1.0 GENERAL

1.1 Related UBC Guidelines

.1 Section 28 16 00 Intrusion Detection
.2 Section 28 13 00 Access Control
.3 Section 28 20 00 Safety and Security Cameras
.4 Section 27 05 08 Cable Infrastructure Design Guidelines, sub sections 1.4.9 and 1.5
.5 Section 27 05 05 Communication Rooms Design Guidelines, sub section 1.4
.6 Section 28 31 00 Fire Detection and Alarm
.7 Section 14 20 00 Elevators

1.2 Coordination Requirements

.1 UBC Campus Security and Secure Access
.2 UBC Campus and Community Planning
.3 UBC Information Technology
.4 UBC Building Operations Electrical Technical Support

1.3 Description

.1 UBC Campus Security and Secure Access supports UBC's ongoing strategy to increase safety and security to the University community. The guidelines herein have been created by Campus Security and Secure Access to clarify the design and installation process of electronic security systems on the UBC campus.

.2 The guidelines are intended to foster cooperation between all parties involved whether they be UBC related or not.

.3 Special consideration must be given to the security industry as being technology based. Industry advancements have an evolutionary effect on the design and manufacturing of security equipment. It is therefore critically important that Campus Security and Secure Access remain flexible in its implementation of UBC standards and guidelines.

.4 This document must be read, interpreted and coordinated with all other related Sections to deliver a complete electronic security system.

.5 The Campus Security and Secure Access Guidelines and others mentioned herein prescribe minimum acceptable standards for all equipment and procedures relating to electronic security.

.6 Security systems to be installed as part of newly constructed buildings or as part of renovations within existing buildings shall always reflect the intent of Campus Security and Secure Access standards and guidelines.

.7 Campus Security and Secure Access is the UBC group solely responsible for the consultation, design installation, verification, maintenance, and management of all electronic security on campus.

.8 Any and all proposed changes to these standards shall be subject to approval in writing by Campus Security and Secure Access prior to implementation.

1.4 Terminology

.1 Electronic Lockbox
- .1 A UBC card-enabled key safe to control onsite distribution of keys.

.2 Access Control System
- .1 A card access system used to manage and control to UBC space and assets. The unlocking of selected entries is scheduled and controlled electronically to allow authorized user entry via card reader, keypad, etc.

.3 Access Control Panel
- .1 An access system's onsite processor that manages access devices and governs the scheduling of all card reader controlled entries. Can be used singly or in tandem.

.4 Access Device
- .1 Any device included in an access system that is connected to and managed by the access control panel (i.e. card reader, RTE motion, etc.)

.5 Access Card
- .1 As provided by the UBC Card program, a proximity credential presented at a card reader by an authorized user to grant access.

.6 Card Reader
- .1 An access card recognition device, typically proximity type that allows for the entry of an authorized card holder.

.7 Card Reader Door
- .1 A "controlled door" that includes a card reader for authorized entry and unlocking.

.8 Controlled Door
- .1 A single, double, or group of doors whose locking functions are provided by system scheduled electronic locking.

.9 Electronic Locking Hardware
- .1 Access control door hardware, typically "handset" or "panic" type aesthetically identical to regular hardware and whose locking function is controlled electro-mechanically.

.10 Electric Strike
- .1 An access control door strike designed as a replacement for a regular strike plate that is controlled electro-mechanically.

.11 Request to Exit (RTE) Motion
- .1 A motion detector installed at a controlled or card reader door to monitor occupant egress.

.12 Request to Exit Hardware
- .1 A dry contact included within a controlled or card reader door's egress hardware to monitor occupant egress.

.13 Intrusion Detection System
- .1 A control system that manages the various installed devices (door contact, motion detectors, etc.) and communicates their status for monitored response. The system is enabled and disabled through devices such as keypads and card readers.

.14 Intrusion Detection Control Panel
- .1 An alarm system's central processor responsible for monitoring and reporting both system and device status.

.15 Intrusion Detection Device
- .1 Any device included in an alarm system that is controlled and monitored by the alarm control panel (i.e. siren horn, keypad, motion detector, etc.).

.16 Intrusion Detection Keypad
- .1 A tactile keyed, multifunction device manually operated by an authorized user typically for arming and disarming.

.17 Monitored (Secured) Area
- .1 A protected area, in whole or in part, within a secured perimeter.

.18 Monitored Door
- .1 A single, double or group of doors that have their open or closed position monitored by a door position contact. Monitored doors typically define the perimeter of a secure area.

.19 Door Position Contact
- .1 A sealed magnetic reed contact that monitors a door's open/close position.

.20 Motion Detector:
- .1 A spatial protection device used to detect movement within a secured area by monitoring changes in microwave and/or infrared field patterns.

.21 Glass Break Detector
- .1 A micro phonic device used to detect glass breakage by "listening" to specific frequencies typical of breaking glass, from initial impact to shattering.

.22 Movable Object Detector
- .1 An optical "transceiver" device used to monitor a fiber optic cable loop that is routed through the protected equipment (i.e. computer, printer, etc.)

.23 Photo Electric Beam
- .1 A continuous narrow focus infrared beam emitted from a transmitter and acknowledged by a receiver. These devices are typically installed outside a building's perimeter in a "fence post" configuration.

.24 Siren Horn
- .1 An audible device triggered to sound during an alarm condition.

.25 Safety & Security Camera System
- .1 Compliant with UBC Policy #118, a video management system typically consisting of cameras, server and storage environment, and software. Used for managing live and recorded images.

.26 Safety & Security Camera
- .1 A video image capturing device installed to view a specific area of concern.

.27 Video Encoder
- .1 A device that converts analogue composite video inputs to Ethernet outputs.

.28 Mid-span Injector
- .1 A device that provides inline PoE/PoE+ to a structured data run.

