DALHOUSIE UNIVERSITY

Div 28 - Electronic Safety and Security Guidelines 2025 02 13 (1)

Table of Contents

Div 28 - Electronic Safety and Security Guidelines 2025 02 13 (1)

Dalhousie University Design Guidelines provide assistance to consultants during the planning and design phases of the University's expansion and renovations. The Guidelines do not relieve a consultant from any professional responsibility, duty or due diligence to design elegant, functional, efficient and low maintenance facilities.

Facility owners have preferred materials and requirements that make the task of maintaining facilities less costly. Dalhousie understands this is a balance between capital and operating cost. The Guidelines are not intended to be the only acceptable solution. Dalhousie expects consultants to bring modern and innovative ideas, materials and methods to the University. If these Guidelines do not allow these new ideas, then the consultant is to make a request in writing to the Dalhousie project manager for an exception to the guidelines. Necessary reasoning and or calculations shall accompany the request. The exception request will be reviewed internally and either rejected or accepted. The consultant will document this rational and/or justification for each exception in the Basis of Design. The University Guidelines may be updated subsequently.

These documents provide design guidelines only, and are not intended for use, in whole or in part, as a specification. Do not copy the guidelines verbatim in specifications or in notes on drawings. Refer questions and comments regarding the content and use of these documents to the Dalhousie project manager. The Guidelines are intended to be read in conjunction with the local codes and regulations, and in no way are to be considered as a code replacement. The codes and regulations represent the minimum acceptable standard. Where the technical design requirements differ from the building codes and other applicable codes and standards, the more stringent of the codes shall be applied.

Maintaining the Standards/Guidelines

The Design Guidelines are created and maintained by Dalhousie's Facilities Management department. Any enquiries about the Guidelines should be directed to Facilities Management, Director of Projects, Central Services Building. Dalhousie encourages design specialists and other interested parties to provide their input and suggestions based on their experience.

Div 28 - Electronic Safety and Security Guidelines 2025 02 13 (1)

ELECTRICAL CONSULTANT COMPLIANCE CHECKLIST

General Requirements

		C	NC	NA
1.	Warranties			
2.	Energy Efficiency			
3.	Efficiency Nova Scotia Rebates			
4.	Equipment Isolation			
5.	Placement of Equipment and Equipment Access			
6.	Abbreviations and Definitions			

Division 28 – Electronic Safety and Security		C	NC	NA
28 10 00	Access Control			
28 13 27	Security Door Supervision			
28 13 28	Building Entrance Control System			
28 14 00	Access Control System Hardware			
28 23 00	Video Surveillance			
28 31 00	Intrusion Detection			
28 31 00.01	Multiplex Fire Alarm System			
28 31 00.02	Multiplex Fire Alarm and Voice Communication Systems			
28 31 00.03	Duress Alarm System			
28 46 00	Fire Detection and Alarm			

(C – Compliant; NC – Non-Compliant; NA – Not Applicable)

The Engineer has verified the existing building systems are adequate for additional capacity noted above

_____

Consultant Name Consultant Signature Date YYYY MM DD

_____

Project Manager Name Project Manager Signature Date YYYY MM DD

Note: If the Guidelines or part of cannot be attained or fulfilled (i.e. NC or NA) during the design process, the consultant should provide reason(s) why such Guidelines are not met. Any modification or alterations to the design guidelines will need to be agreed/accepted by Facilities Management prior to inclusion in the design.

General Requirements

1. **Warranties**

1.1. Standard 12 month warranty for a project begins at Substantial Performance. Systems and or equipment that is not considered complete at the time of the project's (or trade's) Substantial Performance shall be noted as such on the Substantial Performance Certificate's Punch List. Warranty for this equipment (or system) shall be one year from the date upon which it is removed from the Punch List.

1.2. Extended warranties are available for many pieces of equipment and/or products from the manufacturer at no cost. Dalhousie requires suppliers/manufacturers to provide such extended warranties directly to the owner in the name of Dalhousie University. A list of such warranties will be reviewed with the owner at time of shop drawing submission.

1.3. The designer shall recommend any extended warranties (including labour) and/or service agreements to the owner. In all cases, these shall be listed as alternative prices to the base project on the bid form.

2. **Energy Efficiency**

2.1. Variable speed drives should be used for all 3 phase motors that would traditionally require a starter. Specification must state that the associated rebate is to be payable to the University.

3. **Efficiency Nova Scotia Rebates**

3.1. Energy efficiency must be considered and equipment specifications must align with those identified by Efficiency Nova Scotia as eligible for Business Energy Rebates. The rebates include but are not limited to the following categories:

- Hot Water Heating
- Variable Speed Drives
- Lighting
- Transformers

The specifications identified by Efficiency Nova Scotia are available on their website https://www.efficiencyns.ca/business/products/.

The designer shall specify that that the owner will be applying for all applicable efficiency rebates, through Efficiency NS, in collaboration with the successful proponent. The owner will receive these rebates directly. The successful proponent will not apply or receive any manufacturer's instant rebates for any products provided through the project.

4. **Equipment Isolation**

4.1. All equipment shall be able to be individually electrically isolated.

5. **Placement of Equipment and Equipment Access**

5.1. As necessary the designer shall summarize all work necessary to place equipment or systems into existing spaces. Including but not limited to wall removals, door removals, special cranes, knock down equipment.

