UCI CAMPUS SECURITY STANDARDS

1.1 PURPOSE

The purpose of this document is to provide guidelines for the installation of security systems on the UCI campus. This document applies to security installations that will be connected to the primary campus security systems and will be integrated to the UCI Police Department (PD) Dispatch Center.

1.2 CAMPUS SECURITY SYSTEM

A. Overview: The Campus Security System provides the capability to control access at designated portals, transmit alarm and event signals to the UCI PD Dispatch Center, provide video assessment capabilities to Dispatch operators, and provide emergency call stations located at strategic locations throughout the campus and in elevator cabs that connect directly to the UCI PD Dispatch Center. This document covers the following elements of the Campus Security System:

1. Electronic Access Control System (EACS)

2. Intrusion Detection System (IDS)

3. Emergency Phone System (EPS)

4. Video Surveillance System (VSS)

B. UCI PD Dispatch Center: The primary purpose of the PD Dispatch Center is to respond to emergency calls and dispatch officers as needed in response to events. The systems discussed in this document are deployed to enhance the operations of the Campus Police Department. As part of the Dispatch Center standard operations video cameras on campus are not actively monitored. Their purpose is to provide dispatch operators assessment capabilities related to specific events.

C. Security Analysis: When electronic security enhancements are planned for any campus facility a security analysis shall to be conducted. The analysis assesses the security issues that are being addressed, the operation of the facility adding the enhancements, the PD procedures for responding to events at the facility, the proper application of the electronic security elements, and how those elements shall integrate to the Campus Security System.

1.3 ELECTRONIC ACCESS CONTROL SYSTEM (EACS)

A. Purpose: The Electronic Access Control System is designed to monitor and restrict access to specified areas, and to report on the activity and violations of restricted access in those areas.

B. The campus standard EACS is Cardkey utilizing Pegasus 2000 software. The version of software at the time of this document is v3.12. Before any products are purchased for implementation the current version of software should be verified. Contact Facilities Management for information regarding the Cardkey Pegasus system.

C. The campus uses proximity type photo ID badges to provide access through card reader controlled doors. Only credentials provided by Facilities Management are compatible with the Campus standard EACS

D. Controllers: The system currently supports two types of controllers, CK720 series and CK721 series. The CK720 controllers are nearing end-of-life support and can be repaired but will not be used for new projects. All new projects will utilize the most current version of the CK721 controllers. The CK721 series can support up to 16 readers in legacy address configuration or 64 readers in expanded S300 configuration. Users shall coordinate with Facilities Management, Campus Design Engineer, or Johnson Controls before selecting any hardware to be integrated to the existing Campus Security System

E. The EACS is also capable of supporting Bosch Intrusion Detection panels. Refer to Article 1.4 for information on Campus Standard IDS operation.

F. Environment:

1. Primary Monitoring Post: Primary monitoring is located at the PD Dispatch Center with a back-up monitoring station in the mobile command post trailer adjacent to the PD building

2. Administration Station: System administration is managed by UCI Facilities department with administrative workstations located at the lock shop.

3. Additional Stations: Additional administrative stations are located throughout the campus to allow each individual school to administer cards specific to their area of responsibility.

4. Infrastructure and Connectivity:

a. Network communications for the EACS is over UCI’s Facilities Network (FacNet). FacNet is separate from the main campus network (UCInet).

b. The main P2000 server is located in the UCI OIT (Office of Information Technology) Data Center.

G. Product Restrictions: Cardkey is manufactured by Johnson Controls, Inc. (JCI) and only equipment obtained from JCI can be integrated into the Campus Security System

1.4 INTRUSION DETECTION SYSTEM (IDS)

A. Purpose: The Intrusion Detection System is designed to provide alarm monitoring of designated areas within campus buildings. The IDS is equipped with a keypad to allow arming/disarming of the system.

B. The campus standard IDS is the Digital Monitoring Products (DMP) software package for alarm reporting to the Genetec platform in UCI PD Dispatch.