2.0 CONTRACTOR AND/OR CONSULTANT RESPONSIBILITIES

2.1 General

.1 The contractor and/or consultant has the responsibility to ensure that all provisions of these Standards are met and to specifically advise the University in writing of any contemplated exceptions and obtain approval from Campus Security and Secure Access for all contemplated changes.

2.2 UBC Procedure

.1 Campus and Community Planning shall facilitate the communications and efforts of the contractor with Campus Security and Secure Access.

2.3 System Design

.1 The security system shall be designed ~~by~~ through consultation and approval by Campus Security and Secure Access.

2.4 System Infrastructure

.1 Campus and Community Planning and the project architect/engineer must ensure that the contractor provide the correct security infrastructure for the building. This infrastructure shall include:

- .1 Cable pathway.
- .2 Cable.
- .3 Security panel power and space allocation in Comm Rooms.
- .4 Communication lines (telephone or LAN).
- .5 Preparation of door frames, doors, walls, ceilings, etc., to accept security devices and hardware.
- .6 Provision of door hardware to accept UBC keyed cylinders
- .7 Fire Alarm interface.
- .8 Elevator control interface.
- .9 Door hardware power.

.2 All pathways expressly installed for Communications (Data and Telephone) will only be used for other types of cable with the permission of UBC IT. See Section 27 05 08 Cable Infrastructure Design Guidelines sub section 1.5.

.3 Electronic Safety & Security cabling to be installed within Division 27 pathways (cable tray or riser conduit) shall comply fully with all Division 27 requirements. Unless otherwise approved or directed, ESS cabling (outside of cable trays or riser conduit) shall be installed in a separate conduit pathway.

2.5 System Installation

.1 All Intrusion (Section 28 16 00 Intrusion Detection), Access (this section), and Camera system (Section 28 20 00 Electronic Surveillance) equipment installation work shall be performed by Campus Security and Secure Access. If under special circumstances, security installation is to be contracted out to outside companies, the contractor must be acceptable to Campus Security and Secure Access, and all such work shall be done under the direction and supervision of Campus Security and Secure Access. The contractor must use provincially trade qualified technicians who individually have a minimum of five years of Enterprise System level commercial installation experience.

2.6 System Verification

.1 System verification shall be performed by Campus Security and Secure Access. The contractor must ensure and coordinate through Campus and Community Planning the verification of all security related equipment and its performance as an integrated part of the security system (i.e. fire alarm interface, elevator interface, door hardware, etc.).

2.7 Contract Documents

.1 The contract documents shall clearly indicate that Campus Security and Secure Access will be installing the UBC keyed cylinders and security equipment. The contract documents shall also require that all conduit, cable, etc. be clearly marked/tagged and cross-referenced to shop drawings.

2.8 Shop Drawings

.1 Before commencing with the installation of security system infrastructure, the University requires that the consultant or contractor supply Campus Security and Secure Access with design and installation details in the form of shop drawings (i.e. door hardware, system interface, etc.)

.2 The Contractor shall be responsible for all errors or omissions in the shop drawings and for meeting all requirements of the contract documents.

3.0 CAMPUS SECURITY AND SECURE ACCESS RESPONSIBILITIES

3.1 General

.1 Campus Security and Secure Access will assist departments in determining their security requirements and act as the agent to: ensure quality and consistency, ensure justification for the system installation, ensure adherence to the university guidelines.

3.2 Consultation

.1 Consult, coordinate, and/or supervise the consultation of on-campus security systems.

3.3 System Design

.1 Design, coordinate, and/or supervise the design of on campus security systems. Where applicable, work with project architects and engineers to provide input to, and approval of, electronic security systems designs.

3.4 System Installation

.1 Supply and install all electronic security equipment on campus in whole or in addition to existing systems. Coordinate inclusion of related equipment (Door hardware, elevator, fire alarm, etc.

3.5 System Verification

.1 Verify, coordinate, and/or supervise the verification of on-campus security systems (including related equipment).

3.6 Post Installation

.1 Service, maintain, and manage each and all of the electronic security systems on campus.

.2 Arrange for the preparation of as-built documentation of the completed installation, including wiring schedules.

3.7 Performance Standards

.1 To ensure compliance with industry-wide standards, the latest edition of the following documents and standards, current and proposed, are referenced and shall be complied with in the design, material selection, installation, configuration / programming, and system verification. This shall apply equally to new installations, upgrade and renovations at UBC. Whereas referenced codes dictate minimum requirements for safety, where a contradiction may exist between any of the following, and absent written direction from UBC, the most stringent requirement shall be met and included in the project cost.
- .1 Campus Security and Secure Access Guidelines.
- .2 UBC Technical Guidelines incorporating Division 28 Electronic Safety and Security.
- .3 BC Electrical Code (& issued Technical Bulletins).
- .4 BC Fire Code (& issued Technical Bulletins).
- .5 BC Building Code (& issued Technical Bulletins).

4.0 SYSTEM DESIGN

4.1 General

.1 System design shall produce a consistent outcome to increase safety and security for the University, reduce risk, and enable access. Campus Security and Secure Access provides consultative input to project teams and user stakeholders to ensure the successful application of security technology with operational requirements.

4.2 Operational Function

.1 The following functional requirements shall be identified prior to the design of any security system to be installed on Campus:
- .1 Space ownership and usage.
- .2 Location of perimeter doors.
- .3 Location of entrances/exits (daytime and after hours).
- .4 Location of disabled assess points.
- .5 Location of vulnerable interior spaces.
- .6 Location of special areas (computer labs, expensive equipment, library, chemical storage, sensitive research operation, etc.).
- .7 Building hours of operation.
- .8 System monitoring.

4.3 Application

.1 The following requirements shall be included in the consideration and design of any security system on campus:

- .1 Electronic Lockbox
  - .1 A Lockbox shall be installed at an appropriate location to facilitate keyed access to authorized personnel.

