UCONN
UNIVERSITY OF CONNECTICUT

Physical Security Systems Design Standards

Division of University Safety, Facilities Operations and University Planning, Design and Construction
Established: December 2021

1. PURPOSE

The purpose of this document is to provide guidelines for the design and installation requirements of security systems at the University of Connecticut (University). This document applies to all security installations that will be connected to the primary campus system and integrated into the Emergency Communications Center (ECC) in Storrs. The University is comprised of a main campus in Storrs, UConn Health, UConn Law, four regional campuses and leased properties throughout the State of Connecticut.

2. CAMPUS SECURITY SYSTEM OVERVIEW

A. The University generally utilizes the Genetec Security Center unified security platform as the access control, intrusion detection and video management system for all campuses (exception UConn Health). All access control and video management design solutions shall be 100% compatible with the Genetec Enterprise Security Center unified security platform.

B. The campus security system provides the capability to control access, transmit alarm signals to the ECC, and provide video viewing capabilities to the DUS personnel.

C. ECC has the primary purpose of responding to emergency calls and dispatching DUS responders as needed. As part of the ECC standard operations, video cameras are not actively monitored. Their purpose is to provide dispatchers with assessment capabilities related to specific events.

D. In conjunction with the Design Team, DUS shall conduct a security assessment for all renovations and new construction projects. This assessment ensures security needs have been fully identified to support public safety procedures for responding to events at their location.

3. DEFINITIONS

A. ACS – Access Control System
B. AEO – Acceptable exit only: Request to exit,
C. ALPR – License plate recognition
D. ASIS – American Society of Industrial Security
E. CPTED – Crime Prevention through Environmental Design
F. DUS - Division of University Safety
G. ECC - Emergency Communications Center (Storrs)
H. EEO – Emergency exit only:
I. FO - Facilities Operations
J. ITS – University's Information Technologies Services
K. POE – Power Over Ethernet
L. RDR – Card reader: proximity reader or mag & proximity reader,
M. REX – Request to exit
N. VMS – Video Monitoring System
O. Controlled – Any monitored opening that utilizes electronic locking

P. Design Standards – University Design Guidelines and Performance Standards
Q. Designer – Security Design Consultant
R. Integrator – Trade Security Contractor who self-performs installation of security and surveillance systems.
S. Monitored – Utilizes door contacts or request to exit devices.

4. GENERAL RESPONSIBILITIES

A. The University Representative in conjunction with the Division of DUS, ITS and FO shall be involved in the planning and design of all security system projects. The drawings shall specify which doors will have electronic monitoring, locks, locations of surveillance cameras and will identify all other security requirements.

B. The Security Design Consultant (Designer) is responsible to design a fully functional system including, specifying compatible hardware devices, equipment cabinets, controllers, software and integrate electronic door hardware and other components that makeup and support the systems. The Designer shall possess the certifications, experience and is responsible for the following:

1) Holding at a minimum, ASIS Physical Security Professional (PSP) certification, ASIS Certified Protection Professional (CPP) certification is preferred.

2) Highly experienced in self producing security drawings and specifications for large scale projects, which will depict camera view area and horizontal projection of the view area. The Designer shall be independent from any manufacturer and shall not delegate the design and specifications to any sub-consultants who are directly or indirectly a representative of a manufacturer's product, nor have a vested interest in specifying a manufacturer's product.

3) The design and functionality of the security system shall include:
    a. Configuration of embedded systems such as ACS, ALPR, and VMS.
    b. Live event monitoring.
    c. Live video monitoring and playback of archived video.
    d. Alarm management.
    e. Reporting, including creating custom report templates and incident reports.
    f. Federation for global monitoring, reporting, and alarm management of multiple remote and independent ACS and/or VMS systems spread across multiple facilities and geographic areas.
    g. Global cardholder management across multiple facilities and geographic areas each with their own independent ACS system.
    h. Microsoft Active Directory integration for synchronizing user accounts and ACS cardholder accounts.
    i. Intrusion device and panel integration (live monitoring, reporting, and arming/disarming).
    j. Intercom device integration for bi-directional communication.

k. Integration to third party systems and databases via plug-ins (access control, video analytics, point of sale, and more).
l. Dynamic graphical map viewing.
m. Asset management system integration.