C. Control Panels

1. The campus standard alarm panel is a DMP XR150DNL-G alarm panel.

2. Optional Panels: The upgrade of the EACS to Pegasus v3.12 now allows the use of Bosch alarm panels connected and programmed through the EACS. This option provides enhanced functionality and integration to the EACS and VSS. The choice of panels shall be decided by the results of the Security Needs Analysis.

D. System Integration: The DMP software has the availability to communicate alarm messages to the VSS. This provides the capability of IDS alarms to automatically call-up cameras at the PD Dispatch workstation to allow visual assessments of alarms where cameras are positioned to view the alarm location.

E. Environment:

1. Primary Monitoring Post: Primary monitoring is located at the PD Dispatch Center with a back-up monitoring station in the mobile command post trailer adjacent to the PD building.

2. Administration Station: The Administrative workstation is located in the PD Dispatch Center.

3. Infrastructure and Connectivity:

a. Alarm panels communicate using the campus network and report alarms through the Genetec software in the PD Dispatch Room. A redundant alarm receiver is located in the Central Plant.

b. The alarm receiver communicates over a RS-232 connection to a server in the PD Dispatch Data Room. The server communicates to the Dispatch Workstations over FacNet.

4. Acceptance to monitor any IDS panel shall be provided by the PD before the panel is connected to the Campus Security System

F. All alarms and alarm nomenclature need to be coordinated and approved by the PD before any system is connected to the PD Dispatch Center for monitoring.

1.5 EMERGENCY PHONE SYSTEM (EPS)

A. Purpose: The Emergency Phone System is to provide students, staff, and visitors a means to contact the UCI PD Dispatch Center in case of an emergency or other critical event.

B. The current campus standard for emergency phones is GAI-Tronics emergency call stations. Models vary depending on installation requirements. Outdoor locations are equipped with a blue light that identifies the station at night and flashes when a call is initiated. Contact UCI Office of Information Technology (OIT) for requirements related to new installations.

C. Emergency phone devices should meet UL 2017 listing for emergency signaling devices. This identifies emergency phones that are self-monitoring; meaning that if all or a portion of the device faults for any reason, the device's diagnostics can immediately notify those maintaining the system that there is an issue. This is of particular importance in parking garages and exterior spaces, where conditions can fluctuate with the outside weather.

D. Environment:

1. Primary monitoring of the Emergency Phone System is located at the PD Dispatch Center.

2. Calls from the emergency phone stations are routed through the campus 911 call system and are answered by dispatch operators using the 911 stations at each dispatch desk.

3. Communication Infrastructure:

a. Communications from the stations utilizes the existing campus copper infrastructure with phone lines connected to the campus central PBX phone switch.

b. Each phone provides ANI/ALI (Automatic Number Identification/Automatic Location Identification) to assist dispatch operator in identifying the location of the call.

E. Information regarding the ANI/ALI information shall be coordinated with the PD and Dispatch Supervisor before programming is implemented.

1.6 VIDEO SURVEILLANCE SYSTEM (VSS)

A. Purpose: The Video Surveillance System is designed to provide staff with the means to monitor, record, and review activity at strategic areas of the campus. The System shall provide the ability to record images received from cameras located throughout the campus in a digital format and retrieve the recorded video information in random access mode based on parameters requested by the user.

B. The campus standard VSS is Genetec utilizing Security Center v5.5 software. Before any products are purchased for implementation the current version of software should be verified. Contact Facilities Management for information regarding the Genetec Security Center system.

C. Environment:

1. Primary Monitoring Post: Primary monitoring is located at the PD Dispatch Center with a back-up monitoring station in the mobile command post trailer adjacent to the PD building

2. Administration Station: System administration is managed by UCI Facilities department with administrative workstations located at the lock shop.

3. Additional Stations: Additional administrative stations are located throughout the campus to allow each individual school to administer cameras specific to their area of responsibility.

