the camera lens
- The camera view is in focus all the time under changing lighting conditions
- IR illuminators properly activate and deactivate according to lighting conditions
- Camera field of view does not violate reasonable expectation of privacy, or local laws and regulation
- All cameras have been tested for proper image quality according to system design (pixels per foot)

### Installation Wrap-up

- Work areas left neat clean - swept, dusted and free of debris
- All packaging, debris, boxes, old parts, etc. disposed of in a commercial dumpster not office trash cans
Electronics, wiring, components, parts, etc. must be disposed of in accordance with Federal, state, and local laws and University policy regarding hazardous waste and recycling.

As-buils drawings provided to Texas A&M (Digital copy)

**System Validation**

Camera recording and access to recorded video has been verified

Accuracy of recording verified, based on the timestamp and the actual time

All Video Analytics features on each camera tested and verified

Cameras are named using A&M approved naming convention

*Example.* Bldg. #.Room #.Brief Descriptor

0444.101E.Break Room

0518.541E.Office

Assign and document IP address(es) of each camera.

Create additional users as specified

UPD access verified

Building owner trained

**Avigilon Signoff/Project Completion**

Has Sales Engineer with Avigilon reviewed programming and ACC Setup and signed off
Surveillance Camera Integration Policy

Building owners, Department head, Facility Management

When presented with an opportunity to integrate a preexisting set of cameras, the following conditions should be understood and presented to the customer.

Terms:

**Fully Interoperable:** This refers to cameras that will provide full integration of features and functions on the Avigilon platform. These cameras are fully compatible with the Avigilon NVR and support all required analytics features. At this time only Avigilon H5 or newer cameras are considered fully supported and interoperable.

**Fully Supported:** The term "Supported" means Texas A&M video surveillance technicians, system administrators and internal I.T. are able to provide end to end support for the camera.

**Compatible:** This category of cameras are NOT Avigilon branded or sold by Avigilon, but are likely to work within the Avigilon system architecture and surveillance NVR. These cameras may provide live and recorded viewing but may not support analytics features.

Conditions:

For customers with existing camera systems as requested technicians will connect the customers’ existing cameras to the Avigilon system.

- The fact that a camera is currently working on an independent system is no guarantee that it will be compatible with the new Avigilon system being installed.
- If the takeover camera comes up and works, the Field Service Tech will proceed to the next camera or task on the security installation checklist.
- If the customers cameras do not come up on the Avigilon Surveillance NVR System with live video and ability to record:
  - If the cameras come up but display errors, will not record, or otherwise prove troublesome, the Tech will attempt basic troubleshooting of cable terminations, connectors, and network connections.
  - If the technician is unable to resolve the issue the camera will be removed from the system.
    - The customer may opt to purchase and Avigilon camera as a replacement.
- Technician will not use any customer supplied materials or spend time conducting internet searches for assistance in determining how to get the customer owned equipment working.
- At no time will the Technician install or attempt to install or upgrade firmware of any kind onto the customer owned camera or equipment.
- Technicians will spend no more than a total of 30 minutes troubleshooting a customer’s entire existing camera installation before removing or replacing cameras.
- If the technician is able to get the customer’s existing camera working, there is no implied guarantee that customer owned equipment will continue work properly or provide full camera or NVR functionality.
• There will be no option for independent or standalone systems. Once the building is converted to Avigilon surveillance all cameras and components not installed or integrated as part of the Avigilon conversion will be removed. Regardless of age, condition, or operability independent or standalone cameras or camera systems will be removed at the time the building is converted.

Support
• If necessary, the AVST administrator or technician will perform a preliminary evaluation of camera and NVR interoperability before starting troubleshooting. Technicians will only troubleshoot the functionality of the NVR, switch, connections, and network but will not troubleshoot customer provided cameras.
• If the existing camera or camera system continues to be problematic the Technician will remove the equipment and refer the customer to their AVST leader for an estimate to replace existing equipment.
• There is no warranty for existing customer owned hardware that is integrated/taken over and added to the Avigilon system. As a result, the customer will be responsible for costs to maintain or replace takeover cameras.