5.2. The ability to service equipment, including necessary permanent platforms, shall be reviewed with the project manager as part of the shop drawing review/approval. Exceptions to the manufacturer's recommended clearance requirements shall be identified during the shop drawing review/approval stage by the designer.

5.3. The internal dimension of all access doors and panels must be a minimum of 12" x 18". Access doors shall be hinged with a positive locking mechanism.

5.4. Equipment shall not be placed closer than 3 meters (2 meters from the roof edge plus 1 meter for servicing room) from the edge of any roof. If this is not possible, appropriately engineered barriers shall be provided.

5.5. Equipment should be located with consideration of snow accumulation, entry into equipment and removal, as well as protected from university snow removal operations. Where snow accumulation is inevitable, the designer is to complete a structural analysis.

5.6. Equipment to be placed on the roof must include a detailed drawing of sleepers, penetrations, etc. It is the responsibility of the designer to ensure the detailed drawing is signed off by a qualified roofing professional and ensure roof warranties are not voided by works carried out.

6. Abbreviations and Definitions

Access Control System (ACS): an electronic system that allows, restricts and tracks the movement of people through entry/exit points in a site, usually achieved through programmable electronic keys, cards with readers.

BFDO: Barrier Free Door Operator: Power door operator supplied and installed by the door hardware contractor, wired by the electrical contractor.

CX-33 Module: Smart relay interface module used when barrier free door operators are used in conjunction with door access control.

DC - Door Contact: Magnetic door contact flush mounted in door frame at top of door. Provide a 1" diameter hole in door frame for installation of door contacts located 3" from edge of door, opposite the hinge. Door contacts supplied, installed, wired and terminated by the electrical contractor. Contacts shall be equal to GE Interlogix 1078W series normally open magnetic contacts.

DH - Door Hold Open Device: Upon activation of a command (fire alarm, time of day schedule) the door hold open device shall release, allowing the door to close. Door hold open devices may be integrated into door closer or wall mounted. Door hold opens shall be tied into the fire alarm system, wired and terminated by the electrical contractor. Where door hold open devices are required to be tied into the access control system, low voltage hold opens are preferred.

EH - Electrified Transfer Hinge: Electrified hinge allows for transfer of power and signals to door mounted devices. Supplied and installed by the door hardware contractor, wired and terminated by the electrical contractor.

ES - Electric Strike: Electric door strike shall be mounted on the door frame, supplied and installed by the door hardware contractor, wired and terminated by the electrical contractor with a required 12V version. In doors equipped with barrier free door operators, whereas the operator has the capability of providing power to an electric strike, the voltage of the strike needs to be determined from door operator product literature.

ELCK - Electrified Lock: Electrified lockset complete with integrated door contacts and request-to-exit, mounted on door, supplied and installed by door hardware contractor, wired and terminated by the electrical contractor. Electrified locks available in 12V or 24V.

The 12V version shall be preferred as the Access Control system operates at 12V. When requiring 24V electrified locks, a separate 24V power supply must be installed.

ELR - Electric Latch Retraction: Electric latch retraction complete with request-to-exit, mounted on door, supplied and installed by door hardware contractor, wired and terminated by the electrical contractor. A separate power supply must be provided as per the manufacturers door hardware specifications and installed with the distance limitations as per specification.

Elevator control sequence - Floor Tracking: Limits access to specific floors and tracks personnel's travel throughout facility.

Elevator control sequence - Restricted USER Access: Limits access to elevator for authorized personnel and does not prevent floor to floor access on any restricted floors. A simple system to ensure only authorized personnel use the elevator and have full access to the facility.

Intrusion Alarm System (IAS): a system designed to detect unauthorized entry or activity in a building or area. They consist of an array of sensors, a control panel and alerting system, and interconnections.

Input Module: Connects alarm inputs to the access control system, Genetec cat. # MR16IN, supplied, installed, wired and terminated by the electrical contractor. Each input module is capable of controlling up to 16 alarm inputs.

Intelligent Controller: Handles access control decisions and monitors activity, connects to and report real-time events over any IP network, Genetec cat. # EP2500, supplied, installed, wired and terminated by the electrical contractor. Each intelligent controller is capable of managing 32 downstream interfaces (eg. Reader modules, input modules, and output modules) over RS-485 communications cabling.

JB - Junction Box: Similar to a 10"x10"x6" Hoffman cat. # AA-10N106, mounted within 6" of the underside of the ceiling in accessible ceiling space on "secure" side of door. In areas without ceilings, the junction box shall be installed 8'-0" to the bottom of the junction box. Maximum cable length between junction box and card reader shall be 15'-0". Provide and install a #6 AWG insulated copper bonding conductor from junction box to nearest bond bus.

Maglocks: Electromagnetic locks are prohibited.

Multi-technology Reader: Schlage cat. # MTB15 multi-tech mounted on a single gang backbox flush wall mounted at 42" A.F.F., supplied, installed, wired and terminated by the electrical contractor. Where requiring mullion mount, proximity card reader shall be equal to Schlage MTB11. **Typical device used for most interior doors**.