4. Infrastructure and Connectivity:

a. Network communications for the VSS is over UCI's Campus Network (UCINet). Coordinate connection of cameras to UCInet with UCI OIT personnel. OIT shall determine if existing network resources are adequate or additional network equipment is required for each project.

b. The VSS Directory Server and Primary Recording Storage are located in the UCI OIT Data Center. Facilities Management in conjunction with OIT and the Campus Security Design Engineer shall determine if additional VSS hardware is required in the OIT Data Center to accommodate each project.

c. Storage for the PD cameras is provided on an archiver located in the PD server room.

d. An additional archiver is located at the Tierney House (Chancellor's Residence) to provide storage of video from cameras located at that location. Communication from the Tierney House archiver to the campus network is via a Cox cable connection leased by the University.

D. Considerations before Adding Cameras to the System

1. General: The VSS is a dynamic system and a few items need to be considered before additional cameras are added to the system.

2. Video Archiver Servers: The primary component of the VSS that needs to be addressed before additional cameras are added to the system is the video archiver. The video archiver is a computer that is used to manage cameras on the system and directs storage of the video streams to the appropriate hard drive storage system. Due to the high bandwidth of video cameras there is a limit to the number of cameras that can be managed by each video

archiver. If more cameras are assigned to the video archiver than can be effectively managed it can result in system degradation. Before a project is started the VSS needs to be analyzed for current capacity of each video archiver. If more cameras are to be included in a specific project than the available archivers can support an additional video archiver will be required to support the project. This analysis needs to be conducted during the design phase of the project to eliminate the possibility of change orders once the project has been awarded to a contractor.

3. Video Storage: The other critical element to address when adding cameras to the VSS is the amount of storage available on the system. A calculation needs to be completed to determine the amount of added hard drive storage capacity will be required for the number of cameras being added to the system. The calculation will include the number of cameras being added, the resolution of each camera, the anticipated amount of activity in each camera scene, and the number of days required to save the video data. Once this calculation is completed and compared to the existing hard drive storage capacity of the existing system it can be determined if additional storage capacity will be required for the project.

4. Camera and Workstation license: For each camera or workstation added to the system a user license will be required to enable operation of the device. It is recommended that each project include in the specifications the number of licenses required for all devices added to the system.

E. Camera Selection: The following guidance is provided in selecting cameras being added to the Campus Security System. The type of camera required and its function should be determined by the Security Needs Analysis.

1. Camera Resolution: The camera resolution determines the detail of the image as well as the data bandwidth and storage requirements for the camera. Four camera resolutions are defined to meet the majority of applications on campus. Special applications may require variations in these requirements.

   a. SD – Standard Definition comprising 800x600 pixel image

   b. HD – High Definition comprising 1280x720 (720p) pixel image

   c. SHD – Super High Definition comprising 1920x1080 (1080p) pixel image

   d. EHD – Extended High Definition comprising 2560x1920 pixel image

2. Camera Modes: Three camera modes are defined to assist in determine the proper camera selection:

   a. Surveillance Mode: This is the most common mode used for video surveillance. This provides good detail within the field of view and allows the ability to easily differentiate between objects within a scene. Surveillance mode requires a camera selection that provides 20 pixels per foot at the target location.

b. Forensics Mode: Forensic mode provides more detail in the image to assist in identifying detailed information in the scene. A typical application is the ability to clearly read the license number on a vehicle. Forensic mode requires a camera selection that provides 40 pixels per foot at the target location.

c. Facial Recognition Mode: Facial recognition mode provides extremely high detailed information on objects, primarily the human face, to allow special software applications to compare the image captured by the camera with a database of known images. This mode is reserved for very high security applications. Facial recognition mode requires a camera selection that provides 100 pixels per foot at the target location. Currently there are no applications for this mode on the campus.