.2 Monitored Doors
.1 All building perimeter doors shall be monitored and mechanically locked to prevent entry at all times, with the exception of controlled door and card reader doors.

.3 Controlled Doors
.1 Depending on building requirements, selected doors will be designated as controlled doors to be electrically locked/ unlocked on a time schedule basis.

.4 Card Reader Doors
.1 At least one door (typically disabled access door, or if none, the main door to the building) shall be provided with card access control. Additional doors may be designated as card reader doors depending on the building size and layout, after-hours use, space ownership and functionality, and pedestrian traffic into and through the building.

.2 All classroom doors shall be provided with card access control. Refer to UBC Learning Space Design Guidelines 5.12.2 Key Strategies, Card Access, Security of Learning Technology Equipment for additional details.

.5 Intrusion Devices
.1 Areas within a building that are considered high risk shall include the installation of intrusion system devices.

.2 Areas within a building that are considered to be "reasonably accessible" from the building exterior may include the installation of a detection device (i.e. motion sensor, glass-break sensor, photo-beam, or other applicable devices).

.6 Arm/Disarm
.1 System arming/disarming shall be provided on a "per zone or per area" basis via keypad, card reader or combination thereof.

.7 Monitoring
.1 System monitoring shall be provided via UBC Information Technology voice grade phone service or campus LAN.

.8 Safety and Security Cameras
.1 Areas considered high risk or special interest may include the installation of a safety & security camera.

.9 Electronic Safety & Security Typical Application Drawings
.1 For all projects with Electronic Safety & Security scope, the following typical application drawings shall be referenced and complied with, in addition to all aspects of Division 28 Technical Guidelines sections.

.2 ACS Card Reader Door Typical:
https://technicalguidelines.ubc.ca/Division_28/dwg/AS-1_Card_Reader_Door_Typ.a.pdf

.3 Typical Lock Box Installation with Camera (ITSTD-27):
https://technicalguidelines.ubc.ca/Division_27/dwg/ITSTD-27.pdf

.4 Intrusion Devices Typical:
https://technicalguidelines.ubc.ca/Division_28/dwg/AS-2_Intrusion_Devices_Typ.pdf

.5 CCTV Communications Demark for IP Cameras in T-Bar (Typical) (ITSTD-23): https://technicalguidelines.ubc.ca/Division_27/dwg/ITSTD-23.pdf

.6 CCTV Communications Demark for IP Cameras in Solid Ceiling (Typical) (ITSTD-24): https://technicalguidelines.ubc.ca/Division_27/dwg/ITSTD-24.pdf

.7 CCTV Communications Demark for IP Cameras in Solid Ceiling, Outlet in T-Bar (Typical) (ITSTD-25): https://technicalguidelines.ubc.ca/Division_27/dwg/ITSTD-25.pdf

*****END OF SECTION*****

1.0 GENERAL

1.1 Related UBC Guidelines

.1 Section 28 05 00 Campus Security and Secure Access: General Standards
.2 Section 08 71 00 Door Hardware

1.2 Coordination Requirements

.1 UBC Campus Security and Secure Access

1.3 Description

.1 This section covers requirements for Access Control Systems. The Access Control System is installed by UBC Campus Security and Secure Access. General Requirements for this system for Consultants and Contractors are provided in Section 28 05 00 Electronic Security Systems: General Standards.

.2 These guidelines provide reference to particular types, grades and models of products. In general, the references include both generic descriptions and specific product details. These references shall not be construed as a directive to sole-source products from any particular vendor except where this is specifically stated.

.3 Access Control System that manages and controls occupant access into buildings and/or assets, and that the arming and locking of selected entries is scheduled and controlled electronically to allow authorized user entry via card reader, keypad etc., shall include the following:
.1 Electronic lock box
.2 Access control panel.
.3 Access devices.
.4 Card readers.
.5 Access cards.
.6 Door position contacts.
.7 Request to Exit motion detectors.
.8 Hardware egress dry contacts.
.9 Electrified locking hardware.
.10 Power Supply - Hardware.
.11 Power transformers.

2.0 EQUIPMENT SPECIFICATIONS AND REQUIREMENTS

2.1 Lock Box

.1 Device Location
.1 Lock box shall be wall mounted, located in suitably determined area restricted to authorized personnel via card reader. Campus Security and Secure Access to confirm location.
.2 Mounting surface shall include solid plywood material minimum 38 mm thickness to span entire lock box dimensions.

.2 Power Raceway
.1 Armoured cable to enter lock box through rear cutout. Un-switched 120VAC, dedicated breaker c/w generator and/or UPS backup whenever possible.

.3 Data Raceway
.1 Demark for Lockbox. Reference to Communications Standard Drawing ITSTD-27

.4 Device Features
.1 Powered directly from un-switched 120VAC.
.2 Control circuitry housed in mechanically secured lock box c/w with tamper.
.3 Wall mounted.
.4 UBC Card compatible
.5 Minimum 32 key slot capacity. Confirm sizing with Campus Security and Secure Access.

2.2 Access Control Panel

.1 Device Location
.1 Panels to be mounted in communications room within the protected area. (Exact location to be confirmed by UBC IT- Connectivity Infrastructure). If it is not possible to locate the panel in the communication room, panel should be mounted in a secure room within the protected area.
.2 Panels must not be mounted above ceiling if space is "return air" plenum type.

.2 Raceway
.1 Power transformer fed from un-switched 120VAC, dedicated breaker c/w generator and/or UPS backup whenever possible.

.3 Cabling
.1 All related wiring for panels should be concealed and home-run whenever possible.FT4 rated wire, FT6 rated if required.
.2 Wire path and dressing within communication rooms to conform to UBC IT - Connectivity Infrastructure standards.

.4 Device Features
.1 Cabinets/enclosures shall typically be cam lockable, 20” x 24” x 6”, with side-hinged door.
.2 Powered from Class 2 step down transformer (typically 16 VAC).
.3 Control circuitry housed in a mechanically securable keyed box c/w with monitored tamper switch as directed.
.4 Wall mountable.
.5 UBC Card compatible.
.6 Provide 5 Vdc to 12 Vdc for related end devices.
.7 Power supplies shall be 16VAC in, 12VDC out, 2A fused.
.8 Minimum two reader ports.
.9 Minimum one fully programmable per reader port.
.10 Support "end of line resistor" fully supervised zones. Processing capabilities for all major reader formats. Fully programmable or either serially via LAN. Panel to panel expandable either serially or via LAN. Windows based operating software Operating temperature 0° C to +40° C.

2.3 Card Reader

.1 Device Location
.1 To be wall mounted typically on the restricted entry side of the controlled door.
.2 Standard mounting height 915 mm AFF, disabled 760 mm if required.

.2 Raceway
- .1 19 mm conduit terminated to single gang box, stub to Cable Tray.
- .2 Surface Wiremold equivalent: V700 raceway to V5747-1 box.

.3 Cabling
- .1 3 pair twist/strand/shield c/w drain 22 AWG FT4 rated, FT6 if required. Belden 5542FE or approved equivalent.
- .2 Home run to control panel.
- .3 Maximum wire length 80 meters/run unless specified otherwise.

.4 Device Features
- .1 5Vdc to 12 Vdc operation.
- .2 Wiegand and/or other standard protocol
- .3 2-color LED status display.
- .4 Sealed weatherproof construction.
- .5 Operating temperature -40° C to +65° C
- .6 Encrypted authentication read function, 13.56 MHz.

2.4 Request-to-Exit Motion Detector (RXM)

.1 Device Location
- .1 Should be wall-mounted above the controlled door, free from conflict with exit signage, aimed/directed to primary direction(s) of approach.
- .2 Can be ceiling-mounted if necessary.

.2 Raceway
- .1 19mm conduit terminated to 4x4 box c/w 2 gang plaster ring, stub to Cable Tray.
- .2 Surface Wiremold equivalent: V700 raceway to V5747-2 box.

.3 Cabling
- .1 6/22 FT4 rated wire, FT6 rated if required. Belden 5504UE or approved equivalent.
- .2 Home run to control panel.
- .3 Maximum wire length 80 meter/run unless specified.

.4 Device Features
- .1 12 Vdc operation.
- .2 Alarm output dry contact N/O or Form C if required.
- .3 Passive infrared detection or microwave if required.
- .4 Noise filtering adjustable output relay time.
- .5 LED status indicator.
- .6 Insect immunity.
- .7 Fully adjustable viewing angle, vertical and horizontal.
- .8 Integrated 90 db local door alarm sounder (Piezo buzzer) independently controlled by access control panel/system.

2.5 Door Contacts

.1 Device location
- .1 **Frame**: Flush mounted concealed contact to be installed in the top of the door frame 305 mm from strike side edge. Frame to be provided with 25mm diameter by 38mm deep through hole c/w back box for raceway termination.
- .2 **Door:** Concealed magnet should sit no more the 13mm away from contact with the door in a fully closed position. Top of door to allow for installation of 25mm diameter by 38mm deep magnet assembly.

.2 Raceway
.1 13mm conduit terminated to frame back box. Stub to Cable Tray.
.2 Surface Wiremold equivalent: V500 raceway to V5747-1 box.

.3 Cabling
.1 4/22 FT4 rated wire, FT6 rated if required. Belden 5502UE or approved equivalent.
.2 Home run to control panel or keypad/expansion module if applicable
.3 Max wire length 80 meters/run unless specified

.4 Device Features
.1 Hermetically sealed, corrosion-proof reed switch.
.2 Minimum 13mm operating gap between contact and magnet.

2.6 Power Transformers

.1 Device location
.1 Shall be "wire-in" type and mounted close to the control panel in the communication room. Plug-in type under restricted circumstances.
.2 Compatible with any 13mm punch out conduit box.
.3 Must not be installed above false ceiling if space is "return air" plenum type.

.2 Raceway
.1 Power transformer fed from un-switched 120VAC, dedicated breaker c/w generator and/or UPS backup whenever possible.

.3 Cabling
.1 2/18 FT4 rated wire, FT6 rated if required. Belden 5300UE or approved equivalent.
.2 Home run directly to control panel
.3 In communication room, dress cable to UBC IT - Connectivity Infrastructure standards

.4 Device Features
.1 Fully certified Class 2 rated.
.2 ULC and CSA approved.
.3 Fail-safe in the event of current overload or short circuit.
.4 16VAC input, 40VA output minimum.

2.7 Power Supply – Door Hardware

.1 General
.1 UBC Campus Security and Secure Access equipment interfaces to Electrified Hardware at Power Supplies.

.2 Device Location
.1 Power Supply shall be located in communications room (exact location to be confirmed by UBC IT - Connectivity Infrastructure). Locations subject to hardware design.
.2 UBC Campus Security and Secure Access equipment interfaces to Electrified Hardware at Power Supplies.

.3 Raceway
.1 19mm conduit terminated directly to Power Supply enclosure. Wiremold equivalent V700.
.2 Supply may source power to more than one Electrified Hardware Device. Subject to Hardware design.

.4 Cabling/Interface
- .1 Subject to Hardware design.
- .2 Power Supply to be equipped with “Dry Trigger” function (i.e. SDC CR4) to allow complete isolation of UBC Campus Security and Secure Access equipment from Hardware power.
- .3 “Dry Trigger” cable: 4/22 FT4 rated wire, FT6 rated if required. Belden 5502UE or approved equivalent.

.5 Power/Features
- .1 Direct power to Supply fed from un-switched 120VAC, dedicated breaker c/w generator and/or UPS backup whenever possible.
- .2 Equipped with battery backup whenever possible.
- .3 Interface to Fire Alarm when required by code.
- .4 ULC listed power supplies and distribution boards.
- .5 Dual voltage 12 or 24 VDC field selectable continuous output.
- .6 Minimum 2A output.
- .7 Minimum four (4) output distribution boards.

2.8 Electrified Hardware

.1 General
- .1 Electrified Hardware requirements and specifications are not included in this section. See Section 08 71 00 Door Hardware.
- .2 Hardware interface requirements to UBC Campus Security and Secure Access equipment described above, Power Supply – Hardware

*****END OF SECTION*****

1.0 GENERAL

1.1 Related UBC Guidelines

.1 Section 28 05 00 Electronic Security Systems: General Standards

1.2 Coordination Requirements

.1 UBC Electronic Systems and Campus Security and Secure Access

1.3 Description

.1 This section covers requirements for Intrusion Detection Systems. The Intrusion System is installed by Campus Security and Secure Access. General Requirements for this system for Consultants and Contractors are provided in Section 28 05 00 Electronic Security Systems: General Standards.

.2 These guidelines provide reference to particular types, grades and models of products. In general, the references include both generic descriptions and specific product details. These references shall not be construed as a directive to sole-source products from any particular vendor except where this is specifically stated.

.3 Intrusion detection system that monitors the various alarm devices (door contacts, motion detectors, glass break detectors, duress (panic) buttons etc.) and transmits their status over voice grade telephone line or IP network, and that is enabled and disabled through devices such as keypads, card readers or key switches where necessary, shall include:

.1 Intrusion detection control panel.
.2 Intrusion detection devices.
.3 Siren horns.
.4 Intrusion detection keypads.
.5 Door position contacts.
.6 Motion detectors.
.7 Glass breaks detectors.
.8 Photo electric beams.
.9 Movable object detectors.
.10 Power transformers.

2.0 MATERIALS SPECIFICATION

2.1 Alarm Control Panel

.1 Powered from Class 2 step down transformer (typically 16VAC)
.2 Control circuitry housed in a mechanically securable box with tamper option
.3 Wall mountable
.4 Provide 12VDC for related data bus and detection devices
.5 Function in all major communication formats
.6 Support "end of line resistor" fully supervised zones
.7 Fully programmable
.8 Fully upgradeable/downloadable
.9 Multi access code/multi user
.10 Event scheduling
.11 Event logging
.12 Multi keypad

.13 Comm line supervision
.14 A/C fail supervision
.15 Low battery supervision
.16 EXPROM or non-volatile RAM memory retention
.17 Operating temperature 0 C to +40 C

2.2 Keypads

.1 12 VDC operation
.2 Two way digital data transfer to and from control panel
.3 LED arm/disarm status
.4 Back lit keys
.5 Back lit LCD alpha numeric display, with optional configurable audible annunciation
.6 Menu driven/user interactive
.7 Min. 5 digit code length
.8 Equipped with onboard zone inputs

2.3 Motion Detectors

.1 12VDC operation
.2 Alarm output dry contact N/O or Form C if required
.3 Dual detection technology (microwave and passive
.4 Noise filtering for both microwave and passive infrared
.5 White light immunity
.6 Turbulent air immunity
.7 Insect/pet immunity
.8 RIF immunity
.9 Ambient temperature compensation
.10 Operating temperature - 15C to +50 C

2.4 Audio Glass Break Detectors

.1 12VDC operation
.2 Alarm output dry contact N/O or Form C if required
.3 Microprocessor based frequency analysis
.4 Audio discrimination
.5 Processing capabilities for plate, wired, laminated, and tempered glass

2.5 Photo Electric Beams

.1 12VDC operation
.2 Alarm output dry contact N/O or Form C if required
.3 Dual infrared photoelectric beams
.4 Selectable beam frequency
.5 Selectable beam intervention time
.6 Weatherproof housing with tamper switch
.7 Operating temperature - 30C to +40C

2.6 Magnetic Contacts

.1 Hermetically sealed, corrosion proof reed switch
.2 Min. 13mm operating gap between contact and magnet

2.7 Power Transformers

.1 Fully certified Class 2 rated
.2 ULC and CSA approved
.3 Fail-safe in the event of current overload or short circuit
.4 16VAC input, 40VA output minimum.

3.0 EXECUTION

3.1 Alarm Control Panel

.1 Device location
  .1 Panels should be mounted in communications room within the protected area. (Exact location to be confirmed by UBC IT - Connectivity Infrastructure). If it is not possible to locate the panel in the communication rooms, panel should be mounted in a secure room within the protected area. Confirm with Campus Security and Secure Access.
  .2 Panels must not be mounted above false ceiling if space is “return air" plenum type.

.2 Wiring
  .1 All related wiring for panels should be concealed and home-run whenever possible.
  .2 FT4 rated wire. FT6 rated wire when required.
  .3 Wire path and dressing within communication rooms to conform with UBC IT - Connectivity Infrastructure standards
  .4 Power- transformer fed from un-switched 120VAC dedicated breaker c/w generator and/or UPS backup whenever possible.

3.2 Keypads

.1 Device location
  .1 Keypad to be wall mounted within the protected area
  .2 Standard mounting height between 1220mm and 1524mm.