4) By the end of Schematic Design, the Designer should have performed a complete analysis of existing video storage capacity to ensure any additional devices will not degrade system functionality.
    a. Confirm existing hard drive available storage capacity and calculate the required demand of a single camera at high resolution. Meet with the University Representative and ITS to review capacities.
    b. Meet with the University Representative in conjunction with DUS and FO to initially identify exterior locations of required security devices.
5) By no later than 50% design development, meet with the University Representative in conjunction with DUS and FO to determine final locations and number of required security devices for both interior and exterior security requirements.
    a. Identify any impact to existing storage capacities from the proposed number of cameras and ACS devices required in the project. The calculation must include the number of proposed cameras, resolution of each camera, the anticipated activity in each camera's scene with ninety (90) days of video retention.
    b. Present final analysis findings and recommendations to the University Representative in conjunction with ITS, DUS and FO to ensure sufficient capacity remains on the existing hard drive. If it is determined there is not sufficient storage capacity, upgrades to data storage shall be incorporated in the final design documents.
    c. Submit a draft copy of the security plans to the University Representative and ITS, FO and DUS for review and comment.
6) By no later than 100% design development, provide to the University Representative in conjunction with DUS and FO the review comments on security plans and specifications identified during the 50% design development review. Confirm with the University Representative in coordination with DUS the specified placement of security devices in elevation view with all other equipment, fixtures and accessories in close proximity to avoid conflicts in the field and ensure proper coordination has been achieved. Receive final acceptance (Notice to Proceed) of the security plans, prior to entering the construction documents phase.

7) Buildings shall be equipped with the minimum access control, alarm monitoring and video surveillance.
    a.
    b. All security designs must meet Building and Fire Codes.
    c. All hardware shall be located so as not to exceed maximum distance limitation of the Category 6 cable back to the control panels. Instances where there is no other option but to exceed maximum distances beyond what can be supported, such as outside poles, fiber optic cabling dedicated to a network switch shall be installed in a NEMA 4X rated control box mounted to the pole. Locations

with 110 power requirements shall take into consideration the need for step down transformers. Emergency power circuits are preferred. Poles and conduits shall be grounded.

d. Dedicated electrical circuit(s) shall be on the emergency or backup power system for security system and network switches on which security devices are connected.
e. All security system and network switches shall be co-located within an ITS telecommunications room within the facility and shall have ample dedicated wall space and dedicated electrical outlets specifically to support all security support equipment. Identify in elevations the telecommunications room, what equipment is to be mounted where, showing locations for fire alarm, electrical, data and other devices needing to be mounted on the walls. Wall space for security equipment shall be no smaller than a standard half sheet of plywood mounted at five feet centered.
f. All supporting work associated with back boxes and their size, adequate size conduit and its routing, appropriate cable type and power shall be fully coordinated in the design documents by the Designer. Ensure all data drops are located inaccessible and hidden from view to prevent unauthorized tampering with connection.
g. Coordination is not limited to applicable sections of Division 08, Openings but must be coordinated with all surrounding work:
    i. Coordinate access control requirements with doors, door frames and hardware schedules.
    ii. Coordinate with the University Representative on requirements and interfaces with access control hardware.
    iii. Camera location must allow for 84-inch minimum clear space below the camera and their mountings.

h. As a general rule, all building exterior perimeter doors and service areas shall have video surveillance on them. Such surveillance shall be recorded and reported back to the ECC located at the DUS. Inside building entrances, a designated sign that notifies the public that the building is under surveillance shall be posted "This Building is being Monitored". Use of cameras shall be limited to public areas. Refer to Volume II, Section 11 of the Design Standards on interior signs.

8) Incorporate additional design and Integrator requirements that are referred to throughout this document. Ensure the detailed list of required qualifications of the Integrator and the certified training of their own employed staff is included in the specification as a condition to be qualified to oversee and perform the work.
    a. Designer is not to review any submittals on security and surveillance systems equipment, hardware and other products under the responsibility of the Integrator, prior to receipt and review of the Integrator's qualification requirements, list of employees who will be performing the work and their respective current Genetec training certifications ss defined in Section 4C of this document.

9) Include within specifications a level of quality performance expected from the Integrator:
    a. FCC Part 15, Part 68
    b. UL 294, 1076
    c. NEC compliance
    d. NEMA
    e. Technicians and programmers who hold current certifications as outlined within this Appendix
    f. Test Plan
    g. All others as required

C. The Integrator is the party that is directly responsible for the installation and programming of a fully functional integrated access control, alarm monitoring and video surveillance systems, including but is not limited to software licensing, programming, integration of electronic door hardware, systems devices, and equipment, not limited to controllers, mounting brackets, power supplies, equipment cabinets and other components of the system hardware. Coordination with both DUS and FO on programming features and functions is required.

The Designer shall include in their specifications the following requirements of the Integrator:

1) The Integrator shall be a legal business entity registered within the State of Connecticut (not a DBA) who will be self-performing the installation and programming of a fully functional integrated access control, alarm monitoring and video surveillance systems, and whom at a minimum:
    a. be a Genetec approved Licensed Integrator
    b. has their office located within the New England Region
    c. self-perform the oversight, coordination, installation, programming, and commissioning of the various security systems with the Genetec platform and licenses.
    d. shall hold a current Elite Status recognition from Genetec
    e. employs and maintains in-house highly experienced technicians and programmers who:
        i. reside within the New England Region
        ii. hold current training certifications thru Genetec as follows:
            1. Security Center 5.x Enterprise (Advanced) Technical Certification – SC-ETC-001 (or its equivalent based on the most current training certification requirement)
                a. Only having certifications in Security Center 5.x Omnicast (Video) Technical Certification and/or Security Center 5.x Synergis (Access Control) Technical Certification does not meet the minimum requirements.

2. Security Center 5.x AutoVu fixed technical certification - SC-AFC-001 (or its equivalent based on the most current training certification requirement)
3. Security Center 5.x AutoVu Mobile Essentials with Parking technical certification – SC-AMP-001 (or its equivalent based on the most current training certification requirement)
4. Advanced Omnicast Troubleshooting certification (or its equivalent based on the most current training certification requirement)
5. Advanced Synergis Troubleshooting certification (or its equivalent based on the most current training certification requirement)
6. Genetec Security Center System Hardening (or its equivalent based on the most current training certification requirement)
7. Genetec Security Center System Design (or its equivalent based on the most current training certification requirement)

f. assigns only those employee technicians and programmers to the University's project (on-site or remotely who live within the New England Region) who hold current training certifications on the systems platform they are performing work under the project.

g. does not subcontract to other legal business entities for Genetec certified technicians or programmers of systems equipment.

2) The Integrator shall further be responsible for the following:

a. to respond and have the assigned certified technicians/programmers be present on the project site within 2 hours from initial contact for any issues raised by the University during the commissioning and warranty period.
b. ensure systems hardware and software is fully integrated into the existing (when applicable) or new system to present a single, seamless operation system.
c. coordinate their work with applicable sections of Division 08, Openings, including but not limited to:
    i. access control requirements with door, frame, and door hardware schedules.
    ii. on requirements and interfaces with access control hardware with the University.
    iii. all conduit, raceways and box systems requirements for the physical security system components to ensure location requirements are being met.
    iv. mounting and installation of cameras to ensure 84-inch minimum clear space below cameras and their mountings is achieved.
    v. submit RFI's timely notifying the Designer of potential impacts to new door hardware and security devices pending installations by new or

existing door or hollow metal frame locations and provide proactive corrective measures to complete the installation.

d. submitting a minimum of 15 days prior to proposed test date, a test plan that defines the tests required to ensure the system meets technical, operational and performance specifications for review.
e. applies for and hold applicable work permits prior to starting the work.
f. performs the following services in addition to any others identified within the contract documents:
    i. Engineered Shop Drawings
    ii. Wiring and installation diagrams
    iii. Submittals
    iv. Coordination
    v. System installation
    vi. System integration
    vii. Training University staff on the systems installed
    viii. Test Plans and Start up testing
    ix. Commissioning
    x. Close out electronic as-built documentation
    xi. Warranty
g. follows the University's standard naming convention for partitions, areas, doors, elevators and the like when programming.
h. coordinate activation of systems on the University voice and data networks with ITS.
i. warranty the security system and its components for one (1) year from the date of documented acceptance by the University (substantial completion issued by the Designer which notes exceptions to surveillance and security controls does not start the warranty period). Failed equipment shall be replaced by the Integrator at no cost to the University.
    i. Security System components include all hardware, firmware, devices, and other materials and labor.
    ii. University may perform initial troubleshooting; however, such trouble shooting by the University shall not void any warrantees or relieve the Integrator for costs associated with replacement of failed equipment or performing escalated problem for a period of one year from the established date of trouble notification.

5. SYSTEMS AND CONTROLS DETAILS

A. ELECTRONIC SECURITY AND ACCESS CONTROL

Purpose: Electronic security and access control system is designed to monitor and restrict access to specified areas, and to report on the activity and violations of restricted access into those areas.

1) All hardware must be home run to the ACS panel. No hardware shall be physically connected to perform a task outside of the ACS panel but should be programmatically connected unless otherwise approved by DUS in conjunction with FO.

2) The use of proximity, magnetic stripe, and smart technology photo ID badges to provide access through card reader-controlled doors are currently being used
3) System administration for card holder modifications, door schedules and access rules is managed by FO. DUS personnel (both Police and Fire) shall have access to all areas.
4) Standard naming convention for partitions, areas, doors, elevators, and the like shall be obtained from FO.
5) Openings with multiple doors shall have a single reader controlling a single door.
6) All openings with a reader shall have a keyed override. Coordinate lockset with FO.
7) Door operator actuator shall only be active when door is electronically unlocked.
8) No magnetic locks are permitted on exterior doors.
9) No wireless, POE or WiFi locks are permitted.
10) All ITS, Mechanical and Electrical spaces shall be controlled by the access control system.

B. INTRUSION DETECTION SYSTEM

Intrusion detection is designed to provide alarm monitoring of designated areas to the ECC through the Genetec software platform. The option to include Intrusion alarms will be determined by DUS through the security assessment. Not all buildings will be required to have intrusion detection.

1) The intrusion detection system includes a keypad to allow arming/disarming of the system.
2) Alarm panels communicate using the University's network infrastructure.
3) Control Panels: Standard alarm panel is Bosch B series GV2, GV3, GV4
4) System Integration: The security software platform integrated feature will be utilized to automatically call-up cameras at Emergency Communications to allow visual assessments of intrusion alarms.
5) Environmental alarms (high heat, water leaks and the like) report to FO. Interior door prop alarms report to the individual building's building manager.
6) Roof hatches are to be locked at all times; access is controlled by electronic access control system. Forced entry alarms are to report to ECC.