Multi-technology with PIN pad: Combination reader complete with integrated PIN pad, Schlage cat. # MTKB15, mounted on a single gang backbox flush wall mounted at 42" A.F.F., supplied, installed, wired and terminated by the electrical contractor. **The PIN pad must be installed on all exterior card reader doors**.

Schlage (AD350 Wired or AD400 Wireless via RS-485 PIM): Both require a com port dedicated to Schlage devices on a Mercury controller. Schlage devices cannot be mixed with other devices on a Mercury controller com port. Electrified lockset complete with integrated multi-technology card reader, door contact and request-to-exit, mounted on door, supplied and installed by door hardware contractor, wiring and termination by the certified security alarm contractor.

Network Controller: Allows IP-based management of access control system, Genetec Synergis Cloud Link, supplied, installed, wired and terminated by the electrical contractor. Each network controller is capable of managing 256 card readers and electronic locks, as well as monitor events and alarms and provide reporting.

Output Module: Connects output devices or relays controlled by contact closures to the access control system, Genetec cat. # MR16OUT, supplied, installed, wired and terminated by the electrical contractor. Each output module is capable of controlling outputs for up to 16 devices or relays.

PB - Barrier Free Door Operator Push Button: Barrier free door operator push button, supplied and installed by the door hardware contractor, wired and terminated by the electrical contractor at 36" A.F.F.

P/S - Power Supply: Power supply for electrified locks, electric latches, electric strikes, and door hold open devices. Supplied by the door hardware contractor, installed, wired and terminated by the electrical contractor. In facilities equipped with emergency power, all power supplies to be fed from an emergency source.

P/S(ACS) - Access Control System Power Supply: Power supply for access control system components, complete with battery backup. Supplied, installed, wired, and terminated by the electrical contractor. In facilities equipped with emergency power, all power supplies to be fed from an emergency source.

Reader Module: Handles access control decisions at the secured at door equipped with a card reader, Genetec cat. # MR50, supplied, installed, wired and terminated by the electrical contractor. Each reader module is capable of managing 1 card reader. A reader module that can manage 2 card readers is also available but is less preferred.

RTE(EX) - Request-to-Exit in Exit Device: Request to exit device integral to the door hardware exit device or electrified lock. Wiring and termination by the electrical contractor.

RTE(IR) - Infrared Request-to-Exit Device: Infrared request-to-exit device equal to Kantech T.Rex Series, Cat. No. T.TREX-LT2 complete with T-REX-PLATE for mounting over a standard device box, supplied, installed, wired and terminated by the electrical contractor. Device to be mounted above the door frame opposite the latch side of the door as per the manufacturer's recommendations. Coordinate the exact location with site conditions.

Remote Video Surveillance System (RVSS): refers to a system or device that enables continuous or periodic video recording, observing or monitoring of activities in University controlled spaces. Monitoring of this system is at a distant location.

Security Services Command Center: refers to the center of Security Services operations, located in the McCain Building. This center is continuously staffed under the direction of a Shift Supervisor. This Command Center may be relocated to an alternate location due to an emergency event.

SSV - Security system video: The term used to identify the network of IP video devices and cameras throughout campus.

28 10 00 Access Control – Application guideline

1. **Access Control - Building Perimeter:**

   Applies to:

   i) building perimeter doors,

   ii) doors separating Dalhousie occupied portions of a building from public areas or from areas under the control of an outside entity (e.g. in a building not owned by Dal, separating space rented by Dal from other building spaces).

   1) All building perimeter doors will be equipped with a door contact (DC) and request to exit (REX) device, which will allow the door position to be monitored by Dal Security through the campus Access Control System (ACS).
   2) All building perimeter entrance doors will be equipped with an electric locking mechanism controlled by the ACS, to allow the doors to be locked and unlocked automatically on a predetermined schedule by the ACS. The electric locking mechanism will have a manual keyed over-ride feature, which is reserved for the use of Dal Security.
   3) The building “main” entrance will have one door equipped with a Proximity Device (Prox) card reader & PIN pad connected to the ACS, and an automatic door opener. Other building entrance doors will not have a card reader and PIN pad installed unless approval is given by Dalhousie's Director of Security Services.
   4) The building administrator may request that specific building perimeter door locations ** be equipped with an audible and visible alarm (siren/strobe pair) initiated by the ACS for any unauthorized opening of the doors in that area (i.e. door forced open & door held open).
   5) Exit only doors will have a manual keyed lock, which is reserved for the use of Dal Security, and will be locked from the outside at all times.

   ** Note: A "door location" means an area within easy sight and hearing range of single siren/strobe pair such that alarm output(s) for one or more doors in that area may use the same pair of devices as their audible and visible alarm devices.

2. **Access Control - High Security Areas:**

   Applies to high security areas within a building (e.g. animal care areas; regulated areas requiring maximum security such as research reactors or Biohazard Level 3 labs).

   1) All perimeter doors of a high security area will be equipped with a DC and request to exit REX device, which will allow the door position to be monitored by Dal Security through the campus ACS.
   2) All entrance doors of a high security area will be equipped with a Prox card reader & PIN pad connected to the ACS, and an automatic door opener where necessary.