3. Camera Selection Guide: The following table provides some guidelines for camera selection. It is recommended a detail camera analysis be undertaken to ensure proper camera selection and placement to meet the security needs of each project.

   a. SD Surveillance Mode – 40’ scene width

   b. SD Forensics Mode – 20’ scene width

   c. SD Facial Recognition Mode – 8’ scene width (not recommended)

   d. HD Surveillance Mode – 64’ scene width

   e. HD Forensic Mode – 32’ scene width

   f. HD Facial Recognition Mode – 12’ scene width

   g. SHD Surveillance Mode – 96’ scene width

   h. SHD Forensic Mode – 48’ scene width

   i. SHD Facial Recognition Mode – 19’ scene width

   j. EHD Surveillance Mode – 128’ scene width

   k. EHD Forensic Mode – 64’ scene width

   l. EHD Facial Recognition Mode – 26’ scene width

4. Low Light Areas: When cameras are to be placed in areas that may experience low or no light for periods of times the selected camera shall be equipped with an integrated IR illuminator. This will provide the camera the ability to see and record images when adequate lighting is not provided. This is a critical element of the camera selection process as it has a significant impact on the amount of data stored on the system archiver when inadequate lighting is provided.

5. Recording Protocols: Recording protocols determine the amount of computer hard drive storage space required to save the video images for future playback. The following are guidelines to be used to implement for future projects and may be modified as project needs are determined after the system has been in operation over a period of time.

a. Recording Modes: The information listed below is a guideline for cameras not assigned a specific recording protocol. Cameras assigned specific recording protocols shall supersede the modes listed below.

   1) Time Lapse mode: 2 fps (frames per second) at normal compression (CIF for conventional cameras and D1 for megapixel cameras).

   2) Normal Mode: 5 fps at SD. Quality setting medium-high

   3) Near Real-Time Mode: 8 fps at high quality compression at camera native resolution (800x600 for SD, 1280x720 for HD, 1920x1080 for SHD – typical)

   4) Real Time Mode: 15 fps at high quality compression. At native resolution

   5) Alarm, Event, Motion Detection Mode: 10 fps at high quality compression at native resolution

   6) Critical Alarm Mode: 15 fps at high quality compression. At native resolution

b. Recording Periods:

   1) Normal Business Hours: to be determined for each facility.

   2) Off Normal Hours: Hours: to be determined for each facility.

   3) 24-hour Mode

c. Typical Scenarios:

   1) Common Areas (Hallways, Building Entrance, Perimeters)

      a) Programmed for Normal Mode during Normal Business Hours

      b) Programmed for Time Lapse Mode during off normal hours

      c) During off normal hours the cameras shall switch from Time Lapse Mode to Motion Detection Mode when there is motion within view of the camera

      d) If the EACS/IDS goes into alarm mode after normal hours record the cameras in Alarm Mode

   2) Enclosed Low Use Rooms (Irradiator, Labs)

      a) Program the cameras for Time Lapse Mode and assign to 24-Hour Time Period

      b) Switch to Motion Detection Mode when there is activity in the rooms.

      c) If the EACS/IDS goes into alarm mode after normal hours record the cameras in Alarm Mode or Critical Alarm Mode depending on the value of the room

3) Other protocols will be determined as cameras are assigned to specific type areas.

6. Acceptable Cameras: This selection guide should be reviewed and updated on a yearly basis as manufacturers release newer versions of cameras.

   a. SD Indoor Dome: Axis Model P3224-V, Bosch Flexdome IP micro 2000

   b. SD Outdoor Dome: Axis Model P3225-VE or equal

   c. SD w/Integral IR Dome: Axis P3364-LVE or equal

   d. HD Indoor Dome: Axis P3224-V, Bosch NIN-63013-AXXX, Samsung SND-5084/5084R

   e. HD Outdoor Dome: Axis P3224-VE, Bosch NIN 73013-AXX, Samsung SNV-5084

   f. HD Outdoor Dome w/IR: Axis P3364-LVE, Bosch NDI-41012 V3

   g. HD Convention Box Camera: Axis P1364-E, Bosch NKN-71013-BA(X)-XXX, Samsung SNB-5004

   h. SHD Indoor Dome: Axis P3225, Bosch NIN-932-VXXX, Samsung SNV-6084

   i. SHD Outdoor Dome: Axis P3225-VE, Bosch NIN-63023-AXX, Samsung SNV-6084

   j. SHD Convention Box Camera: Axis P1365-E, Bosch NBN-932V-IP, Samsung SNB-6004

   k. EHD Indoor Dome: Bosch NUC-51022/51051 – F2M

   l. EHD Outdoor Dome: Axis P3367-VE, Bosch NDN/NDI-50051-A3

   m. EHD Convention Box Camera: Axis model P1357-E or equal

1.7 CAMERA SPECIFICATION GUIDE

A. General Requirements:

1. The camera shall be of manufacturer’s official product line, designed for commercial/industrial 24/7/365 use.

2. The camera shall be based upon standard components and proven technology using open and published protocols.

B. Technical Requirements:

1. Video Standard for Standard Definition (SD), High Definition (HD) and Super High Definition (SHD)

   a. SD – 800 x 600 pixels

   b. HD - SMPTE 296M (HDTV 720p)

   c. SHD - SMPTE 274M (HDTV 1080p)

d. EHD – 2560 x 1920 pixels

2. MPEG-4:

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

3. Networking:

   a. IEEE 802.3af (Power over Ethernet – 15w standard, PTZ cameras might take more)

   b. IEEE 802.1X (Authentication)

   c. IPv4 (RFC 791)

   d. QoS – DiffServ (RFC 2475)

4. Network Video:

   a. ONVIF Profile S or ONVIF Version 1.01 or higher as defined by the ONVIF organization

5. Mechanical:

   a. IEC 62262 Class IK10 (Impact resistance)

C. Functions

1. Be capable of providing video streams at camera rated resolution at 30 frames per second using H.264 or Motion JPEG

   a. SD – 800 x 600 pixels

   b. HD – 1280 x 720 pixels (720p)

   c. SHD – 1920 x 1090 pixels (1080p)

   d. EHD – 2560 x 1920 pixels

2. Be equipped with Day/Night functionality and remote zoom and focus capabilities.

3. Operate on an open source; Linux-based platform, and including a built-in web server.

4. Be manufactured with an all-metal vandal resistant body.

5. Use a high quality IR-sensitive progressive scan megapixel sensor.

6. Be equipped with a removable IR-cut filter, providing so-called day/night functionality.

7. Be equipped with a high quality varifocal lens with automated iris functionality, providing remote zoom and focus functionality.

8. Provide pictures down to 0.5 lux while in day mode (with IR-filter in use) and down to 0.08 lux while in night mode (with IR-filter removed).

9. Support memory expansion by providing an available SD/SDHC card slot.

10. Be manufactured with an all-metal body, support operation between -40 to +55°C (-40 to +131°F) and be both IP66 and NEMA 4X-rated.

11. Video Resolution; Camera shall support at a minimum the following resolutions:

    a. CIF – 320x240

    b. 2 CIF – 640x240 or 704x240

    c. 4 CIF – 640x480 or 704x480

    d. SD – 800x600

    e. HD – 1280x720 (not required for SD)

    f. SHD – 1920x1080 (not required for SD or HD)

    g. EHD – 2560x1920 (not required for SD, HD, or SHD)

12. Encoding

    a. Support Motion JPEG encoding in a selectable range from 1 up to 30 frames per second in all resolutions up to HDTV 1080p.

    b. Support H.264 encoding in a selectable range from 1 up to 30 frames per second in all resolutions up to HDTV 1080p.

    c. Be able to provide independently configured simultaneous H.264 and Motion JPEG streams.

    d. Support both Constant Bit Rate (CBR) and Variable Bit Rate (VBR) in H.264.

    e. Provide configurable compression levels.

    f. Support motion estimation in H.264.

    g. Support standard baseline profile H.264 with motion estimation.

13. Transmission

    a. HTTP (Unicast)

    b. HTTPS (Unicast)

    c. RTP (Unicast & Multicast)

    d. RTP over RTSP (Unicast)

    e. RTP over RTSP over HTTP (Unicast)

    f. Camera shall support Quality of Service (QOS) to allow prioritization of traffic

14. Image Control

    a. The camera shall incorporate Automatic and Manual White Balance and an electronic shutter operating in the range 1/6 and 1/35.500 second.

    b. The camera shall provide Wide Dynamic Range and backlight compensation with automatic and definable exposure zones.