.2 Wiring
  .1 6/22 FT4 rated wire. FT6 rated if required
  .2 Home run to control panel
  .3 When using conduits to conceal wire, mount keypads to double- gang boxes
  .4 When using V series wire mold to conceal wire, mount keypads to shallow double-gang boxes
  .5 Max wire length 80 meters/run unless specified

3.3 Motion Detectors

.1 Device location
  .1 Motion should be wall or ceiling mounted
  .2 Standard wall mounting height 2286mm
  .3 Motion should be corner mounted facing away from perimeter windows

.2 Wiring
  .1 6/22 FT4 rated wire. FT6 rated wire if required
  .2 Home run to control panel or keypad/expansion module where applicable
  .3 When using conduit to conceal wire, mount detector to single gang box

.4 When using V series wire mold to conceal wire, mount detector to shallow single gang box
.5 Max wire length of 80 meters/run unless specified otherwise

3.4 Audio Glass Break Detectors

.1 Device location
.1 Wall or ceiling mounted within protected area
.2 Standard wall mount height 2438mm
.3 Detector should be facing perimeter glass

.2 Wiring
.1 6/22 FT4 rated wire. FT6 rated wire if required
.2 Home run to control panel or keypad/expansion module if applicable
.3 When using conduit to conceal wire, mount detector to single gang box
.4 When using V series wire mold to conceal wire, mount detector to shallow single gang box model
.5 Max wire length 80 meters/run unless specified otherwise

3.5 Photo Electric Beams

.1 Device location
.1 For external use mostly
.2 Defines protected area by creating an "electronic fence"
.3 Should be pole-mounted at a height between 610mm and 1829mm

.2 Wiring
.1 Adhere to NF standards
.2 6/22 FT4 rated wire. FT6 rated wire if required
.3 Home run to control panel or keypad/expansion module if applicable
.4 Concealed pathway
.5 Max length of 80 meters/run unless specified otherwise

3.6 Magnetic Contacts

.1 Device location
.1 Contact should be installed in the top of the door frame, in line with the center of the door.
.2 Magnet should sit no more the 13mm away from contact with the door in a fully closed position.
.3 Contact should be flush mounted and concealed in door frame whenever possible.

.2 Wiring
.1 4/22 FT4 rated wire. FT6 rated wire if required
.2 Home run to control panel or keypad/expansion module if applicable
.3 When using conduit to conceal wire, the pipe should stub directly into the frame or terminate directly above frame in a single gang box
.4 When using wire mold to conceal wire, the wire mold should stub directly into the frame or terminate directly above frame in a shallow single gang box model
.5 Max wire length 80 meters/run unless specified otherwise

3.7 Power Transformers

.1 Device location
- .1 Should be "wire-in" type and mounted as close to the control panel as possible, preferably in the communication room. Plug-in type under restricted circumstances.
- .2 Compatible with any 13mm punch out conduit box.
- .3 Must not be installed above false ceiling if space is "return air" plenum type.

.2 Wiring
- .1 Adhere to UBC IT - Connectivity Infrastructure standards
- .2 2/18 FT4 rated wire. FT6 rated wire if required
- .3 Home run directly to control panel
- .4 In communication room, dress wire to cable facilities standards

*****END OF SECTION*****

1.0 GENERAL

1.1 Related UBC Guidelines

.1 Section 28 05 00 Access Services: General Standards

1.2 Related UBC Policy

.1 Policy No.: SC16 - Safety and Security Cameras

1.3 Coordination Requirements

.1 UBC Electronic Systems and Campus Security and Secure Access.

1.4 Description

.1 All Safety and Security Camera installations shall comply with UBC Policy No. SC16: https://universitycounsel.ubc.ca/policies/video-cameras-policy/

.2 This section covers requirements for Safety and Security Cameras. Cameras are installed by Campus Security and Secure Access. General Requirements for this system for Consultants and Contractors are provided in Section 28 05 00 Electronic Security Systems: General Standards.

.3 These guidelines provide reference to particular types, grades and models of products. In general, the references include both generic descriptions and specific product details. These references shall not be construed as a directive to sole-source products from any particular vendor except where this is specifically stated.

.4 Safety and Security Camera system that monitors both live and recorded events may include the following:
- .1 IP camera.
- .2 Video Encoder
- .3 Mid-span Injector
- .4 Video Management System (VMS) software.
- .5 VMS server and storage.
- .6 Desk top computer.

2.0 MATERIALS

2.1 IP Camera

.1 Device Location
- .1 Wall or ceiling mountable. Whenever possible, camera should be faced away from available light source. Exact location and viewing angle shall be confirmed by Campus Security and Secure Access.

.2 Wiring
- .1 Demark for IP Cameras. Reference to Communications Standard Drawings ITSTD-23, ITSTD-24, and ITSTD-25

.3 Device Feature
- .1 PoE Class 3 or better.

.2 Minimum resolution 1920 x 1080 (2MP), capable of 30+ IPS, minimum 2 streams at full resolution.
.3 Minimum illumination 0.16 lux (Colour), 0.08 lux (Black & White).
.4 RJ45 connector.
.5 Video Compression supported includes H.264, H.265, MJPG.
.6 Support for optional onboard memory card (microSD) for backup storage, minimum Class 10, sized for minimum 72 hours video retention at full stream quality (i.e. 2MP, 30+ IPS).
.7 Where directed, IK10 vandal resistant rating.
.8 Unless otherwise directed for a specific application, all cameras shall be indoor/outdoor rated, IP66/67 rated for outdoor applications, complete with IP66/67 connectors in all outdoor applications.
.9 New cameras shall support minimum 120dB Wide Dynamic Range, unless directed or approved otherwise.
.10 All supplied devices shall be CSA/ULC listed, unless approved otherwise.

2.2 Mid-span Power over Ethernet (PoE) Injector

.1 Device Location
  .1 Should be installed in the Telecom Room or closet rack mounted, subject to input from Div. 27, else a mechanically secured and alarmed room. Shelf, bracket, or rack mountable.

.2 Wiring
  .1 Dedicated power 120Vac. RJ45 Ethernet connectors.

.3 Device Features
  .1 120VAC, 60hz operation. Provides PoE/PoE+, 30/60W full power per port, 100m data extension. IEEE 802.3af compliant. Operating temperature -20° C to +40° C.
  .2 Minimum eight (8) POE/POE+ ports.
  .3 Include a network port for remote connection and management.

.4 Application
  .1 Where a small quantity (one or two) cameras are fed from a network switch, they shall be connected to and powered from that PoE/PoE+ switch, without a separate PoE midspan.
  .2 Where three or more (3+) cameras are connected to the same switch, a multi-channel PoE/PoE+ midspan shall be installed in a mutually approved space, and cameras shall be fed from that midspan.
  .3 Any cameras which have an integral heater, and most PTZ cameras, will generally require PoE+ power supply.

*****END OF SECTION*****

1.0 GENERAL

1.1 Related UBC Guidelines

.1 Section 27 05 08 Cable Infrastructure Design Guidelines – 1.4.10
.2 Section 27 05 05 Communication Rooms Design Guidelines – 1.4
.3 Section 08 71 00 Door Hardware

1.2 Coordination Requirements

.1 UBC Energy & Water Services (Vancouver)
.2 UBC Building Operations Electrical Technical Support (Vancouver)
.3 UBC Information Technology
.4 UBC Facilities Electrical (Vancouver)
.5 UBC Facility Management (Okanagan)

2.0 MATERIALS AND DESIGN REQUIREMENTS

2.1 General Requirements

.1 The fire alarm system shall be a complete electrically supervised, single stage, non-coded addressable system. The system shall incorporate only addressable notification appliances in addition to addressable speakers if required.

The system shall be the following:
Vancouver: Simplex 4100ES series control panel, Autocall 4100ES or equivalent.
Okanagan: Edwards EST3 series or equivalent.

Equivalents will be evaluated by UBC Facilities Electrical (Vancouver) / Facility Management (Okanagan). Approval of equivalent equipment will be provided in writing by UBC Facilities Electrical (Vancouver) / Facility Management (Okanagan).

.2 All fire alarm systems must be designed by a Professional Engineer currently registered in BC.

.3 All fire alarm systems shall comply with the following standards:
.1 CAN/ULC-S524.
.2 CAN/ULC-S537.
.3 BC Building Code.
.4 Canadian Electrical Code as amended for British Columbia.

.4 Interfacing fire alarm system with BMS system.
.1 Review Section 25 05 00 Building Management System (BMS) for interfacing.
.2 Provide form C dry contact signals to BMS as applicable.
.3 The fire alarm system shall not be controlled by the BMS during a fire alarm event.

.5 Each ancillary function of the fire alarm system shall have its own independent bypass switch, (i.e. fans, door holders, security locks, bells, elevator homing, BMS, monitoring, etc.). Each switch is to be clearly labeled with LED annunciation of its normal and active positions.

.6 Commissioning/Verification

.1 At the completion of verification of the fire alarm system and before fire alarm monitoring is connected, UBC Building Operations Fire and Life Safety (Vancouver) / Facility Management (Okanagan) shall be provided with:

.1 A colour photocopy of the current red line electrical drawings.

.2 A complete copy of the Verification Report.

.3 A complete list in excel format of all field devices installed.

.4 A detailed matrix describing device inputs and outputs. Included are all smoke control sequences, FEO Service matrix and other ancillary operations.

.5 A copy of the currently installed fire alarm panel program and ES Panel Programmer Report.

.7 Any operation of the smoke control sequence of operation shall be controlled by hard wired interlocks with the fire alarm panel whenever possible. BMS control of smoke control system components shall not be permitted.

.8 Avoid nodes and networked panels in buildings where possible. One panel is preferred.

.9 Ancillary functions requiring 120VAC shall be fed from separate circuits, independent of the A.C circuit that feeds the fire alarm panel.

.10 All fire alarm system field circuits shall have connected loads/devices to a maximum of 60% of manufacturers allowable.

.11 Window actuator systems shall not be tied to the fire alarm system.

.12 FA devices in grey or black colour is not permitted. FA Devices in non standard colours shall only be considered if the surrounding finishes provide adequate contrast for ease of identification. Non standard colours must be approved by UBC Facilities Electrical.

2.2 Main Control Panel

.1 The main control panel shall be modular type, complete with all necessary plug-in modules or plug-in cards, and shall contain zone indication and all manually operated functions in the front cover behind a lockable door with viewing window. The panel shall contain enough bypass switches with a least 3 spares to provide each special system and/or ancillary system with bypass capability.

.2 The location of fire alarm control panel shall be in the Main Electrical Room.

.3 The 120VAC circuit supplying the Main Fire Alarm Control Panel shall have a surge protection device installed in or connected to a 4” square electrical box within 1m of FACP or as per manufacturer specifications. Preferred device is a Ditek DTK-120HW or equivalent.

.4 The FACP shall be fed from a 120/208V Panelboard within the same room as the control panel. Distribution Boards/Switchboards are not acceptable.

.5 The FACP enclosure shall not be used as a raceway for power or ancillary system wiring. All power and ancillary wiring within the FACP enclosure shall only be permitted when terminating (not splicing) to FAS cards and modules mounted within the FACP enclosure.

2.3 Pre-Action Control Panel for Sprinkler System

.1 Pre-action control panel for sprinkler system, if required, has the following requirements:

.1 Capable of disabling the following using a separate switch for each:
  .1 Notification appliance circuits (audible & visual).
  .2 Notification appliance circuits (audible & visual).
  .3 Releasing circuits.
  .4 Alarm, supervisory and trouble signals to base building FACP.
  .5 Ancillary equipment required by design (hatches, shutters, fans, etc.).
.2 Monitored by the base building FACP individual points for:
  .1 Releasing panel alarm.
  .2 Releasing panel supervisory.
  .3 Releasing panel trouble.
.3 Connected to:
  .1 All tamper switches on a supervisory zone.
  .2 All low air and low water pressure switches on separate supervisory zone.
  .3 All devices that monitor release on an alarm zone.
.4 If annunciation is required using a separate LED as part of a base building FACP graphic type annunciator then the releasing panel shall be networked with the base building FACP.

.2 A complete sequence of operation matrix identifying all possible input conditions and corresponding outputs shall be provided to UBC Facilities Electrical (Vancouver) / Facility Management (Okanagan) before system demonstration.

2.4 Central Fire Alarm Monitoring

.1 The Project Manager shall contact the UBC Facilities Electrical (Vancouver) / Facility Management (Okanagan) and request the UBC Fire Alarm Monitoring Installation Procedure at least 3 months before substantial completion.

.2 UBC IT Voice Services, upon receipt of valid request, will provide analog service for fire alarm monitoring at the designated service demarcation in the building. The completion timing of this service is based on the date of submission of the request for service. The designated UBC fire alarm monitoring company will be responsible to make the final connection between the monitoring equipment and the analog service demarcation point. The analog demarcation point is not to be altered or modified in any way.

2.5 Monitoring Transponder

.1 (Vancouver) UBC Electrical Technical Support shall provide monitoring equipment at the project's cost.

.2 The Electrical Contractor shall install the provided cabinet, internal stand-offs, transformer and all required conduit complete with pull strings as per UBC Standard Drawing E11-1.

.3 The transponder shall use a dedicated circuit from the same power panel as the fire alarm panel. This circuit shall not share a neutral with any other circuit.

.4 The UBC Fire Alarm System monitoring company shall install, connect, test and commission all components within the cabinet, cabling to the UBC ITS demarcation and cabling to the Fire Alarm Panel including all required terminations.

2.6 Alarm Annunciator

.1 The location of the annunciator shall be acceptable to the Authority having jurisdiction.

.2 The fire alarm annunciator shall be located on the inside of the building envelope to protect against rain and weather damage.

.3 The fire alarm annunciator shall be mounted on an insulated wall, interior wall or on standoffs to avoid cold condensation issues.

.4 The annunciator shall be manufactured by a company usually engaged for such equipment.

.5 The fire alarm annunciator shall have a keyed enable switch to avoid tampering by the public when in alarm acknowledge, supervisory acknowledge and trouble acknowledge functions.

.6 An active graphic style annunciator shall be required for buildings with 10,000 square meters of space or greater.

2.7 Other Requirements

.1 No combined type detectors will be acceptable.

.2 Each valve, switch, contact, etc. that requires connection to the FACP shall be monitored by an individual module.

.3 All remote monitor, isolator and relay modules shall be mounted in a dedicated electrical box external to the cabinet of the equipment they monitor or control with manufacturer supplied mounting brackets and covers.

.4 Door hold open devices shall be monuments rather than integrated door closure and hold open devices.

.5 Where an Emergency Generator is supplied, the Fire Alarm Control Panel and all remote Fire Alarm equipment shall be supplied with power from the Life Safety Distribution.

.6 Where an Emergency Generator is supplied, the Fire Alarm System shall monitor the Generator and Transfer Switch for any and all abnormal conditions.

.7 Beam type detectors shall be Fire Ray 5000 or approved equivalent. Approval of equivalent equipment shall be provided in writing by Building Operations Electrical Technical Specialist. (Vancouver)

.8 Aspiration type detection shall be VLP-012 VESDA LaserPLUS or equivalent. The end sampling point of each pipe run shall terminate 1m to 2m above finished floor in a readily accessible area to allow for system testing and maintenance. Approval of equivalent equipment shall be provided in writing by Building Operations Electrical Technical Specialist (Vancouver).

.9 (Vancouver) Contact UBC Building Operations Electrical Technical Support for acceptable temporary Fire Alarm Control Panel passwords.

.10 One minute inhibit shall be disabled in panel program unless required by any applicable code or standard.

.11 One minute time delay shall be active from time of AC power loss until Fire Trouble is activated.

.12 The following requirements apply to UBC Okanagan only:

.1 Commissioning should include proper verification to UBCO Campus Wide Systems (CHP and Security Firework stations)
.2 Fire system contractor responsible for insuring Omega Communications Ltd converts EST-3 signal to be able to communicate to Kelowna Fire Department. This is to be done minimum two weeks prior to verification to allow for scheduling of Omega.
.3 Fibre connections to the Campus Wide System from Library to CHP needs to be scheduled minimum 2 weeks prior to verifications with IT Services and Facilities Management.
.4 Fire system contractor responsible for updating maps on Fire Works Stations in CHP and Security.

.13 Ceiling Mounted notification appliances shall be installed in locations that are accessible with a maximum 12' ladder. Wall mounted locations shall be considered in instances where ladder access is not possible.

.14 Back boxes shall be utilized for any surface mounted pull station. Manufacturer supplied steel stamped boxes shall be utilized for interior applications and cast iron for exterior applications.

.15 Exterior Fire Alarm Devices installation requirements:
.1 Bottom Entry
.2 Weather Rated
.3 Metal Shroud: Required to be mounted such that it does not interfere with operation or maintenance of FA device or adjacent equipment. Minimum of 6" vertical clearance from device and sized with a minimum 6" extension from the outermost edges of the FA device.

2.8 Panel Manufacturer's Responsibility and Inspection Requirements

.1 Notwithstanding the Contractor's obligations, the entire fire alarm system shall be the responsibility of the panel manufacturer. Prior to acceptance of the system by the Consultant, the manufacturer shall check the entire system and certify the operation of all devices.

.2 The manufacturer shall make an inspection of the new fire alarm equipment installed under this contract, including those components necessary to the direct operation of the system such as manual stations, fire detectors and controls. The inspection shall comprise of an examination and subsequent verification of all equipment in accordance ULC-CAN4-S537. All equipment of the fire alarm system shall be listed for use with the panel manufacturer.

.1 In case of partial occupancy of a building; a partial verification of the fire alarm system may be performed. This shall not waive the requirement of a complete verification as part of the substantial completion process for the entire building when complete.

*****END OF SECTION*****