1. **GENERAL**
   1. **Coordination Requirements**
      1. BCIT Safety, Security and Emergency Management (SSEM).
      2. BCIT Facilities and Campus Development (FCD).
      3. BCIT Information Technology Services (ITS).
      4. Division 08 Openings
   2. **Description**
      1. BCIT SSEM supports BCIT’s strategy to provide a safe and healthy environment for our employees, students, and for the communities where we live and operate. The guidelines herein have been created by SSEM to clarify the design and installation process of electronic safety and security systems on the BCIT campuses.
      2. The guidelines are intended to foster cooperation between all parties involved whether they be BCIT 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 SSEM remain flexible in the implementation of BCIT 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 SSEM 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 SSEM standards and guidelines.
      7. SSEM is the BCIT group solely responsible for the consultation, design installation, verification, maintenance, and management of all electronic safety and security on campus.
      8. Any and all proposed changes to these standards shall be subject to approval in writing by BCIT and SSEM prior to implementation.
   3. **Terminology**
      1. *Access Control System (ACS)* - A card access system used to manage and control access to BCIT spaces. Some areas on campus are locked/unlocked on a programmed schedule to allow free access without the use of a card reader. Other areas on campus are armed/disarmed on a programmed schedule to allow access via the use of an electronic access card, without the need for a cardholder to have access to arming/disarming functions (card commands).
      2. *Access Control Panel (ACP)* - One or more access control system processors or add-on circuit boards that manage the connected access devices. This includes the intelligent controller itself and any associated door controllers, input controllers, output controllers, elevator controllers, etc.
      3. *Access Device* - Any device included in the Access Control System that is connected to and managed y the Access Control Panel (i.e. card reader, motion REX, glass break sensor, passive infrared sensor, etc.).
      4. *Access Card* - A proximity or magnetic stripe credential read by a card reader that provides access to a given area or performs functions as programmed into the Access Control Software.
      5. *Card Command* - A special command issued to a Card Reader, before a valid Access Card is presented, which executes a programmed set of instructions (i.e. arm all sensors and lock the door).
      6. *Access Control Software* - A scalable access control and security management solution that manages access, processes alarms, and produces reports from a central location.
      7. *Card Reader* - A device mounted near a controlled door which recognizes an Access Card (proximity or magnetic stripe), and allows entry to an authorized card holder or a programmed function to occur by way of a card command.
      8. *Electronic Locking Hardware* - Access control door hardware, typically “cylindrical”, “mortise”, or “panic”-type that is aesthetically identical to regular hardware and whose locking function is controlled electro-mechanically.
      9. *Electric Strike* - An access control door strike designed as a replacement for a regular strike plate that is controlled electro-mechanically.
      10. *Full Card Reader Door* - A single or double door that includes a card reader for access and intrusion functions, as well as electronic locking hardware and a door contact, and connected to an access control panel.
      11. *Request to Exit (REX) Motion* - A motion detector installed on the secure side of a secure space.
      12. *Request to Exit (REX) Switch* - A mechanical switch integrated into electronic locking hardware which serves to monitor an occupant’s egress.
      13. *Intrusion Detection System* - The combination of a full card reader door and monitor points connected to an access control panel which communicates their status to the access control software for a monitored response. The system is able to be armed or disarmed via the use of a card reader at a door to the secure space, or independently managed via the access control software.
      14. *Door Contact* - A sealed magnetic contact that monitors a door’s open or closed position.
      15. *Passive Infrared Sensor (PIR)* - A spatial protection device used to detect movement within a secured area by monitoring changes in microwave and/or infrared field patterns.
      16. *Glass Break Sensor (GBS)* - A device containing a microphone which is triggered by a loud noise indicating potential glass breakage.
      17. *Closed Circuit Television (CCTV) System* - A video management system that consists of cameras, computer servers, and software which manages live and previously-recorded video.
      18. *Mid-span Injector* - A device that provides inline PoE/PoE+ to a structured data run.
      19. *Secure Space* - An enclosed room that is accessed by at least one full card reader door, with any non-full card reader doors into or out of the room fit with a door contact.
      20. *Secure Side* - The area within the protected perimeter of a secured space to which a person must be authorized to enter.
      21. *Video Management System (VMS)* - A video management system is a component of a security camera system that collects video from cameras, records / stores that video to a storage device, and provides an interface to both view the live video and access recorded video.
2. **CONTRACTOR and/or CONSULTANT RESPONSIBILITIES**
   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 Institute in writing of any contemplated exceptions and obtain approval from SSEM for all contemplated changes.
      2. Software licences are to be provided by BCIT’s current maintenance contractor.
   2. **BCIT Procedure**
      1. FCD shall facilitate the communications and efforts of the contractor with SSEM.
   3. **System Design**
      1. The security system shall be designed through consultation with and approval by SSEM.
   4. **System Infrastructure**
      1. FCD and the project architect/engineer must ensure that the contractor provides the correct security infrastructure for the building. This infrastructure shall include:
         1. Cable pathway.
         2. Security panel power and space allocation in communication rooms. When generator/emergency power is present in a communication room, the ACP shall be tied to a dedicated emergency power circuit.
         3. Installation of conduit and junction boxes (JB) where required. Provide 1” EMT conduit for each door (with pull string) from the Access Control System cabinet (typically in the nearest communications room) to a 4”x4” JB located on top of the secure side of the door.
         4. Installation of ½” EMT conduit (with pull string) from the 4”x4”x JB located above the door to all access control devices for each door (card reader, door contact, transfer hinge, PIR, GBS, etc).
         5. Communication lines (Network, coordinated with BCIT ITS) to be installed in a data outlet beside the security panel. A conduit path from the JB to the communications rack must be provided.
         6. Preparation of door frames, walls, ceilings, etc to accept security devices and hardware. If doors are to be fitted with electrified mortise, doors must be prepared to accept an electrified mortise with transfer hinge.
         7. Fire Alarm Interconnect where required (i.e. for Maglock-type doors).
         8. Dedicated 120V AC circuit to power door hardware and access control panel.
         9. Plywood backing, when required, to ensure the LifeSafety cabinet is securely fastened to the wall, dimensions 1219 mm H x 1016 mm W (48”H x 40”W).
      2. All safety and security system cabling will be installed in conduit unless a cable tray is present. The use of J-hooks is permitted, as needed, when cables are run above ceiling tiles.
   5. **System Installation**
      1. All electronic access control and CCTV system equipment final connections and system programming are completed by the SSEM contractor who holds the current maintenance agreement. The contractor must use technicians qualified in the specific VMS or Access Control Software. Before electrical work commences for the access control system and the monitor points, a walk-through will be required to finalize the location of all devices.
   6. **System Verification**
      1. System verification shall be performed by SSEM. The contractor must ensure and coordinate through FCD the verifications 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.).
   7. **Contract Documents**
      1. Facilities and IT Services project standards are to be met.
   8. **Shop Drawings**
      1. Before commencing with the installation of an electronic access control project, SSEM requires that the consultant or contractor supply BCIT and SSEM with design and installation details in the form of shop drawings (i.e. proposed door hardware, cable and conduit path, location of sensors, etc.). The shop drawings must be approved by BCIT and SSEM to ensure it meets the needs of the Institute/Occupants/end-users.
      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. **SSEM RESONSIBILITIES**
   1. **General**
      1. SSEM 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 Institute guidelines, and provide basic end-user training.
   2. **Consultation**
      1. Consult, coordinate, and/or supervise the consultation of on-campus security systems.
   3. **System Design**
      1. Design, coordinate, and/or supervise the design of on-campus security systems.
   4. **System Installation**
      1. Coordinate activation of Network VLANs and installation of network drops for safety and security systems with ITS Department.
   5. **System Verification**
      1. Verify, coordinate, and/or supervise the verification of on-campus security systems (including related equipment).
   6. **Post Installation**
      1. Create service tickets for the contractor who holds the current maintenance agreement unless the failure of a hardware component is covered under warranty with the original installer.
      2. Receive the updated floor plans and project drawings to be copied on the SSEM network share**.**
4. **SYSTEM DESIGN**
   1. **General**
      1. The system design shall produce a consistent outcome to increase safety and security for the Institute, reduce risk, and enable access. SSEM provides consultative input to project teams and user stakeholders to ensure the successful application of security technology with operational requirements.
   2. **Operational Function**
      1. The following functional requirements shall be identified prior to the design of any security system to be installed on a campus:
         1. Space ownership and usage.
         2. Location of all perimeter doors.
         3. Location of primary entrances/exits (daytime and after hours).
         4. Identification of entrances/exits with a handicap operator.
         5. Identification of special areas (i.e. containing high-value assets, chemical storage, etc.).
         6. Building hours of operation.
         7. Desired scheduled operations (i.e. automatic locking, unlocking, etc.).
         8. Location of vulnerable personnel.
   3. **Application**
      1. The following requirements shall be included in the consideration and design of any security system on campus:
         1. Monitored Doors
            1. All building perimeter doors shall be monitored with the use of a door contact and be mechanically locked to prevent entry at all times, with the exception of full card reader doors.
         2. Full Card Reader Doors
            1. Depending on building requirements, selected doors will be designated as card reader doors to be electrically locked/unlocked on a time schedule basis. At least one door 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, and space ownership and functionality.
         3. Intrusion Devices
            1. Areas within a building that are accessed via card access will include the installation of a detection device such as a PIR that is armed/disarmed via a card command issued to the card reader that gains access to the secure space.
            2. Areas within a building that is “reasonably accessible” from the building exterior will include the installation of a detection device such as a GBS (i.e. a ground-level room with a window), or a PIR (motion) sensor will be installed in a way that does not detect movement outside the door/window (ie: the PIR does not face the door of the secure space.
            3. PIR sensors are not installed in rooms designated as “communication rooms” for the reason that air currents generated by network equipment and air conditioning units would result in false alarms being generated.
         4. Arm/Disarm
            1. System arming/disarming will be accomplished using one or more card readers that lead into the secure space.
         5. Monitoring
            1. Access Control System Monitoring shall be performed by the SSEM Security Services Provider
         6. Access Control Panel Location
            1. Card reader doors and detection devices will be controlled by an access control panel located on the same floor as the card reader/detection device. Typical access control panel locations are in a room designated as a “communications room”. The exception to this is if there is no communications room located on the same floor as the card reader (i.e. a card reader that provides roof access would be unlikely to have a communications room on the roof. In such case, the wiring for the full card reader door can be run down to the communications room one floor lower.
         7. Handicap / Automatic Door Operator (ADO)
            1. In the event an ADO is being installed and the door is to be connected to a card reader, the door must be fit to accept an electric strike in addition to the electrified lockset. Upon pushing the handicap door operator button, the signal is intercepted to unlock the electrified strike and allow the door to open. This requires consultation between the ACS integrator and the ADO operator to ensure appropriate relays are installed in the ADO.
5. **EQUIPMENT SPECIFICATIONS**
   1. **General**
      1. The following list of equipment defines the current standards in use at the Institute as well as the intended purpose:
         1. Access Control Panel
            1. Product:

Amag Symmetry Multinode M2150-8DBC, Purpose: Access control panel intelligent controller.

Amag Symmetry Multinode M2150-8DC, Purpose: Access control panel door controller.

Amag Symmetry Multinode M2150-4DC, Purpose: Access control panel door controller.

* + - * 1. Device Location

ACP to be mounted in the nearest communications room on the same floor as the card reader(s) being installed. Exact location to be confirmed by SSEM. If it is not possible to mount the ACP in a communications room, it should be mounted in a secure room within the protected area. New installations must have enough room to install a LifeSafety cabinet as defined later in this document.

ACP and expansion boards must not be mounted above ceiling.

* + - * 1. Raceway

Power transformer fed from 120VAC dedicated circuit c/w generator and/or UPS backup whenever possible.

* + - * 1. Cabling

All related wiring for panels should be concealed and home-run whenever possible. FT6 rated cable required.

Wire path and dressing within communication rooms to conform to BCIT IT Services standards.

* + - * 1. Device Features

ACP housed in a mechanically securable keyed box c/w tamper switch.

Wall mountable, minimum 8 reader ports.

* + - 1. Card Reader
         1. Product

Amag S849 Contactless Smart Card Reader, Purpose: Card reader.

* + - * 1. Device Location

Card readers are installed between 900 mm and 1100 mm AFF as per BCBC 3.8.3.6. (6) and (7).

* + - * 1. Cabling

Product: Noramco 42GA2203, Purpose: Multi-pair stranded foil shield FT6 cable for card reader.

* + - 1. Door Contacts
         1. Product

Flair MSS100-7 WHT, Purpose: Balanced door contact in 1” size, recessed.

Flair MSS100-17 WHT, Purpose: Balanced door contact, 3 ¾” size, surface mount.

* + - * 1. Device Location

Frame: Flush-Mounted concealed contact to be installed in the top of the door frame.

Door: concealed magnet should sit no more than 13mm away from contact with the door in a fully closed position.

A double door which is fit with electrified hardware may have the door contact installed on the side of the door (as opposed to the top) to allow for the opening of either door to be monitored using a single door contact.

Any double doors that use panic hardware will have both door leaves wired for electrified hardware.

* + - * 1. Cabling

Product: Noramco 42LA2204, Purpose: Multi-conductor Station-Z FT6 cable for REX and door contact.

* + - 1. Electrified Hardware
         1. Product

Schlage L9092-EU-RX (Standard trim 03), Purpose: Electrified mortise, fail secure with REX.

Product: Schlage ND96PDEU-RX (Finish 626), Purpose: Electrified cylindrical lock, fail secure with REX.

* + - * 1. Cabling

Product: Noramco 42AA1802, Purpose: Multi-conductor stranded FT6 cable for lockset.

* + - 1. Miscellaneous Hardware Specifications
         1. Product

Product: Amag Symmetry MN-NIC-4-ENC, Purpose: Access control panel encrypted network interface card.

Product: Amag Symmetry M2150-AC8/4, Purpose: Access control panel input and output module.

Product: Amag Symmetry M2150-AC24/4, Purpose: Access control panel input and output controller.

Product: Amag Symmetry M2150-OC4/24, Purpose: Access control panel input and output controller.

Product: LifeSafety Power FP0150/250-2C82D8E8A, Purpose: Power supply and cabinet for access control panels.

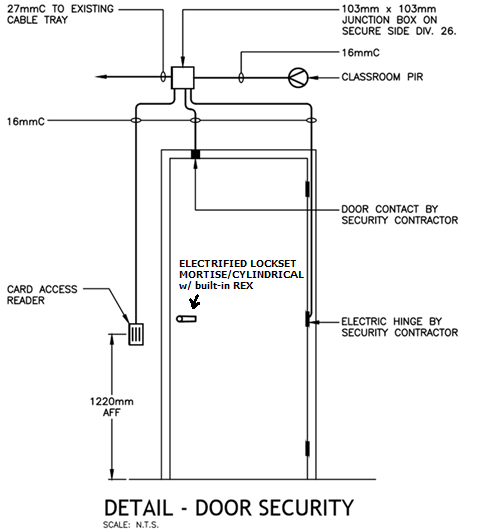
Product: Bosch DS936 PIR, Purpose: Ceiling mount low profile panoramic PIR detector.

Product: Bosch Blue Line Gen2 PIR, Purpose: Wall or corner mount motion detector.

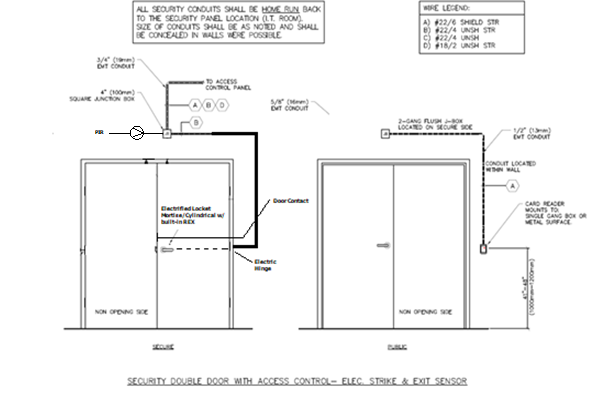
Product: Honeywell FG-730/FG1625 GBS, Purpose: Dual technology glass break detector.

Product: Command Access ETH8WH (Wire QTY 6-10, wire gauge 28), Purpose: Electrified hinge, 5 knuckle heavy weight, 4-1/2”x4” (typical).

1. **DOOR PREPARATION SPECIFICATIONS**
   1. **Single Door Diagram**

****

* 1. **Double Door Diagram**

****

\*\*\* END OF **ACCESS CONTROL - SYSTEM HARDWARE** SECTION \*\*\*