C. VIDEO SURVEILLANCE SYSTEM

Video surveillance is designed to provide authorized staff with the means to monitor, record, or review activities through the Genetec software platform.

1) Video surveillance equipment shall be compatible with Genetec Security Desk. Only equipment and devices identified by Genetec as compatible shall be used.
2) Video surveillance cameras shall have sufficient resolution and be located such that recognizable images are captured by the Genetec Security Center system.
3) All exterior doors shall have surveillance cameras installed.
4) Surveillance cameras are to be fixed unless otherwise specified.
5) No microphones are to be activated under any circumstance.
6) All exterior doors shall have signage stating "Cameras In Use" posted.
7) Surveillance cameras shall be hard-wired, Ethernet connected devices utilizing TCP/IP communication protocol.

8) Wiring for surveillance cameras is to follow the Design Standards, Appendix IV for detailed information. Wiring shall not exceed 90 meters from nearest distribution frame. Lengths exceeding 90 meters shall require fiber optic cable. Authorization to view live video feeds within a specific partition require approval by the Chief of Police. No users are to be created by the Integrator.

6. PRODUCTS

A. ACCESS CONTROL

1) Only access control, intrusion and surveillance camera components manufactured by Genetec, Mercury, HID, Bosch, DSC and others supported by the Genetec system will be acceptable.
   a. Existing Residence Halls are the exception, such access control system is Millenium and is managed by Residential Life.
2) All exterior systems hardware must be exterior rated and installed per manufacturer specifications and instructions for exterior installation.

B. CARD READER:

1) Access control will support a variety of card readers that shall encompass a wide functional range.
2) Supported readers:
   b. Mullion: HID 20TKS-00-0010E-UCONN (means preprogramming of mod code) Description: Signo 20 Mullion, Black/Silver or DUS approved equal
   c. Regular Reader HID 40TKS-00-0010E2 (UCONN preprogramming of mod code) Description: Signo 40 Single Gang, Black/Silver or DUS approved equal
   d. PIN: 40KTKS-00-0010E2-UCONN Description Signo 40 Keypad, Black/Silver or DUS approved equal
   e. Magnetic Stripe: HID
3) Readers are black in color and shall be weatherproof.
4) Cards
   a. UConn supplies and programs

C. DOORS AND DOOR HARDWARE

1) All electronic access control door hardware shall be fail secure unless otherwise required to meet building, fire, AHJ or other code.
2) All doors shall require the use of request to exit and door contacts.
3) Doors that require power shall use power transfer devices. Door loops shall not be accepted.

D. DOOR STRIKES

1) Must be fail secure
2) Electronic strike can be flush or surface mounted
3) Reference door hardware section within Volume II of the Design Standards for acceptable manufacturers and series.
4) Acceptable manufacturers for door strikes: Hess, Adams Rite, Von Duprin, or Folger Adams.

E. SYSTEM INTELLIGENT

1) **Access Control Functionality** not limited to:
   a. Controller (Unit) management, door management, elevator management, and area management
   b. Cardholder and cardholder group management, credential management, and access rule management
   c. Badge printing and template creation.
   d. Visitor Management.
   e. People counting, area presence tracking, and mustering
   f. Offer a framework for third party hardware integration such as card and signature scanner
   g. System Intelligent Controller shall operate and control access to multiple doors as a total standalone unit with full distributed database and no dependency on the central system.
   h. Multiple reader access control panel shall support Wiegand, magnetic stripe, and proximity credentials.

2) **Synergis Cloud Link Controller (by Genetec) Basis of Design – Systems Controller of the whole system (controls whole building).**
   a. Control module shall contain 2GB of DDR3 RAM, 16GB on-board SSD, two Gigabit Ethernet ports and four RS-485 communication ports.
   b. Control module shall be connected to the LAN and receive and transmit data to/from Genetec Security Desk.

3) **Intelligent Controller Basis of Design**
   a. Mercury Intelligent Controller shall communicate between the System Intelligent Controller and the 2 Reader Interface Module.
   b. The device shall support Wiegand, magnetic stripe, and proximity credentials.
   c. Controller shall be connected to the LAN and receive and transmit data to/from Genetec Security Desk.
   d. Mercury EP1502 module shall contain 16GB of DDR3 RAM, 2 reader ports, eight supervised inputs and four Form C output relays. The controller shall provide capacity for 240,000 credentials and 50,000 transactions.
   e. Controller shall communicate with reader interface modules via RS-485 communication bus.