15. Web Server

    a. The camera shall contain a built-in web server making video and configuration available to multiple clients in a standard operating system and browser environment using HTTP, without the need for additional software.

    b. Optional components downloaded from the camera for specific tasks, e.g. Active X, shall be signed by an organization providing digital trust services, such as VeriSign, Inc.

16. IP Addressing

    a. The camera shall support both fixed IP addresses and dynamically assigned IP addresses provided by a Dynamic Host Control Protocol (DHCP) server.

    b. The camera shall allow for automatic detection of the Camera based on UPnP and Bonjour when using a PC with an operating system supporting this feature.

    c. The camera shall provide support for both IPv4 and IPv6 (future growth).

17. Events

    a. The camera shall be equipped with an integrated event functionality, which can be trigged by:

        1) External input

        2) Video Motion Detection

        3) Audio Detection

        4) Schedule

        5) Camera tampering

        6) Local storage full

    b. Response to triggers shall include:

        1) Notification, using TCP, SMTP or HTTP

        2) Image upload, using FTP, SMTP or HTTP

        3) Activating external output

        4) Recording to local storage

    c. The camera shall provide memory for pre & post alarm recordings.

d. Event functions shall be configurable via the web interface.

18. Protocol Support

a. The camera shall incorporate support for at least IP, HTTP, HTTPS, SSL/TLS, TCP, ICMP, SNMPv1/v2c/v3 (MIB-II), RTSP, RTP, UDP, IGMP, RTCP, SMTP, FTP, DHCP, UPnP, ARP, DNS, NTP and Bonjour.

b. The SMTP implementation shall include support for SMTP authentication.

19. Text Overlay

a. Provide embedded on-screen text with support for date & time, and a customer-specific text, camera name, of at least 45 ASCII characters.

b. To ensure accuracy, the camera shall accept external time synchronization from an NTP (Network Time Protocol) server.

c. Provide the ability to apply a privacy mask to the image.

d. Allow for the overlay of a graphical image, such as a logotype, into the image.

20. Multi-streaming

a. The camera shall be capable of a minimum of 6 configurable video streams

b. The camera shall be capable of providing a stream for live viewing of 15 fps a full resolution independent of any stream configuration used for recording.

21. Security

a. Support the use of HTTPS and SSL/TLS, providing the ability to upload signed certificates to encrypt and secure authentication and communication of both administration data and video streams.

b. Support IEEE 802.1X authentication.

c. Provide support for restricting access to pre-defined IP addresses only, so-called IP address filtering.

d. Restrict access to the built-in web server by usernames and passwords at three different levels.

22. API Support

a. The camera shall be fully supported by an open and published API (Application Programmers Interface), which shall provide necessary information for integration of functionality into third party applications.

b. The camera shall conform to the network video standard as defined by the ONVIF organization.

23. Installation Maintenance

    a. Be supplied with Windows-based management software which allows the assignment of IP addresses, upgrade of firmware and backup of the Cameras' configuration.

    b. Support the use of SNMP-based management tools according to SNMP v1, 2c & 3 / MIB-II.

    c. Allow updates of the software (firmware) over the network, using FTP or HTTP.

    d. Provide the ability to apply a rectangle of customer-defined number of pixels to the image, which can be used as a pixel counter identifying the size of objects in number of pixels.

    e. All customer-specific settings shall be stored in a non-volatile memory and shall not be lost during power cuts or soft reset.

24. User Logs

    a. Provide a log file, containing information about the 250 latest connections and access attempts since the unit's latest restart. The file shall include information about the connecting IP addresses and the time of connecting.

    b. Provide a connection list of all currently connected viewers. The file shall include information about connecting IP address, time of connecting and the type of stream accessed.

25. Diagnostics

    a. Be equipped with LEDs, capable of providing visible status information. LEDs shall indicate the camera's operational status and provide information about power, communication with receiver, the network status and the camera status.

    b. Be monitored by a Watchdog functionality, which shall automatically re-initiate processes or restart the unit if a malfunction is detected.

