



# Facilities Planning and Construction

## Design & Construction Standards

### **DIVISION 28 – Electronic Safety & Security**

#### **Preface**

The Texas Tech University System's '*Design and Construction Standards*', as administrated by Facilities Planning and Construction, are intended to serve as guidelines to the Design Professional and Construction Management teams for design development and construction administration of Texas Tech University System (TTUS) Capital Projects. They communicate the minimum expectations and requirements relative to specific building systems, design provisions, general specification requirements, and administrative procedures for new facilities being constructed on Texas Tech University System (ASU, MSU, TTU, TTUHSC, and TTUHSC El Paso) campuses. Several, but not all requirements for each component Institution or Agency within the TTU System are covered. Design Professionals, Construction Managers at Risk and/or Design-Build Firms shall also refer to provisions covered in their service Agreements, as well as within the project's Basis of Design (BOD) document.

In addition, the 'Design and Construction Standards' shall also be utilized in conjunction with the approved project specific Program and Schematic Design development. In the event of conflict between this document and specific project requirements, Design Professionals, Construction Managers at Risk and/or Design-Build Firms shall contact Facilities Planning & Construction for clarification.

The guidelines within the '*Design and Construction Standards*' are not intended to prohibit the use of alternative design solutions, methods, systems, products or devices not covered in this document. Offered alternatives deviating from or not covered in these standards shall be documented by the Design Professional and/or Construction Management teams and submitted to Facilities Planning & Construction for approval prior to implementation.

Throughout the '*Design and Construction Standards*' there are references to manufacturer specific products. These are to be considered the 'Basis of Design' to establish the expected minimum quality requirements. Design Professionals are encouraged to identify and include equivalent products and/or manufacturers offering comparable products to facilitate open bidding environments.

### **28 13 00 Access Control**

Refer to Texas Tech **OP 61.14 “Electronic or Keyless Locking Systems”** (security systems in housing facilities are not addressed in this OP).

Each component Institution (ASU, MSU, TTU, TTUHSC, TTUHSC El Paso) Facilities Department is responsible for the management of all locking systems. Electronic access control is managed through each component Institution’s Police Department. Standards may vary contingent on the Agency in which the project is being executed.

Standards and programs have been established for the control and issuance of keys, development of keying systems, standardization of hardware, and maintenance programs for the upkeep of these systems. Installation of systems other than those approved in the standards or deviation from the standards may occur only with the approval of the Managing Director of BMC under the guidelines set forth in this OP.

Due to the large number of electronic or keyless security systems available on the open market, standards and limitations must be established for the use of these systems on the TTU campuses. The option to choose between the two approved access control systems provides departmental security and flexibility without jeopardizing existing security and affords Texas Tech Police Department the ability to maintain the systems without heavy investment in inventories and equipment.

Two electronic access control locking systems have been selected that will serve the requirements of most departments. Requests to install electronic or keyless locking systems will be limited to the systems described in OP 61.14. The elected systems allow any departmental requirement to be met. Each component Institution’s Lock Shop and the Texas Tech Police Department will assist departments in making selections. The only electronic access control locking systems allowed on campus will be C-CURE for exterior building perimeter security or CS Gold (CBORD) for Student Housing facilities and interior door access control. The two approved systems are limited to:

#### **C-CURE 9000 Manufactured by Tyco – Software House**

C-CURE is a scalable security management solution encompassing complete access control and

Division 28 - Electronic Safety & Security

advanced event monitoring. The system integrates with critical business applications including video systems from American Dynamics, as well as third-party devices such as fire alarms, intercoms, and burglar and other alarms. This system is managed and maintained by the Texas Tech Police Department.

The TTU official ID card can be used for access or specialized access devices are obtainable from vendors at the expense of each department on campus. The Texas Tech Police Department can assist in providing a list of vendors for purchasing these devices. The Texas Tech Police Department will maintain a list of authorized people who can request and approve access to employees or students.

Access changes including removal, addition, or transfer will be completed through the KMS <https://odis.operations.ttu.edu/odkms/default.aspx>. The Texas Tech Police Department is located at **413 Flint Avenue** and will make changes to the system between the hours of 8 a.m. and 5 p.m., Monday through Friday.

### **CS Gold (CBORD)**

CS Gold offers wireless or wired on-line locks, including biometric readers. CS Gold hardware within E&G facilities will be installed and maintained by the Electronic Maintenance Shop and the Lock Shop. Access changes including removal, addition, or transfer will be completed through the KMS (<https://odis.operations.ttu.edu/odkms/default.aspx>). The CS Gold systems security features include Banner daily synchronization, lock down, and emergency modes. New employees, students, or existing staff can obtain new or replacement TTU ID cards from the TTU ID Office located at the Student Union Building, Room 103, between the hours of 8 a.m. and 5 p.m., Monday through Friday.

Any new electronic or keyless system will interface or coexist with the existing restricted keyway system.

The existing master key will remain functional for service, custodial, police, and emergency access. If an electronic key/card system replaces the existing key/lock system, the university Lock Shop will control the issuance of key/cards under the same provisions outlined in **OP 61.15 “Control and Issue of Keys to University Buildings”**.

All access control providers interested in bidding must have a valid license through the Texas

Division 28 - Electronic Safety & Security

Department of Public Safety and Private Security Bureau for their portion of the work. The awarded Contractor will be required to submit this information to the Texas Tech Police Department. The Texas Tech Police Department may validate the licensing submitted with the State at their option.

### **Access Control System**

Specifications are to be based on the Software House C-Cure 9000 Security Management System. The existing security management system (C-Cure System) is managed by TTPD and hosted at TOSM. Contractor will be required to provide Ethernet connection and programming of new Software House security devices, camera system and controller to be accessed on Texas Tech Police Department existing C-Cure Security System. The Company of Record for the Texas Tech University C-Cure System is Firetrol. Firetrol will be the only electronic security company authorized to modify/program the existing C-Cure system front end server located at TOSM.

*NOTE: TTU University Student Housing is currently using CS Gold (CBORD) as their card access system and Bosch DVR's or ExacqVision for their video surveillance. The CBORD card access system is/has been used in existing academic/administration buildings where "security" is not needed but card access is needed. The Design Professional needs to clarify with the Owner and TTU Police Department on the type of system to specify.*

The access control system will be a separate system from the video surveillance camera system. The access control system will operate from existing C-Cure software system managed by the Texas Tech Police Department.

The access control system shall be from a single-source manufacturer that specializes in intrusion detection and access control systems with a minimum of five years' experience. Installer shall be a company specializing in intrusion detection and access control systems with a minimum of three years' experience on systems of similar size and scope. Technicians working on project must have been certified on the hardware and software used for this project. Companies bidding on the project and their salesmen MUST have a valid license through the Texas Department of Public Safety, Private Security Bureau for their appropriate portion of the work. Additionally, the company that is awarded the project, their salesmen and all technicians that work on the project MUST have a valid license through the Texas Department of Public Safety, Private Security Bureau. This licensing may be checked by the Texas Tech Police Department at any time. Violations may be filed as appropriate.

A final inspection walk-through will be conducted with the Texas Tech Police Department to verify system operation and final acceptance of the work.

### **Access Control General Design Guidelines**

1. Perform two (2) scheduled preventative maintenance site visits per year during the warranty period.
2. Normal business hours shall be 8 AM to 5 PM Monday through Friday. Calls for service before noon shall be responded to on-site before the end of the day. Calls after noon shall be responded to on-site by noon the following business day.
3. The access control integrating company selected to install and maintain the system shall have duplicate system parts available within 50 miles of installation site should any part of the system fail.
4. All cabling and wiring must meet University guidelines. Specifically, cabling may be installed in above ceiling cable trays. Cabling that is not utilizing above ceiling, housed within cable trays or leaving from a cable tray to a final destination should be in conduit of the appropriate size to accommodate the specific number of cables or low voltage wiring required. All device cabling and wiring shall be labeled correctly with pathways identified before termination in the iStar panel. Junction boxes above controlled/monitored doors or windows shall be placed above the ceiling on the secured side of the opening. Junction boxes shall not be accessible from the non-secured side of the door.
5. All security access and camera systems shall derive power from new emergency panels (fed from generator). 12-volt battery backup to provide 12 hours of standby power supply shall be provided.
6. The iStar intelligent field controller panels should be installed in climate-controlled areas such as phone or technology rooms where access is controlled by maintenance or “tunnel” keys. Electronic security control systems are not to be planned or scheduled to be installed in the Main Distribution Frame (MDF) or Intermediate Distribution Frame (IDF) spaces.
7. Wiegand mag stripe readers will not be an acceptable way to control access to controlled doors. Proximity readers or proximity readers with keypads are to be specified at locations (controlled doors) where card access is required. Wiegand HID proximity readers, Software House proximity readers and Software House proximity readers with keypad and LCD display are required.

Division 28 - Electronic Safety & Security

8. An Ethernet network port that resides on the TTPD secured V-Lan is required. The cost of this port shall be incorporated into the cost of the project and arranged through the component Institution.
9. Door contacts and Request to Exit devices for monitored doors may be used at locations (doors or windows) needing to monitor the status of such locations. Contacts hidden in the door frame and door are preferred, however, external contacts may be used where hidden contacts are not feasible. Magnetic contacts behind hinges, push button switches or 'roller ball switches' on doors are not acceptable.
10. In a new building construction, all building perimeter exterior doors are to be monitored, including all roof hatches.
11. All projects shall include digital graphical mapping installed on the C-Cure server and/or at the monitoring stations. The graphical mapping system shall allow digital graphics and floor plans to be linked to points and events within the system.
12. Each card access-controlled door shall include four devices: card reader, door contact, electronic lock or crash bar and a request to exit. Controlled doors not requiring card access shall include three devices: door contact, electronic lock or crash bar and a request to exit. These doors should be set up in the system as a "door" and not an "output and two inputs". No doors should have only a contact and electronic lock.
13. Individual inputs (panic switches or individual door contacts) or outputs should be terminated on an expansion card, leaving the inputs and outputs on the ACM available for future controlled door expansion.
14. No fire alarm devices shall be attached to the system for the purpose of primary reporting.
15. Final "as-built" drawings shall be supplied at the completion of the project.
16. A final walk through shall be conducted for acceptance of work.

### **Warranty and Service Requirements**

All equipment, materials, and labor shall have a two-year warranty from the date of final acceptance by the Owner. Provide any software maintenance updates or upgrades at no additional cost to the Owner for this period.

### **Basic Central System Components**

If a new installation at a regional campus is needed, a computer server running the CCure9000 system may be required. This server will control all buildings at the regional campus.

Division 28 - Electronic Safety & Security

A minimum of one Software House iStar intelligent controller enclosed in a metal case using a locking device keyed the same as the existing panels on campus shall be provided for each project. Software House APS power supply for iStar intelligent field controller. Field devices will not be powered from this power supply.

1. Security Controllers: Software House I-star Edge or Ultra.
2. IP-enabled Control Panel. Unless otherwise noted, provide 16-door controller.
3. Input Modules: Software House I8-CSI. Enclosure: RM-DCM-CAN.
4. Output Modules: Software House R8 Output Module. Enclosure: RM-DCM-CAN.
5. Card Readers:
  - a. Wiegand HID MultiCLASS SE
  - b. Software House
6. Door Strikes or electronic lock: TBD based on door configuration and TTPD recommendations.
  - a. Maglocks are not an acceptable way to secure any area. Exceptions must be approved by the AHJ and TTPD.
  - b. Locking devices (electric strikes and electrified hardware) must be 24-volt devices. Twelve volt locking devices are not acceptable.
7. Request-to-Exit: Bosch DS150i Series or approved equal.
8. Door Contacts: Sentrol or approved equal.
9. Overhead Door Contacts: Sentrol or approved equal.
10. Access Power Controllers: Supply: Altronix Maxim 33 or approved equal.
11. Panic Button: USP HUB2 Series or approved equal.
12. Proximity Cards: HID Corporate 1000. Contractor shall verify requirements with Texas Tech Police Department.
13. Motion Sensor: Sentrol or approved equal.
14. Glass break sensors may be used at locations where there is a window(s) that if broken could allow access to a secured area.
15. No substitutions. All Devices shall be compatible with existing system.
16. Other technologies identified as needed. Subject to approval by the Texas Tech Police Department.

### Hardware Requirements

1. Controllers:
  - a. Software House iSTAR Edge which supports two (2) readers. (if required)

Division 28 - Electronic Safety & Security

- b. Software House iSTAR Ultra which supports thirty-two (32) readers. (if required)
  - c. Each iSTAR panel shall have an Ethernet network connection.
  - d. Contractor shall provide installation, connection, 120V emergency power or 12 volt UPS battery to provide minimum 12 hours of stand-by power, patch cords, power supply conduit and wire.
2. Input Modules:
- a. Software House C#I8-CSI (if required).
  - b. Software House enclosure #RM-DCM-CAN (If required).
  - c. Contractor shall provide installation, input modules, enclosure, 120V emergency power, patch cables for connection, power supplies, conduit and wire.
3. Output Modules:
- a. Software House #R8 output module. (if required)
  - b. Software House enclosure #RM-DCM-CAN. (if required)
  - c. Contractor shall provide installation, connection, enclosure, modules, patch cords, power supply, 120V power, conduit and wire.
4. Card Reader:
- a. Proximity Card Reader:
    - i. HID (Specific model dependent upon application).
    - ii. Software House # RM2-LCD with keypad.
  - b. Refer to plans for exact number and location card readers.
  - c. Proximity card reader shall be weatherproof exterior applications.
  - d. Provide proximity card reader for elevators. Coordinate requirement with elevator contractor.
  - e. Contractor shall provide installation, connection, back box, power supply, 120V emergency power, communication cable, programming and conduit.
  - f. Biometric readers may be used in areas where top level security access is required. These areas may include but are not limited to cash vaults and/or areas where drugs, narcotics or hazardous chemicals are stored.
5. Proximity Card:
- a. HID Corporate1000 card (Standard University ID cards will work with CCure9000)
6. Electric Door Strikes:
- a. HES 1006 (Sargent mortise locksets) or HES 9500/9600/9700 (Sargent rimmed exit devices).



Division 28 - Electronic Safety & Security

- b. Locking devices must be 24-volt devices. 12-volt locking devices will not be accepted.
  - c. Electric door strikes for all exterior doors will be programmed to fail-secure in the event of building power loss.
7. Electrified Door Hardware
- a. Locking devices must be 24-volt devices. Twelve volt locking devices will not be accepted.
  - b. Coordinate door strike with door frames.
  - c. Electrified door hardware for all exterior doors will be programmed to fail-secure in the event of building power loss.
8. Removable Mullions
- a. Contractor shall provide a quick disconnect and pigtail in the top of the mullion.
  - b. Contractor shall provide quick disconnect, power supply 120V emergency power, relays, wiring and conduit.
9. Request-to-Exit (REX) Devices:
- a. Provide REX: PIR or approved equal
  - b. Coordinate location of device with door and wall conditions.
  - c. Refer to plans for exact number and locations of REX's.
  - d. Provide installation connection power supply, 120V emergency power, relays, backboxes, wiring and conduit.
10. Door Position Switches and Contacts:
- a. Provide Software House/Tyco door contacts.
  - b. Contacts shall be hidden in the top of the door frame. Coordinate requirement with door manufacturer. Contacts behind the hinges are not acceptable.
  - c. Provide Software House/Tyco overhead contacts.
  - d. Contractor shall provide installation, connection, control wiring and power supply.
11. Access Control Power Controller/Supply:
- a. Provide one (1) dedicated circuit power supply for each I-star controller.
  - b. Refer to plan for location of power supply.
  - c. Contractor shall provide installation, connection, patch cords, 120V emergency power, wiring and conduit.
12. Panic Alarm
- a. Provide at least one (1) panic button by USP HUB2 Series or approved equal.
  - b. Coordinate location of button with owner.
  - c. Contractor shall provide installation, control wiring and conduit

### 13. Motion Sensor

- a. Provide Sentrol / 6E PIR # AP100PI or approved equal.
- b. Sensor shall be PIR Type.
- c. Sensor shall be adjustable to accommodate different size rooms.
- d. Contractor shall provide installation connection, communication cable as required.

Each card access-controlled door may require four devices:

1. Proximity Card Reader (CR)
2. Door Position Switch (DPS)
3. Electrified hardware or manual crash bar hardware with electronic strike (dog down function prohibited)
4. Request to Exit (REX)

Controlled doors not requiring card access shall include three devices:

1. Door Position Switch (DPS)
2. Manual crash bar door hardware (dog down function prohibited)
3. Request to Exit (REX)

These doors should be set up in the system as a “door” and not an “output and two inputs. All monitored exterior building perimeter access control points are required to include a Request to Exit device.

Install system in accordance with manufacturer's instructions.

Install wiring for detection and signal circuit conductors in conduit back to the building cable tray. An Ethernet network port shall be incorporated into the cost of the project and arranged through TTU or HSC Network services and coordinated with TTPD.

Coordinate connection requirements with Texas Tech Police Department. Texas Tech Police shall have capability of monitoring security access and video at Police Department site. Test in accordance with Tyco security standards. The contracted security system provider shall maintain duplicate system parts inventory and make available within 50 miles on installation site.

## **28 23 00 Video Surveillance**

The video surveillance camera system will be a complete local system at the new building. Contractor shall provide software to monitor at different location via an IP connection. Contractor shall coordinate remote operation of camera monitoring system with Texas Tech Police Department.

1. Network Video Recorder (NVR)
  - a. American Dynamics NVR approved equal to meet Owner and TTPD specifications.
    - i. Provide RAID storage system.
    - ii. NVR shall be sized and capable of capturing and storing minimum of thirty days of video captured images without archiving. Coordinate video storage requirements with Texas Tech Police Department. NVR hard drive storage calculation must include minimum 50% expansion storage capacity.
    - iii. NVR camera channels should be loaded with more than 50% of the camera channels.
  - b. Provide 17" monitor or approved equal.
  - c. Provide uninterruptable power supply for NVR/Computer system. UPS shall provide 20 minutes of continued operation in the event of an AC power failure.
  - d. Provide 2 Ethernet network ports for system (coordinated with TTPD and TTUNet or HSC Network Services).
    - i. Private camera subnet
    - ii. Public NVR port
  - e. Provide manufacture equipment rack if requested by owner.
  - f. Contractor shall provide installation, connection, software, programming patch cord, and conduit.
2. Cameras:
  - a. At a minimum, all video surveillance cameras shall be an IP camera with minimum 2MP native resolution. Higher resolution cameras are preferred.
    - i. Interior Cameras:
      1. American Dynamics Illustra Pro (IP Mini-Dome, 5MP), as determined by TTPD.
      2. American Dynamics Illustra Pro (3MP and 4K Mini-dome), as determined by TTPD.
      3. American Dynamics Illustra Flex (8MP Mini-Dome), as determined by TTPD.

4. American Dynamics Illustra Pro (8MP, 30x PTZ), as determined by TTPD.
  5. Arecont Omni G3 (20MP – 5MP x 4 cams), as determined by TTPD.
  6. ***Fisheye cameras are not approved and should not be specified.***
- ii. Exterior Cameras:
1. Arecont Omni G3 (20MP), as determined by TTPD.
  2. American Dynamics Illustra Pro (8MP, 30x PTZ), or as determined by TTPD.
  3. American Dynamics Illustra Flex (8MP Mini-Dome), as determined by TTPD.
- b. Cameras may utilize Power over Ethernet (POE) for camera power. In specific cases, POE injectors may be utilized.
- c. Refer to plans for exact number, locations and targeted fields of view for cameras.
- d. Contractor shall provide installation, connection, mounting plates, domes, cameras, power supply 120V power, and communication video cable, and conduit.
- e. Cameras should be wired to the closest TTU LAN or TTUHSC LAN Network switch for communication with the NVR.

### ***28 31 11 Digital Addressable Fire-Alarm System***

The system shall have a microprocessor based intelligent addressable fire alarm system with printer and voice evacuation. The fire alarm system and design shall be Fire Control Instruments E-3 Series or approved equal.

***The TTU Fire Marshal's Office is the Authority Having Jurisdiction for the fire alarm system.***

#### **System Description**

1. The system shall have the capabilities of sounding a digitally pre-recorded voice/audible fire evacuation message in English and Spanish and a digital severe weather message that can be activated through a separate pull station or button labeled for severe weather. No strobes are required for weather alerts.
2. The system shall have the capabilities of flashing the strobes after the system has been silenced and until system reset has occurred.
3. The fire alarm system shall have the capabilities of shutting down all heating and air handling units during general alarm.

Division 28 - Electronic Safety & Security

4. The fire alarm system shall monitor all ancillary life safety systems.
5. All corridors, stairwell and any other fire door that would tend to be propped open will be equipped with magnetic door hold open devices that will release on the activation of the fire alarm system or loss of power.
6. All fire alarm systems shall be tied into and monitored at Central Heating and Cooling Plant 1 (CHACP 1) emergency maintenance facility and Texas Tech Police Department through the U.L. Listed fiber loop system (preferred method) or Ethernet. The head-end monitoring equipment is Fire Control Instruments, and all new equipment must be compatible and capable of interfacing with the current equipment. The fire alarm contractor is responsible for the purchase and installation of all the equipment that is required to make the interface.
7. Fire alarm testing will be done only after the elevator has been certified by a State QEI Inspector.
8. Fire alarm duct detectors should be programmed for supervisory condition due to the dusty conditions of this area.
9. IDC and SLC circuits shall be allowed to be class "B" circuits, NAC circuits shall be allowed to be class "B" circuits unless a High-Rise classification requires Class A circuit configuration.
10. Install plastic stopper covers for each manual pull station and weather alert button unless directed otherwise by the Owner.
11. Exit signs shall not be interfaced to the fire alarm system to flash on alarm.
12. Strobes shall be located relevant to exit locations to draw attention to exit doors.

The system shall include, but not be limited to the following components:

1. Master system CPU including all fire detection, voice/audio and visual evacuation alarm control modules, and supervised power amplifiers with the required back up modules.
2. Circuit interface panels including all modules.
3. Power supplies, batteries and battery chargers.
4. Pre-amplifiers, amplifiers, tone generators, and master microphone.
5. Equipment enclosures.
6. Intelligent addressable manual pull stations, heat detectors, analog smoke detectors, alarm monitoring modules, and supervised control modules.
7. Beam smoke detection system.
8. Annunciator panel and printer.
9. Voice/Audible and visual evacuation signals.
10. Color graphic displays and historical archiving.

Division 28 - Electronic Safety & Security

11. Software and firmware as required to provide a complete functioning system.
12. Wiring and raceway.
13. Installation, testing and certification and training.
14. Interface with air handling units and stairwell pressurization system.
15. Interface with Clean Agent Suppression System serving computer rooms.
16. Remote annunciator panel.

Before commencing work, submit data showing the Contractor has successfully installed fire alarm systems of the same type and design as specified, or that they have a firm contractual agreement with a subcontractor having the required manufacturers' training and experience.

The Contractor shall include the names and locations of at least two installations where the Contractor, or the subcontractor above, has installed such systems. Specify the type and design for each system and furnish documentation that the system has performed satisfactorily for the preceding 18 months.

Provide the services of a representative or technician from the manufacturer of the system, experienced in the installation and operation of the type of system provided. The representative shall be licensed in the State of Texas. The technician shall supervise installation, software documentation, adjustment, preliminary testing, final testing and certification of the system. The technician shall provide the required instruction to the Owner's personnel in the system operation, maintenance and programming.

The system shall be a complete, electrically supervised multiplex style fire detection and voice evacuation system with intelligent analog alarm initiation, to be device addressable and annunciated as described and shown on the Drawings. Fire Control Instruments is the acceptable manufacture. Other manufacturers meeting the requirements of this specification for design, function and performance will be considered upon submittal of manufacturer's data to the Texas Tech University Fire Marshal's Office.

The system shall support intelligent analog smoke detection, manual station, water flow, supervisory, security, and status monitoring devices. Fire alarm, supervisory, trouble, security and status shall each be treated as a separate level of alarm, each with its own level of priority. The system shall also support amplifiers, voice/visual circuits, and stairwell pressurization fans and dampers.

The system shall be programmed in the field via a laptop computer. All programmed information shall

Division 28 - Electronic Safety & Security

be stored in nonvolatile memory after loading into the control panel. No special programming terminal or prom burning shall be required and the system shall continue in service during reprogramming.

Systems requiring online terminal programming or not capable of mass reading of panel software for offsite documentation or editing will not be considered acceptable. Disabling of devices must be able to be accomplished by push buttons located on the front of the main control panel and must be capable of doing this by device type, floor, zone etc. This disabling feature shall also include flow and tamper switches, etc., that may require maintenance. In the event of an alarm or power disruption this action of disabling shall remain intact after the reset function has been activated. The alarm panel shall alert the technician that devices have been disabled and give the option to keep them disabled. This will prevent the inadvertent clearing of these disabled devices and cause false alarms due to repairs or work in progress.

Each intelligent addressable device on the system shall be displayed at the fire alarm control panel by a unique alpha numeric label identifying its location.

Activation of any alarm verified smoke detector in a single elevator lobby or an elevator equipment room shall, cause the recall of the elevators to the terminal floor and the lockout of controls. In the event of recall initiation by a detector in the first-floor lobby, the recall shall be to the alternate floor. Activation of any heat detector in the elevator machine room, elevator pit, or elevator shaft shall shunt trip the circuit breaker serving the associated elevators.

Unless otherwise allowed by the TTU Fire Marshall, all wiring shall be run in metal conduit throughout. Paint all junction box covers red.

Perform work in accordance with the requirements of NEC, NFPA 70, NFPA 72, TTU Fire Marshall's Office, and Factory Mutual recommendations.

Coordinate with Telecommunications installer and Mechanical subcontractors.

Complete and submit to the Owner a Certificate of Compliance in accordance with NFPA 72.

Fire pumps shall report a "general fire alarm" upon activation.

A written acceptance test procedure (ATP) for testing the fire alarm system components and installation

Division 28 - Electronic Safety & Security

will be prepared by the Acceptance Inspector in accordance with NFPA 72, and the Owner's requirements. The Contractor shall be responsible for the performance of the ATP, demonstrating the function of the system and verifying the correct operation of all system components, circuits, and programming.

The Contractor shall warrant the entire system against mechanical and electrical defects for a period of 18 months. This period shall begin upon completed certification and test of the system. During this warranty period the contractor shall respond to a trouble call within 2 hours for problem determination, and resolution to the problem within 24 hours.

Construction documents for fire alarm systems shall be submitted for review and approval prior to system installation. Construction documents shall include, but not be limited to the following:

1. A floor plan which indicates the use of all rooms.
2. Locations of alarm-initiating and notification appliances.
3. Alarm control and trouble signaling equipment.
4. Annunciation.
5. Power connection.
6. Battery calculations.
7. Conductor type and sizes.
8. Voltage drop calculations.
9. Manufacturers, model numbers and listing information for equipment, devices and materials.
10. Details of ceiling height and construction.
11. The interface of fire safety control functions.
12. Systems and their components shall be listed and approved for the purpose for which they are installed.