3) The area administrator may request that specific perimeter door locations ** be equipped with an audible and visible alarm (siren/strobe pair) initiated by the ACS for any unauthorized opening of the doors in that area (i.e. door forced open & door held open).
4) Exit only doors will have a manual keyed lock which is reserved for the use of Dal Security and will be locked from the outside at all times.

3. **Access Control - Administrative or Academic Spaces:**

Applies to:

i) doors of large common pool auditoriums/teaching labs,
ii) large office suites,
iii) doors separating building spaces which have different functional uses and user groups (e.g. separating student commons or residential space from food service or administrative space; separating a building atrium with food services from academic space; separating one faculty's space from another; etc).

1) All perimeter doors of an access-controlled space must have a door contact (DC) and request to exit (REX) device to provide door position monitoring through the campus ACS by Dal Security.
2) All entrance doors must have an electric locking mechanism controlled by the ACS, to allow the doors to be locked and unlocked automatically on a predetermined schedule by the ACS. The electric locking mechanism must have a manual keyed over-ride feature.
3) One door at each entrance location will be equipped with a Prox card reader connected to the ACS and an automatic door opener.
4) The building administrator may request that specific perimeter door locations ** be equipped with an audible and visible alarm (siren/strobe pair) initiated by the ACS for any unauthorized opening of the doors in that area (i.e. door forced open & door held open).
5) Exit only doors will have a manual keyed lock which is reserved for the use of Dal Security and will be locked from the outside at all times.
6) Department controlled classrooms/labs/seminar rooms, individual offices, storage areas, etc. will generally not have access control equipment installed on the entrance doors. In certain instances (e.g. where an area or room is frequently accessed by many people, or where it is important to identify who has entered the space) the Dept may request that the entrance be equipped, at its expense, with a Prox card reader connected to the ACS.

Note: The project manager will identify the doors that require access control.

4. **Access Control - Building Services Spaces:**
   Applies to main mechanical/electrical/telecom rooms, service tunnels, mechanical penthouses, rooftops.

   1) The entrance door will be equipped with a Prox card reader connected to the ACS, and the electric locking mechanism will have a manual keyed over-ride feature. (Note: the card reader will be installed on the building side of a service tunnel entrance).
   2) Exit only doors will have manual keyed locks and will be locked from the unsecure side at all times.
   3) Local building services (mechanical/electrical/telecom) or custodial closets, storage areas, etc. will generally not have access control equipment installed.
   4) Doors leading to rooftop areas will generally have manual keyed locks with the door locked from the inside only to prevent persons from becoming stranded on the roof.

5. **Access Control – Student Apartments & Bedrooms:**
   Applies to private residential living spaces, not hallways, and other common areas.

   1) All entrance doors to an apartment or suite of bedrooms, and all bedroom doors, will be equipped with a combined card reader/electric lock set connected to an Off-Line Access Control System (OLACS); the electric locking mechanism will have a manual keyed over-ride feature. Dalhousie's Housing & Conference Services will specify the OLACS that is to be used in a residence building.
   2) Where applicable, other student residence building doors will be equipped as in I. II. III. or IV. above.

6. **Access Control - Elevators and Lifts:**
   Applies to all elevators and lifts that provide entry to areas which have access control installed.

   1) Elevator doors are to be considered as main entrance doors, and therefore they must be equipped to provide the appropriate level of access control as specified in I. II. III. or IV. above. All access control functions will be performed by the building ACS, and not by the elevator control system.
   2) When an elevator provides access to areas that have **different** functional uses, security requirements, or user groups, the elevator control system must be capable of:
      a. providing access only to floors for which the individual user has access rights, as determined by the building ACS when the users presents their card to the elevator card reader.
      b. and providing confirmation to the ACS of the actual floor selection.

In this application, because control of individual floor selection is required, a special ACS Elevator Interface Panel will be installed in a location that facilitates wiring connections to/from the elevator control system, and the Prox card reader, and PIN pad if required, will be installed inside the elevator cab. In addition, the elevator controller must have the capability to:

- use individual dry contact inputs from the building ACS to separately supervise each of the elevator cab's floor selection buttons;
- provide an individual dry contact output to the building ACS, to provide confirmation that a particular floor has been selected.

3) When an elevator provides access to areas within a building that have the same functional use and user groups, access control can be achieved by one of two methods:
    a. using a dry contact from the ACS to supervise the elevator controller functions (Note: the Prox card reader, and PIN pad if required, will be installed inside the elevator cab).
    b. using a dry contact from the ACS to supervise the elevator lobby call buttons (Note: the Prox card reader, and PIN pad if required, will be installed on the lobby wall next to the elevator call buttons).

   In this application, because control of individual floor selection is not required, a standard ACS Multi-Door Control Panel can be used.

28 13 27 Security Door Supervision – Application guideline

1. **Security alarm systems:**

   Applies to rooms where items of high value are used or stored.

   1) Each room or suite of rooms that constitutes a single Alarm Partition will have the following equipment installed to detect a forced entry:
      a. an alarm system keypad for arming and disarming the areas partitions, located inside the main entrance door;
      b. DCs on all perimeter doors;
      c. motions sensors to ensure coverage of all forced entry routes points such as doors, windows, hollow gypsum board walls, solid walls that do not extend above the drop ceiling, etc;
      d. a siren/strobe pair for local alarm annunciation located outside the protected area;
      e. an alarm partition will typically have an auto- disarm/arm scheduled to disable the perimeter alarms during normal "open" hours, and restore

the protection at a set time after normal "open" hours in case the partition is not manually armed by the last person leaving the area.

2) The valuables within the room or suite of rooms will be protected by separate partitions, that are normally armed 24/7, and will have the following equipment installed to detect tampering with the valuables:
    a. PC Tabs **DELETED – discontinued**;
    b. tamper switches on all cabinets or cupboards used for storage of valuables;
    c. these partitions will also trigger the siren/strobe pair (see 1.d. above).

28 13 28 Building Entrance Control System – Performance Guideline

Functional Statements: To achieve the objective of these guidelines, the design and construction of a building shall enable Security Services to achieve the following functional requirements:

1. To identify and minimize the risks present in and around the building.
2. To identify and validate building occupants authorized for access to secure area(s) of the building.
3. To control the access of validated persons to the whole or parts of the building that are considered secure.
4. To resist the unwanted entry of invalid persons.
5. To provide Security Services situational awareness of developing risks in or around the building.
6. To minimize exposure of occupants to unacceptable risks.
7. To discourage illicit use of building and premises.
8. To contact the building occupants in case of emergency or potential hazard.
9. To compile usage data on building occupancy.

1. **To identify and minimize the risks present in and around the building:** Provide a Preliminary Design Report which shall include identification of all risks and design recommendations, organized into the following table of contents:

1.1. Building Occupants, as indicated By Security Services in association with Bldg Administrators.

1.1.1. Intended uses and daily operation of building

1.1.2. Intended occupants and their expectations from Building Security System

1.1.3. Potential for unintended use or occupancy

1.2. Building Assets as indicated by Bldg Administrators, Security Services and EH&S Office
  1.2.1. Identification of high risk assets
  1.2.2. Hazardous Areas.
1.3. Potential Risk of Security Breach as indicated by Security Services.
  1.3.1. Affect on Building Occupancy
  1.3.2. Affect on Building Contents
  1.3.3. Affect on Dalhousie University Operations
  1.3.4. Affect on general public
1.4. Design Recommendations to Manage Risk:
  1.4.1. Building Theory of Operation (Daily, Seasonal, Academic Year etc.)
  1.4.2. Circulation
  1.4.3. Compartmentalization
  1.4.4. CPTED analysis including interior and exterior design
  1.4.5. Access Control System Recommendations
  1.4.6. Intrusion Alarm System Recommendations
  1.4.7. Remote Video Surveillance System Recommendations

2. To identify the building occupants:

2.1. Identification of building occupants shall be accomplished through the Access Control System (ACS).
2.2. The ACS shall ensure that building occupants can be identified when entering the building.
2.3. The ACS shall provide user access through the University's single keycard (Dalcard) system.
2.4. The ACS shall be capable of independent subdivided control of any combination of the following:
  2.4.1. Division by different groups of people. Some people may belong to more than one group.
  2.4.2. Division by zones / building compartments. Compartmentalization ensures discreet areas have appropriate levels of security access.
  2.4.3. Division by time and date.
2.5. The ACS shall have remote control capability from Security Services Command Center.
2.6. The ACS shall record the identity of the occupants and allow instant retrieval of this information by Security Services.
2.7. The ACS shall have a system administration function, allowing authorized administrators override controls. Administrative privileges shall be organized into hierarchical trees, with high level administrators collecting the privileges of subordinate administrators.
2.8. The ACS shall have a computerized log system which records all events.

3. To control the access of validated persons to the whole and/or parts of the building:

3.1. The ACS shall provide automated door locking and unlocking based on section 2 above.

3.2. The ACS shall provide garage door entry control on a unified system.

3.3. The ACS shall permit locking and unlocking of all systems on an automated and flexible schedule. This automation system shall have remote control capability from the Security Services Command Center.

4. To resist the unwanted entry of not validated persons:

4.1. Entrances and Exits from all Buildings / Compartments shall resist forced entry without dependency on house power or Access Control System.

4.2. The ACS shall report any attempts of unauthorized entry to Security Services Command Center including:

4.2.1. Failed access attempts.

4.2.2. Forced entry.

4.2.3. Propped doors.

4.3. ACS hardware components shall be of sufficient quality construction and design to resist vandalism and tampering.

4.4. Intrusion Alarm Systems (IAS) shall be provided in areas designated from the risk assessment, shall be integrated with ACS system to allow simultaneous monitoring, and shall seamlessly report to Security Services Command Center any system events including:

4.4.1. Forced entry.

4.4.2. Motion detection.

4.4.3. Security Sensors Alarms.

4.4.4. The system shall have a computerized log system which records all events.

4.5. IAS hardware components shall be of sufficient quality construction and design to resist vandalism and tampering.

5. To provide situation awareness of developing risks in or around the building:

5.1. A Remote Visual Surveillance System (RVSS) shall be provided in areas designated by the risk assessment and shall :

5.1.1. Connect seamlessly into the Access Control System (ACS) and the Intrusion Alarm System (IAS).

5.1.2. Be reviewable from Security Services Command Center.

5.1.3. Be capable of archival at the Security Services Command Center in full quality for future retrieval.

5.1.4. Be securely accessed by authorized Security Services personnel only. All access shall be recorded in a log.

5.2. All RVSS events, system information, and remote control functions must be remotely controlled and monitored at the Security Services Command Center in the McCain Building.

5.3. All RVSS Information shall be well integrated, organized, and displayed for fast and accurate Situational Awareness by the Security Services Shift Supervisor.

5.4. RVSS hardware components shall be of sufficient quality construction and design to resist vandalism and tampering.

5.5. All Systems including Access Control System (ACS), Intrusion Alarm System (IAS), and Remote Video Surveillance System (RVSS) shall be capable of rerouting to an alternate emergency Command Center.

6. To minimize exposure of occupants to unacceptable risks:

6.1. All systems, hardware, and building design shall meet all Provincial Building Code and Municipal Bylaw requirements, including any special local requirements by all Authorities Having Jurisdiction.

6.2. Access Control System (ACS) shall permit remote control of Building / Compartment egress at Security Services Command Center during an emergency response including:

6.2.1. Unlimited Exiting – Unlock Building / Compartment to permit exiting during an event.

6.2.2. Lock Down – Locking to restrict entry into a Building / Compartment during an event.

6.2.3. Remote control system shall not allow violation of Building Code, Municipal Bylaws, or directives from Authorities Having Jurisdiction.

6.3. The ACS shall be connected to emergency power generation where available.

6.3.1. Where emergency power generation is not available, all components shall have a minimum (8) hour battery backup. All systems shall have integrated battery test system which notifies Security Services Command Center in event of low battery.

7. To discourage illicit use of building and premises:

7.1. Building Design shall respond to the requirements of the CPTED analysis and Risk Assessment Recommendations to discourage illicit use of building and premises.

8. To contact the building occupants in case of emergency or potential hazard:

8.1. This section reserved for future use.

9. To compile usage data on building occupancy:

9.1. All Systems (ACS) (IAS) (RVSS):

9.1.1. Location, time, and duration of Events.

9.2. Access Control System (ACS) shall record and archive the following data:

Identity and time of an individual making a request to access and reason for access denial to a building / compartment.

28 14 00 Access Control System Hardware

This section shall be applied in conjunction with sections 28 10 00 and 28 13 28.

1. **Door Access Control:** For new construction, the door access control system shall be based on the "Genetec" electronic door control system consisting of the following components:
   1.1. Network Controller (Synergis Cloud Link): Each network controller shall be capable of managing up to 256 readers and electronic locks, as well as monitoring events and alarms. Dalhousie has developed a network architecture for the network controllers (Contact the Electrical Planning Engineer for assigned controllers). Design teams shall verify system capacity to determine if additional cloud link units may be required. Dedicated network controller shall be installed in the main communication room serving the building. At each network controller, provide the following:
      1.1.1. One FT4 rated Cat. 6 cable (blue) from the data patch panel to a surface mount data outlet installed within a 6" square junction box complete with a hinged cover, located within 12" of the network controller. If this cable passes through a return air plenum system, this cable shall be rated FT6 as per the NBCC.
      1.1.2. One FT4 rated Cat. 6 patch cord cable (white), 24" long, to connect network controller to above data outlet.
   1.2. **Intelligent Controller (Mercury LP2500 & LP1502):** Each intelligent controller shall be capable of managing 32 downstream interfaces (eg. Reader modules, input modules, and output modules) over RS-485. The intelligent controller shall be installed in communication rooms on a dedicated wall (for access control and intrusion) with fire-resistant plywood. At each intelligent controller, provide the following:
      1.2.1. One FT4 rated Cat. 6 cable (blue) from the data patch panel to a surface mount data outlet installed within a 6" square junction box complete with a hinged cover, located within 12" of the network controller. If this cable passes through a return air plenum system, this cable shall be rated FT6 as per the NBCC.

1.2.2. One FT4 rated Cat. 6 patch cord cable (white), 24" long, to connect intelligent controller to above data outlet.

1.3. **Reader Module (MR50, and MR52):** controls readers, alarm inputs and device outputs. Installed in the door access control junction box and powered from access control system power supply. Refer to standard wiring diagrams for specific details on wiring requirements.

1.4. **Input Module:** controls up to 16 alarm inputs, Mercury cat. # MR16IN. Typically, there would be an input controller installed on each level of the building. The input module shall be installed in the communication rooms serving the respective floor.

1.5. **Output Module:** controls up to 16 device or relay outputs, Mercury cat. # MR16OUT. The output module shall be installed near the intended use location (e.g. elevator machine room).

1.6. Power Supplies:

1.6.1. **Network Controllers, Intelligent Controllers, Reader Modules and Input/Output Modules** require a separate power supply (P/S(ACS)). The access control system shall use a central 12V power supply complete with battery backup. These power supplies shall be hardwired to a dedicated 120V circuit (emergency power when available) and located adjacent to the intelligent controllers in each communications room. **Battery supervision output shall be monitored via Genetec input**.

1.6.2. **DH - Door Hold Open Devices** - Deleted. Refer to Electrical Guideline Section 26.

1.6.3. **ES - Electric Strikes** require a separate power supply. A 12V DC version is preferred for all applications with the intent to utilize a central power supply. This central power supply is typically installed adjacent to the network controller power supply. In doors equipped with barrier free door operators, a Camden CX-33 interface shall be used.

1.6.4. **ELCK - Electrified Locks** require a separate power supply. A 12V DC version is preferred for all applications with the intent to utilize a central power supply. This central power supply is typically installed adjacent to the multi door controller power supply. When 24V electrified locks are required, a separate 24V central power supply must be installed.

NOTE: Electric Strikes and Electrified Locks can be fed from the same central power supply unit, provided the overall amp-hour requirements are properly calculated and unit sized correctly.

1.6.5. ELCH - Electric Latch Retraction requires a separate power supply, provided as per the manufacturer's door hardware specifications with assurance it is installed with the distance limitations as per specification.

1.7. **Junction Box complete with Reader Module:** At each door tied to the network controller, install a 12" x 12" x 6" junction above the door on the **secured side** with a minimum Belden cat. # 9841 and cat. # 9952 cable runs (or equivalent). These junction boxes shall be accessible and mounted less than 12'-0" A.F.F. Refer to Appendix "A" for typical door control details for additional information on components, locations and cabling requirements.

1.8. **Wiring / Cabling:** Wiring and cabling for the door access control system shall be installed in a raceway system consisting of wire basket tray and/or J-hooks in accessible ceiling space and EMT conduit where run concealed in inaccessible ceiling areas such as drywall ceilings or bulkheads. Where the door access control cables are installed in a wire basket shared with communication cables, they shall be bundled together with Velcro cable straps and identified as door access control cables.

1.9. **Barrier Free Door Operators:** When installed on exterior doors, the operator shall be tied into the card access system controller to prevent damage to the motor. When the door has been locked, the outside barrier free operator button shall be disabled. Upon presentation of the proper credentials, the door access control system shall enable the outside door operator button for 5 seconds. Upon activation of the barrier free operator pushbutton, the door will open. After 5 seconds, the outside door operator button shall once again be disabled.

1.9.1. **Sequence:** Upon presentation of the proper credentials, the door access control system shall enable the outside door operator button for 5 seconds. Once the barrier free operator pushbutton is activated, the door will open. After 5 seconds, the outside door operator button is once again disabled.

1.10. **Card Access Control in an Elevator Cab:** The elevator controls must have the ability to accept external inputs from, and send a signal back to, the Access Control System (ACS) via dry contacts.

1.10.1. **Option #1, Elevator control sequence - Floor Tracking (preferred):** The elevator floor selection buttons shall be interlocked with the ACS. When the occupant pushes a floor selection button, the elevator controller sends an output signal (dry contact) to the ACS via the Input Module indicating a request to travel to the specific selected floor. The ACS will then check the user credentials. If the user has permission to travel to the selected floor, the ACS will send a signal (dry contact) to the elevator controller via the Output Module device thus enabling the floor

selection and allowing the user to travel to the selected floor. If the user does not have permission to travel to the selected floor, the floor selection times out and the elevator remains stationary.

1.10.2. **Option #2, Elevator control sequence - Restricted USER Access:** The elevator floor selection buttons shall be interlocked with the ACS. Certain facilities may be configured to restrict access to all or specific floors through the elevator. When the user provides credentials requesting to travel, the ACS checks the user credentials. If the user has permission to travel to the selected floor, the ACS will send a signal (dry contact) to the elevator controller via the Output Module thus enabling the floor selection and allowing the user to travel to the selected floor. This configuration does not prevent users from accessing other restricted floors.

1.11. **Card access control at the elevator call button (hallway or elevator lobby):** The elevator must have the ability to accept external inputs (i.e. dry contacts) from the Access Control System (ACS). The elevator call buttons will be disabled until proper credentials have been presented at the card reader mounted in each of the elevator lobbies.

1.11.1. **Sequence:** When a user presents credentials at the reader, the ACS checks the user credentials. If the user has permission to use the elevator from that floor, the ACS will send a signal to the elevator controller via the Output Module enabling the elevator call button and will call the elevator. The elevator call button shall light up to indicate to the user that the elevator has been called. If the user does not have permission to use the elevator, the floor selection remains disabled, and the elevator remains stationary.

1.12. **Symbols and definitions:** For consistency, all definitions, acronyms and legends contained within this document must be utilized in all related door access control system documents or drawings supplied as part of any construction process.

28 23 00 Video Surveillance

This section shall be applied in conjunction with section 28 13 28.

1. Application guideline:

Applies to:

i) building perimeter entrances (including parkade entrances);

ii) building perimeter doors which have local audible and visible alarms installed;

iii) exterior spaces where there is a security concern such as parking lots, loading bays, etc.;
iv) interior "public" spaces with high pedestrian traffic levels such as the elevator main lobby, atriums, interiors of student residence elevators;
v) the entrance to a high security area (see section II. above);
vi) the entrance to an interior "public" space that is located in an isolated area such as the building basement or parkade (e.g. bicycle storage areas and related change/shower rooms), where single individuals may be at risk;
vii) retail areas, where the presence of significant amounts of cash or valuables may create a significant risk of theft or holdup.

1) All building perimeter entrance/exit doors will be monitored by 2 cameras located to capture face-on images of persons entering and leaving the building.
2) When exterior spaces are being monitored, care must be taken to limit camera coverage, as far as practicable, to Dal property and to avoid inadvertent viewing of adjacent building windows.
3) When interior public spaces are being monitored, cameras should be located to provide:
    a. complete coverage of pedestrian traffic flow within the area to ensure all persons entering and exiting the area will be recorded;
    b. coverage of most of the usable space within the area.
4) Cameras mounted inside of residence elevators should be located to:
    a. capture face-on images of all persons entering the elevator;
    b. capture the floor being accessed;
    c. avoid views down hallways and toward student room doors when the elevator doors are open.
5) High Security areas and isolated interior public spaces will be monitored by 2 cameras at each entrance located to capture face-on images of all persons entering and exiting the area.
6) Retail areas may have video surveillance cameras installed, at the retailers' expense, upon written request to the Dalhousie project manager and the approval of the Dalhousie's Director of Security Services.
7) Cameras should be located to avoid vandalism and to be accessible by maintenance staff using a step ladder.

2. **Technical guideline - Security System Video System:**
2.1. The Security System Video System shall consist of the following components:

2.1.1. IP Based, Power Over Ethernet (POE), fixed and multi-sensor type cameras compatible for use with Dalhousie's Security System Video System (Genetec). Coordinate with the project manager on a case-by-case basis.

2.1.2. DELETED

2.1.3. DELETED

2.1.4. DELETED

2.2. Cameras: Ceiling mounted shall be the preferred location for interior cameras. However, wall mounted cameras will be acceptable in areas with obstructions, no ceilings, or ceiling greater than 12'-0". Cameras shall be IP Based with Power Over Ethernet (POE). The cameras shall use HTTP over port 80 or RSTP over port 80 but not over multiple ports. The video format shall be H.264. Cameras must be compatible with Dalhousie's current version of Genetec Omnicast. Coordinate compatible cameras during the project design basis with the project manager.

2.2.1. Fixed type interior cameras - ceiling mounted: Ceiling mounted, interior fixed type cameras shall be fixed dome cameras. Camera shall not be mounted on ceiling greater than 12'-0".

2.2.2. Fixed type interior cameras - wall mounted: Wall mounted, interior fixed type cameras shall be complete with wall mount bracket. Mount camera at 8'-0" A.F.F. to the bottom of the dome unless indicated otherwise.

2.2.3. Multi-sensor type interior cameras - ceiling mounted: Ceiling mounted, interior multi-sensor type cameras shall be fixed dome camera complete with suspended ceiling installation kit.

2.2.4. Multi-sensor type interior cameras - wall mounted: Wall mounted, interior multi-sensor type cameras shall be fixed dome camera complete with wall mount bracket.

2.2.5. 2.2.5. Fixed or Multi-sensor type exterior cameras - wall mounted or post mount: Wall mounted, exterior Fixed or Multi-sensor type cameras shall be fixed dome camera with wall mount bracket. Post mounted, shall be fixed dome camera with post mount bracket. Mount cameras no more than 16'-0" Above Finished Grade.

2.3. SSV Rack: DELETED.

2.4. Uninterruptible Power Supply (UPS): DELETED.

2.5. Network Video Recorder (NVR): DELETED.

2.6. Cabling Requirements: At each camera location, provide and install a data jack complete with a blue Cat. 6 communication cable back to the respective floor data network switch. The Cat. 6 communication cable shall have mechanical protection (in conduit or interlocking armour).

2.7. Refer to Appendix "B" for a typical SSV camera details.

28 31 00 Intrusion Detection

1. **Application guideline:**
   Applies to rooms where items of high value are used or stored.

   1.1. Each room or suite of rooms that constitutes a single Alarm Partition, and will have the following equipment installed to detect a forced entry: an alarm system keypad for arming and disarming the areas partitions, located inside the main entrance door; DCs on all perimeter doors; motion sensors to ensure coverage of all forced entry routes points such as doors, windows, hollow gypsum board walls, solid walls that do not extend above the drop ceiling, etc.; a siren/strobe pair for local alarm annunciation located outside the protected area; an alarm partition will typically have an auto-disarm/arm scheduled to disable the perimeter alarms during normal "open" hours, and restore the protection at a set time after normal "open" hours in case the partition is not manually armed by the last person leaving the area. The valuables within the room or suite of rooms will be protected by separate partitions that are normally armed 24/7 and will have the following equipment installed to detect tampering with the valuables: PC Tabs on all valuables that are fixed in place such as computer lab PCs (maximum 10 tabs per zone), ceiling projectors, etc.; tamper switches on all cabinets or cupboards used for storage of valuables; these partitions will also trigger the siren/strobe pair (see 1.d. above).
2. **Technical guideline:** The Intrusion Alarm System shall be based on a DSC Neo system. The Intrusion Alarm System shall consist of a complete end to end system consisting of raceways, backboxes, cabling, devices, termination and testing all supplied and installed by the electrical contractor.
   2.2. The intrusion alarm system shall consist of the following components:
      2.2.1. DSC Neo Model HS2128 control panels complete with TL280E ethernet communicator, batteries, and alarm output to Dalhousie Security Sur-gard receiver via the ITS Network.
      2.2.2. