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*****