26. Connectors

    a. Input/outputs: The camera shall be equipped with one digital (alarm) input and one digital output, accessible via a removable terminal block. This input shall be configurable to respond to normally open (NO) or normally closed (NC) dry contacts.

    b. Audio: The camera shall be equipped with one 3.5 mm jack for line/microphone input and one 3.5 mm jack for line output.

    c. Network: The camera shall be equipped with one 100BASE-TX Fast Ethernet-port, using a standard RJ-45 socket and shall support auto negotiation of network speed (100 MBit/s and 10 MBit/s) and transfer mode (full and half duplex).

27. Construction

    a. Manufactured with an all-metal vandal resistant body providing encapsulated electronics

    b. Clear and smoked transparent cover

    c. IP66-rating

    d. NEMA 4X-rating

    e. Impact resistance of 2200lbs / 1000kg according to IK10

    f. Thermostat, heater and fan inside the enclosure

    g. Fitted with a dehumidifying membrane

    h. Removable weather shield

    i. The camera enclosure shall provide the ability to adjust the camera modules angle with at least ±180° horizontal, ±85° vertical and ±170° rotation while maintaining an image that is not interfered with by the camera housing.

28. Power

    a. Power over Ethernet according to IEEE 802.3af - Class 3

    b. 24 VAC from Camera Power Supply

29. Environmental

    a. Operate in a temperature range of -40°C to +55°C (-40°F to +131°F).

    b. Operate in a humidity range of 15–100% RH (condensing).

D. Camera Types

1. Four camera types are identified in the specifications and drawings

    a. SD – Standard Definition comprising 800x600 pixel image

    b. HD – High Definition comprising 1280x720 pixel image

    c. SHD – Super High Definition comprising 1920x1080 pixel image

    d. EHD – Extended High Definition comprising 2560x1920 pixel imager

E. Acceptable Cameras

1. SD Indoor Dome: Axis Model P3364-V or equal

2. SD Outdoor Dome: Axis Model P3364-VEor equal

3. SD w/Integral IR Dome: Axis P3364-LVE or equal

4. HD Indoor Dome: Axis P3364-V, Samsung SND-5058/5080F or equal

5. HD Outdoor Dome: Axis P3384-VE, Samsung SNV-5080 or equal

6. HD Outdoor Dome w/IR: Axis P3364-LVE or equal

7. HD Convention Box Camera: Axis P1354-E, Samsung SNB-5001 or equal

8. SHD Indoor Dome: Axis P3367, Samsung SNV-6084, or equal

9. SHD Outdoor Dome: Axis P3367-VE, Samsung SNV-6046 or equal

10. SHD Convention Box Camera: Axis P1365-E, Samsung SNB-6004, or equal

11. EHD Outdoor Dome: Axis P3367-VE or equal

12. EHD Convention Box Camera: Axis model P1357-E or equal

F. Camera Lenses

1. Provide varifocal lens compatible with selected camera to cover the field-of-view as indicated on the plan drawings.

2. Provision for lens changes: Contractor shall include provision and installation of one (1) lens change per camera where necessary to provide acceptable viewing performance. Exchanged lenses shall remain the property of the Contractor.

3. Contractor shall field verify each location and coordinate field-of-view requirements with the Owner before ordering camera/lens combination. Contractor shall be responsible to select proper camera/lens combination to provide the field of view as shown on the drawings.

4. Some configuration of dome camera and lens combinations may not meet field of view requirements as indicated on the plan drawings. Where this occurs notify Owner to coordinate acceptable alternative.

G. Camera Enclosure Mounting Hardware

1. Provision for mounting hardware: The Contractor shall include provision and installation of miscellaneous hardware and mounting extensions at each camera location to provide acceptable viewing performance.

2. Exterior Inside-Corner Mount Bracket: Bosch VDA-CMT-DOME or equal, to match camera requirements.

3. Exterior outside-corner mount: Axis T91A series, Bosch VDA-WMT-DOME pendant mount attached to a Pelco ECM100 corner plate modified for attaching the Bosch pendant or custom corner mount provided by the contractor.

4. Ancillary Hardware shall be provided by the Contractor, if required, and shall be compatible with and comparable in strength to other attached hardware.

END OF CAMPUS DESIGN STANDARDS