Not Interoperable:
• Cameras and systems purchased and installed independently. Typically, items purchased from Retail Box Store, online resellers and DIY are typically not interoperable.
• Any camera that does not comply with NDAA regulatory requirements will not be allowed on the network. These cameras will never be allowed on the network regardless functionality.
Texas A&M University
Camera & Keyless Wiring Standards
(Existing buildings)

II. Outside of the Communications Rooms
A. Horizontal cable run requirements:
   *NOTE: These standards only apply to pre-existing buildings. New construction or building renovations must follow Texas A&M University Network Installation Design Standards (commonly referred to as “Red Book - division 27”).

   1. Contractor shall only use approved cable basket tray, stand off or j-hooks for all primary horizontal cable runs.
   2. Cables shall never share a path with other trades’ low voltage cable or electrical.
   3. Cable installations above solid ceilings should follow, but not share path with other network cable.
   4. Cable installations in drop ceilings shall only use approved cable basket tray, stand off or j-hooks for all horizontal cable runs. Cable must be attached to a permanent building structure. Cable shall not be left in contact with drop ceiling tiles except for required service loops.
   5. Cable installations on building exteriors shall be in EMT conduit. A conduit body (pull station) shall be installed every 50’. A wet location single gang junction box shall be installed at the point where wire penetrates the wall. Industry best practice weatherproofing techniques shall be used to prevent water from migrating into the building.
   6. Cable installations on rooftops shall be in EMT conduit. Conduit should follow existing pathway. Conduit shall be raised off of the roof surface a minimum of 4”. A conduit body (pull station) shall be installed every 50’. A wet location single gang junction box shall be installed at the point where wire penetrates the building. Industry best practice weatherproofing techniques shall be used to prevent water from migrating into the building.
   7. Cable installations involving a Wall fish may be installed directly in-wall and do not require conduit or a junction box.
   8. Surface mount cable installations on building interiors shall use approved surface mounted raceway such as Panduit and terminate in a junction box.
   9. Cable installations in riser closets or where cables are run vertically between floors should follow, but not share, existing wire path. It is recommended that EMT conduit be used. Holes and conduit must be sealed with fire block that meets NFPA standards.
10. Cable installations in Historical buildings must be reviewed and approved by the university architect.
11. Any cable penetrating a wall shall be properly weather sealed to prevent water migration. Additionally, all holes and conduit must be sealed with fire block that meets NFPA standards.
12. Conduit no more than 180 degrees of direction change/bend in each “section” of conduit. After 180 degrees, a conduit body/pull box needs to be added.
13. There shall be a service loop at each termination point:
   a. Service loop in the I.T., IDF, MDF closet shall be coiled or left in a figure 8 per minimum bend radius and attached with Velcro or hook and loop to the outside of the cable basket tray. **Do not** leave cable slack in cable basket tray.
   b. Service loop shall be provided at each camera, card/biometric reader and shall minimum bend radius and provide sufficient slack to allow service technicians to remove and service the device without undue difficulty.
14. All conduit shall have plastic bushings at both ends to protect cable.
15. J-hooks are acceptable ONLY in existing buildings.
17. Cable runs shall have a manufactured label that follows the Texas A&M wire identification scheme.

**III. Testing**

**A. Cable testing**

1. Contractor shall test and certify the data wiring systems for conformance with the ANSI/TIA-568-C.2-2 CAT 6 or CAT 6A wiring standards.
2. Contractor shall provide test results prior to project closeout.
3. Contractor shall provide laminated, half-size, as-built drawing per communications room indicating each outlet location, final room number and outlet number.
4. Contractor shall provide laminated wire ID sheet per communications room. Duplicate wire ID sheets shall be provided to the facility coordinator and keyless or AVST leader.

**Appendix A:**

1. Wiring termination
   a. CAT 6 shall be T-586B pinout

РJ45 Pinout

T-568B

1. White Orange
2. Orange
3. White Green
4. Blue
5. White Blue
6. Green
7. White Brown
8. Brown