

## **1.0 GENERAL**

### **1.1 Related UBC Guidelines**

- .1 UBC Technical Guidelines
- .2 Section 17910, 17920 and 17930

### **1.2 Coordination Requirements**

- .1 UBC Electronic Systems and Secure Access (ESSA)
- .2 UBC Campus and Community Planning
- .3 UBC Information Technology

### **1.3 Description**

- .1 UBC ESSA is responsible for providing an electronic solution to the security problems of on campus, mainly theft and vandalism. The guidelines herein have been created by ESSA to clarify the design and installation process of electronic security system 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 ESSA 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 ESSA 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 ESSA standards and guidelines.
- .7 ESSA 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 UBC ESSA prior to implementation.

### **1.4 Terminology**

- .1 Access Card
  - .1 A "credit card" or "key tag" type device presented at a card reader by an authorized user.
- .2 Access Control System
  - .1 A card access system used to monitor and control occupant access into building(s) and/or area(s) thereof. The arming and locking of selected doors is scheduled and controlled electronically to allow authorized user entry via card reader, keypad etc.

- .3 Access Control Panel
  - .1 An access system's central processor that monitors access devices and governs the scheduling of all controlled and card reader doors. Can be used singly or in tandem with other panels, depending on system size.
- .4 Access Device
  - .1 Any device included in an access system that is controlled and monitored by the access control panel (i.e. card reader, RTE motion, etc.)
- .5 Alarm Control Panel
  - .1 An alarm system's central processor responsible for monitoring and reporting both system and device status.
- .6 Alarm 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.).
- .7 Alarm Keypad
  - .1 A tactile keyed, multifunction device manually operated by an authorized user typically for arming and disarming.
- .8 Burglary Alarm System
  - .1 A control system that monitors the various installed alarm devices (door contact, motion detectors, etc.) and transmits their alarm condition via modem over voice grade telephone lines. The system is enabled and disabled through devices such as keypads, card readers, or key switches where necessary.
- .9 Card Reader
  - .1 An access card recognition device, typically proximity type that allows for the entry of an authorized card holder.
- .10 Card Reader Door
  - .1 A "controlled door" that includes a card reader for authorized entry and unlocking.
- .11 CCTV Camera
  - .1 A video surveillance device designed to capture or "view" a specific area of concern and transmit a representative composite video signal.
- .12 Closed Circuit Television (CCTV) System
  - .1 A video surveillance system typically consisting of CCTV cameras, video switching, and video recording. Used for monitoring both live and recorded events.
- .13 Controlled Door
  - .1 A single door, double door, or group of doors whose locking functions are provided by system scheduled electronic locking hardware or electric strikes.
- .14 Door Position Contact
  - .1 A sealed magnetic reed contact that monitors a door's open/close position.
- .15 Duress ( Panic ) Button
  - .1 A push button device that requires manual activation by an occupant under duress.
- .16 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.

- .17 Electric Strike
  - .1 An access control door strike designed as a replacement for a regular strike plate that is controlled electro-mechanically.
- .18 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.
- .19 Hardware Egress
  - .1 A dry contact included within a controlled or card reader door's egress hardware to monitor occupant egress.
- .20 Monitored Door
  - .1 A single door, double door 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.
- .21 Monitored (Secured) Area
  - .1 A protected area, in whole or in part, within a secured perimeter.
- .22 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.
- .23 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.)
- .24 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.
- .25 Request to Exit (RTE) Motion
  - .1 A motion detector installed at a controlled or card reader door to monitor occupant egress.
- .26 Siren Horn
  - .1 An audible device triggered to sound during an alarm condition.
- .27 Video Switcher/Multiplexer
  - .1 A "rack mount" or "counter top" video component designed to route multiple video signals typically from camera to video monitor and/or video recorder.
- .28 Video Recorder:
  - .1 A "rack mount" or "counter top" video component designed to record and playback video images.
- .29 Video Monitor
  - .1 A "rack mount" or "counter top" video component with viewing screen designed for the monitoring of live and/or recorded video images.

## **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 ESSA for all contemplated changes.

### **2.2 UBC Procedure**

- .1 Campus and Community Planning shall facilitate the communications and efforts of the contractor with UBC Information Technology and ESSA.

### **2.3 System Design**

- .1 The security system shall be designed by UBC ESSA. If designed by a consultant, the designer shall be approved by UBC ESSA.

### **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 Commons rooms.
  - .4 Communication lines (telephone or LAN) .
  - .5 Preparation of door frames, doors, walls, ceilings, etc., to accept security devices and hardware.
  - .6 Fire Alarm interface.
  - .7 Elevator control interface.
  - .8 Door hardware power.

### **2.5 System Installation**

- .1 All alarm (Section 17910), access (this section), and CCTV security system (Section 17920) installation work shall be performed by UBC ESSA. If under special circumstances, security installation is to be contracted out to outside companies, the contractor must be acceptable to UBC ESSA. The contractor must use provincially trade qualified technicians who individually have a minimum of five years commercial installation experience.
- .2 Based on the above criteria, UBC ESSA will pre-approve contractors for performing security work at the University. Poor performance may revoke pre-approval of an installation contractor.

### **2.6 System Verification**

- .1 System verification shall be performed by UBC ESSA. 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 ESSA will be installing the 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 a security system the University requires that the consultant or contractor supply ESSA with design and installation details in the form of shop drawings.
- .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 UBC ESSA RESPONSIBILITIES

### 3.1 General

- .1 UBC ESSA 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 through UBC Information Technology liaison.

**Note 1:** For projects not managed by Campus and Community Planning, NF involvement may not be required. In such cases, ESSA shall deal directly with the UBC department and/or building occupant.

### 3.3 System Design

- .1 Design, coordinate, and/or supervise the design of on campus security systems through UBC Information Technology liaison.

### 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.) through UBC Information Technology liaison.

See **Note 1** above.

### 3.5 System Verification

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

See **Note 1** above.

### 3.6 Post Installation

- .1 Service, maintain, and manage each and all of the electronic security systems on campus as per ESSA's contractual agreement with individual departments and/or building occupants.
- .2 Arrange with the department and/or building occupant for the issuance of cards, the development of the access privilege database, user training, etc.
- .3 Arrange for the preparation of as-built drawings of the completed installation, including wiring schedules.

**Note:** UBC Information Technology involvement with any and all security projects on campus concludes after successful system verification.

### 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 and system verification. This shall apply equally to new installations, upgrade and renovations at UBC. Where contradictions are found between the referenced standards and this document, this document shall prevail.
  - .1 UBC ESSA Guidelines.
  - .2 UBC Technical Guidelines incorporating Division 17 - Information Technology.
  - .3 BC Electrical Code.
  - .4 BC Fire Code.
  - .5 BC Building Code.

## 4.0 SYSTEM DESIGN

### 4.1 General

- .1 System design shall be based on two primary considerations; function and application. Both will vary depending on building structure and occupant concern. Despite the inevitable variance, basic requirements shall be followed to ensure Campus wide compliant.

### 4.2 Function

- .1 The following functional requirements shall be identified prior to the design of any security system to be installed on Campus:
  - .1 Number and location of accessible perimeter doors.
  - .2 Number and location of entrances/exits (daytime and after hours).
  - .3 Number and location of disabled access points.
  - .4 Number and location of vulnerable interior spaces.
  - .5 Number and location of arm/disarm devices.
  - .6 Number and location of special areas (computer labs, animals, 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 design of any security system on campus:

- .1 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.
- .2 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.
- .3 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, functionality and anticipated or actual pedestrian traffic into and through the building.
- .4 Interior Devices
  - .1 Ground floor areas or areas within a building that are considered to be "reasonably accessible" from the building exterior shall include the installation of a detection device (i.e. motion sensor, glass-break sensor, photo-beam, or other applicable devices).
- .5 Arm/Disarm
  - .1 System arming/disarming shall be provided on a "per zone or per area" basis via keypad, card reader or combination thereof.
- .6 Monitoring
  - .1 System monitoring shall be provided via UBC Information Technology voice grade phone service or campus LAN.