4) **Reader Interface Module – Basis of Design**
   a. Mercury interface module shall be the microprocessor-based interface device between the card readers and the access control system. Module shall be compatible with card readers and access control system specified.
   b. Module shall be mounted in metal enclosure with ample space to accommodate equipment necessary for the number of readers specified plus 20% growth.
   c. Mercury MR52 module shall contain 2 reader ports, eight general purpose inputs and six Form C output relays.

d. Controller shall communicate with reader interface modules via RS-485 communication bus.

5) **Field Hardware Power Supplies**
   a. Auxiliary power supplies for doors or other field devices that require power outside of the access control system shall be located as close to the door or field device they are providing power to as possible. Power supplies shall be installed no more than 20 feet from the device they are providing power for.
   b. Provide low voltage power supply units associated with Local Interface Units and Door Control Panels, and as required to provide 12 and 24-volt regulated, filtered D.C. power for locking controls, D.C. locks, signal devices, and readers. Output power shall be 24-volt D.C. with ampere rating not less than 150% of load imposed on power supply under most severe conditions of load. D.C. output shall be fused. Output voltage shall be regulated within plus or minus 5% from no load to full load. Power supply shall be UL listed.
   c. Provide low voltage power supply units as required to provide 5-volt regulated, filtered D.C. power for magnetic stripe card readers. Output power shall be 5-volt D.C. with ampere rating not less than 150% of load imposed on power supply under most severe conditions of load. D.C. output shall be fused. Output voltage shall be regulated within plus or minus 5% from no load to full load. Power supply shall be UL listed.
   d. Battery back-up required inside each panel. Battery should be sized for a minimum of one hour of constant operation.

6) **Door Contacts**
   a. Door contacts shall be recessed mounted. ¾" door contacts are required for all steel and metal doors.
      i. Sentrol 1078 series or DUS approved equal
   b. Where surface mount contacts are required, the contacts shall be provided with a supervision loop and shall have flexible armored cable with total encapsulation to protect against moisture.
      i. Sentrol 2700 series or DUS approved equal
      ii. Sentrol 1078 series or DUS approved equal for sliding doors
   c. Overhead door contacts shall be provided with armored cable and be surface mounted. The floor mount units shall be constructed with a low-profile heavy cast aluminum housing. The contact assembly shall be fully encased in polyurethane potting material to prevent damage due to moisture or humidity. A wide operation gap distance of up to three (3) inches shall be required to prevent false alarms caused by door movement or damaged and loose-fitting doors.
      i. Sentrol 2200 series or DUS approved equal
   d. Door contacts shall have anodized aluminum finish with stainless steel flexible cable.
   e. Door contacts shall be UL Listed

7) **Request to Exit (REX) Devices**
   a. Door hardware shall provide free egress

b. Request to Exit devices shall be used to shunt door contact alarm only and when applicable shall not unlock the door hardware
c. Motion REX (PIR) devices shall have a wide-angle, long-range lens to detect motion of personnel exiting through the door. Coordinate exact field mounting location to provide best operation of PIR type REX device.
d. REX PIR device shall operation at 9.0 to 16.0 VDC and have Form C output contacts rated at minimum 24 VDC / 0.5 amps
    i. Bosch DS series or DUS approved equal
e. When REX is provided in door hardware, REX signal must be sent prior to door physically unlocking. REX signal should be sent on initial operation of level handle on panic bar.
    i. Bosch DS150i, DS160 or DUS approved equal

8) **Motion Detection Devices**
   a. Shall be Tri-tech motion detectors or DUS approved equal
   b. Shall use these technologies:
      i. Passive infrared
      ii. Microwave
      iii. Digital signal processing

9) **Enclosures (Panel/Canister)**
   a. Physical panel box type shall be equal to Life Safety FlexPower MClass Integrated Mercury Power system or Altronix Trove2m series
   b. Tamper switches must be installed on all panels and enclosures
   c. A standard key must be used on all panels and enclosures
   d. Battery back-up required inside each panel. Battery should be sized of one hour of constant operation.

10) **Low Voltage Cabling for Security Systems**
   a. Card reader connection cables shall be of a type specified by the access control system manufacturer. Cable must meet minimum NEC requirements for Class 2 wiring.
   b. Power wiring for electrified door hardware shall not be smaller than # 22 THWN or XHHW
   c. All wiring systems shall use stranded copper conductors. Terminations can be made to crimp type screw lug
   d. All cabling will be continuous from control equipment to door hardware. No splicing is permitted
   e. Conductors shall be color coded so each conductor for individual lock set is a distinct color
   f. All conductors within junction boxes, pull boxes, and equipment cabinets shall be grouped and laced with nylon tie straps with identification tab for individual lock sets
   g. All cabling is to be plenum rated

h. Ethernet cabling related to access control system shall be white rated CAT6. Refer to Appendix IV to the University's Design Guidelines and Performance Standards for information on wiring.
i. Ethernet cabling related to video surveillance shall be purple rated CAT6. Refer to Appendix IV to the University's Design Guidelines and Performance Standards.

11) **Transient Voltage Surge Protection**

a. Protect all equipment against surges induced on all control, video and power cables. All copper cables and conductors which serve as 120v power, control or video conductors shall have surge protection circuits where conductors enter or exit a building.
b. All power connections, including 24 VDC and 24 VAC power supplies and direct wired or plug-in 120 VAC power connections, for all systems and components specified herein, shall be equipped with surge suppression devices. Devices shall be bonded to the building grounding system in accordance with Article 250 of the National Electric Code.
c. Fuses shall not be used for surge protection
d. Surge protection devices shall meet the following:
    i. UL 497B
    ii. UL 1449 (must meet 330v suppression rating)
    iii. IEEE Category B impulse and ring waves tests
e. Acceptable manufacturers: Northern Technologies, Inc, or DUS approved equal. Products shall be warranted against defects for a period of not less than five (5) years.
f. Grounding
    i. Provide a dedicated, separate # 6 AWG copper conductor from the building grounding system to all security equipment rooms, security equipment cabinets and control rooms.
    ii. Connect all lightning protection devices and security equipment non-current carrying metal parts to grounding conductor.
    iii. Provide ground bus bar in each equipment room and control room with dedicated ground conductor to each cabinet, enclosure, pull/junction box and all equipment.

12) **Surveillance Cameras**

Cameras shall be an integrated IP-based field mounted camera. Basis of design for Cameras shall be on the needs of performance. As technology advances the basis of design will change therefore it is the Designer's responsibility to inform the University Representative for any new innovative devices that will provide enhanced surveillance for the application.

Components shall be protected from voltage surges originating external to equipment housing and entering through power, communication, signal, control, or sensing leads. Include coverage for voltage surges of external wiring of each conductor's entry connection to the manufacturer's requirements for the camera.

Conduits, connectors, hand holes and secured boxes shall be weather-proof.

The following guidance is provided in selecting cameras to be added to the existing campus security system. The specific type of camera function (fixed, PTZ, multisensory) is determined by the security assessment conducted by DUS prior to the Designer specifying.

a. ensure proposed cameras are compatible with the existing campus security system. The list of accepted devices can be found at: https://www.genetec.com/solutions/resources/supported-device-list
b. for each camera added to the system, a Genetec license and a failover license is required to enable operation of the device.
c. for situations where the camera needs optimum night –time camera viewing, include back focus and adjustments necessary to obtain such viewing.
d. microphones shall be disabled. No audio recording is permitted.
e. cameras shall be of manufacturer's official product line, designed for commercial/industrial 24/7/365 use.
f. cameras shall be based upon standard components and proven technology using open and published protocols such as Linux-based platform and must include a built-in web server.
g. installation of cameras shall be 84-inch- minimum clear space below cameras and their mountings. Designer shall include an elevation to show close coordination on locations of camera mounting, lighting mounting and other equipment and roof overhangs which may impact the maximum view area of the camera to ensure clear unobstructed view.
h. Camera Modes
    i. Surveillance Mode: provide good detail within the field of view and insures it is easy to differentiate between objects within a scene. Surveillance mode requires a camera selection that provides 20 pixels per foot at the target location.
    ii. Forensics Mode: provides more detail in the image than surveillance mode. Forensics mode requires a camera selectin that provides 40 pixels per foot at the target location.
i. Technical Requirements
    i. Camera Resolution
        1. SD Standard Definition – 800x600 pixel image
        2. HD High Definition – 1280x720 pixel image
        3. SHD – Super High Definition – 1920x1080 pixel image
        4. EHD – Extended High Definition – 2560x1920 pixel image
    ii. Image Control
        1. Camera shall incorporate Automatic and Manual White Balance and an electronic shutter operating in the range 1/6 and 1/35.500 second.
        2. Camera shall provide Wide Dynamic Range and backlight compensation with automatic and definable exposure zones.
    iii. MPEG-4

1. ISO/IEC 14496-10 AVC (H.264)

iv. Networking
   1. Camera shall support both fixed IP addresses and dynamically assigned IP addresses provide by a Dynamic Host Control Protocol server.
   2. IEEE 802.3af (Power over Ethernet 15w) PTZ cameras may require addition power
   3. IEEE 802.1x (Authentication)
   4. IPv4 (RFC 791) and IPv6 (RFC 8200) future growth
   5. QoS – DiffServ (RFC 2475)

v. Network Video
   1. ONVIF Profile S or ONVID Version 1.01 or higher as defined by the ONVIF organization

vi. Mechanical
   1. IEC 62262 Class IK10 (impact resistant)
   2. Thermostat, heater and fan inside the enclosure
   3. Fitted with a dehumidifying membrane.

vii. Cameras must be manufactured with an all-metal vandal resistant body and be both IP66 and NEMA 4X-rated.

viii. Cameras must support operation between -40° to +55° C (-40° to +131° F) and operate in a humidity range of 15-100% RH (condensing)

ix. Cameras must be equipped with a high-quality varifocal lens with automated iris functionality, providing remote zoom and focus functionality.

x. Transmission
   1. HTTP (Unicast)
   2. HTTPS (Unicast)
   3. RTP (Unicast & Multicast)
   4. RTP over RTSP (Unicast)
   5. RTP over RTSP over HTTP (Unicast)
   6. Camera shall support QoS to allow prioritization of traffic.

j. Recording Protocols
   i. Cameras must be capable of providing video streams at camera rated resolution at 30 frames per second using H.264 or Motion JPEG
   ii. Recording Modes
      1. Normal: 5 fps at SD. Quality setting medium-high
      2. Near Real-Time: 8 fps at high quality compression at camera native resolution
      3. Real Time: 15 fps at high quality compression
      4. Time Lapse: 2 fps at normal compression
      5. Alarm, Event, Motion Detection: 10 fps at high quality compression
      6. Critical Alarm: 15 fps at high quality compression
   iii. Recording Periods
      1. Normal business hours – to be determined for each building.
      2. Off business hours – to be determined for each building.

3. 24 hour continuous

iv. Typical Scenarios
    1. Common Areas (hallways, entryways, elevator landings, stairwells, perimeters)
        a. Normal mode for normal business hours as defined for each building.
        b. Programmed for time lapse mode during off business hours
        c. Alarm event of any kind will automatically change recording mode to Alarm, Event, Motion Detection
    2. Enclosed Low Use Rooms (Labs, Server rooms, Data Center)
        a. Time Lapse Mode 24 hours
        b. When motion is detected automatically change recording mode to Real Time.
        c. Alarm event of any kind will automatically change recording mode to Alarm, Event, Motion Detection
        d. Other protocols may be determined depending on the project scope.
    3. Large Capacity Gathering Spaces (sports facilities, auditoriums, lecture halls)
        a. Time Lapse Mode 24 hours
        b. When motion is detected automatically change recording mode to Real Time.
        c. Alarm event of any kind will automatically change recording mode to Alarm, Event, Motion Detection
    4. Roadways, Parking Lots and Intersections
        a. Real Time recording mode 24 hours continuously.
        b. Forensics mode (ability to clearly read license plates in target location)
    5. Pan Tilt Zoom Cameras
        a. Each PTZ camera shall be programmed with a home position (defined by DUS). When a camera is moved, camera shall return to home position after defined period of time.

k. Acceptable Cameras Models
    i. Indoor Fixed Dome Camera:
        1. Basis-of-Design Product: Subject to compliance with requirements, provide Axis P3247 LV or DUS approved equal.
        2. Description:
            a. Image Sensor: Progressive scan.
            b. Lens: Varifocal.
            c. Minimum Illumination: Color: 0.2 lux, F1.2, B/W: 0.04 lux, F1.2.
            d. Video Compression: H.264.
            e. Resolution: 2592x1944 (5 MP).
            f. Frame Rate: 12 fps.

g. Video Streaming: Multiple stream, H2.64 and MJPEG.
h. IP Routing: Multicast and Unicast.
i. Protocol: IPv4 and IPv6.
j. Security: Password protection, SSL encryption.
k. Alarm: External input and output.
l. Casing: PVC plastic.
m. Power: PoE.
n. Mounting: Recessed.
o. API: Open API

ii. Outdoor Fixed Video Surveillance Cameras:
1. Basis-of-Design Product: Subject to compliance with requirements, provide AXIS P3247 LVE or DUS approved equal.
2. Description:
a. Image Sensor: Progressive scan.
b. Lens: Varifocal.
c. Minimum Illumination: Color: 0.2 lux, F1.2, B/W: 0.04 lux, F1.2.
d. Video Compression: H.264.
e. Resolution: 2592x1944 (5 MP).
f. Frame Rate: 12 fps.
g. Video Streaming: Multiple stream, H2.64 and MJPEG.
h. IP Routing: Multicast and Unicast.
i. Protocol: IPv4 and IPv6.
j. Security: Password protection, SSL encryption.
k. Alarm: External input and output.
l. Casing: PVC plastic.
m. Power: PoE.
n. Mounting: Pole & Wall.
o. API: Open API

iii. Outdoor Multisensor Video Surveillance Cameras:
1. Basis-of-Design Product: Subject to compliance with requirements, provide AXIS P3717-PLE or approved equivalent. Where a PTZ is required with multisensory, Basis-of-Design Product: AXIS Q6000-E or equivalent. For deployment in parking lots and on corners of buildings.
2. Description:
a. Image Sensor: 360-degree multi-sensor
b. Lens: four varifocal camera heads
c. Minimum Illumination: Color: 0.3 lux.
d. Video Compression: H.264.
e. Resolution: 1920x1080 (8 MP).
f. Frame Rate: 12.5/15 fps.
g. Video Streaming: Multiple stream, H2.64 and MJPEG

7. EXECUTION

The Designer shall include in the specifications the following requirements of the Integrator:

A. Integrator shall submit required submittals on the qualification (certifications) of the technicians and programmers who will be performing work on the project for review and acceptance by the University Representative in conjunction with DUS and FO prior to the review of submittal submission on equipment, associated door and system's hardware and other products.
B. Submittals shall be acceptance by FO and DUS, prior to ordering and installing equipment.
C. The Integrator shall orchestrate a seamless integration of electronic door hardware and other components in support of the security system. Quality control shall include but is not limited to:
    1) Coordination of door hardware, location of card readers and cameras with their associated supporting devices and power/data requirements.
    2) Conducts a thorough testing point by point to ensure the information is transmitted and received at the monitoring stations is complete and accurate.
    3) Ensures camera call-ups are synchronized accurately with ECC.
    4) When applicable, installation of all hardware devices, mounting brackets, power supplies, equipment cabinets, controllers, and as shown and/or specified.
    5) Programs all requirements:
        a. Obtain the assigned IP addresses related to access control, intrusion and/or surveillance cameras from the University Representative prior to beginning any programming.
            i. University ITS provides IP addressing information and switch port connectivity.
            ii. DUS provides component names as defined in Genetec (ie – cameras, doors, alarms)
            iii. FO coordinates schedules, access rules and card holders
            iv. Provide the following data to obtain the IP addresses:
                1. MAC address
                2. room number in which the device will be installed
                3. data jack label, function of device (camera, alarm controller, or access controller).
        b. Put all devices created in the correct partition.
        c. All valid card numbers, time zones, relay pulse times, and alarm point shunt times shall be loaded into the controller's memory.
        d. Ensure the microphones to the video surveillance are off at all times.
        e. Follow identical naming convention established in existing system. Do not, under any circumstances change any entities or configurations from another integrator without direct permission from the University.
        f. Ensure all access control units and cameras have default factory passwords changed.
        g. Ensure new video units are load balanced on the storage infrastructure.

h. Create, configure, and test all Event to Actions that are required for alarm monitoring. Alarm description shall include Campus Name, Building Name, room number and description of alarm.
i. Coordinate with FO cardholders, schedules, and access rules are entered into the University's Genetec platform to ensure system is fully functional prior to test date.
j. Ensure all card holder groups University Safety, Fire Department and FO are provided access to all areas as soon as the card readers are activated.
k. Additional responsibilities as noted in Section 3.C of this document.

D. Pre-testing and Inspection before Substantial Completion
1) Integrator is responsible to:
a. Test all door hardware prior to inspections.
b. Submit a Test Plan that defines the tests required to ensure the system meets technical, operational and performance specifications 15 days prior to the proposed test date. DUS must approve the test plan before the start of any testing. The plan shall identify the capabilities and functions to be tested and include detailed instructions for the setup and execution of test and procedure for evaluation and documentation of results.
c. Verify operation of auto-iris lenses.
d. Set back-focus of fixed focal length lenses. At focus set to infinity, simulate nighttime lighting conditions by using a dark glass filter of a density that produces a clear image. Adjust until image is in focus with and without the filter.
e. Set back-focus of zoom lenses. At focus set to infinity, simulate nighttime lighting conditions by using a dark glass filter of a density that produces a clear image. Additionally, set zoom to full wide angle and aim camera at an object 50 to 75 feet (17 to 23 m) away. Adjust until image is in focus from full wide angle to full telephoto, with the filter in place.
f. Set and name all preset positions.
g. Set sensitivity of motion detection.
h. Connect and verify responses to alarms.
i. Verify operation of control-station equipment.
j. Each control panel shall have each connector labeled with the applicable door/room number and reader or camera number.
k. Train University operation and maintenance personnel in the use and maintenance of any systems installed, including but not limited to alarm keypads

E. Closeout
a. At the time of final inspection and before final payment will be released, the Integrator shall submit for review as part of their Operations and Maintenance Manuals for the Project, draft records and documents in accordance within Division One of the contract documents. Such documents are not limited to:
i. two (2) sets hard copy of complete data on equipment used in the project, manufacturer's technical product data including specifications, installation, operations and maintenance for each type of system equipment, warrantees and guarantees, etc.

ii. two (2) sets of hard copy record drawings which contain complete wiring and schematic diagrams and other details required to demonstrate that the system has been coordinated and will function properly. Drawings shall include floor plan layouts of device locations, components, vertical riser diagrams, equipment rack details, elevation drawings of equipment racks, sizes and types of all cables and conduits. For each IP networked device, provide jack label, patch panel port, MAC address.
iii. Record drawings shall include "as built" system interconnection diagrams with major components identified. Drawing will include MAC address, IP address, jack label, TR, patch panel termination port.
iv. all finalized programming settings including camera names, door names, alarm names, elevator names, alarm points, schedules etc.
v. In locations where alarm keypads are installed, security vendor must provide a completed document that provides which codes are in use and what access code is programmed. See appendix for document that is to be completed and submitted.
vi. Upon final submission of O&M's and As-builts, provide two (2) electronic files in AutoCAD and two (2) hard copy pdf formats.
vii. Punch list items will be corrected and verified prior to acceptance of the system.

END OF APPENDIX X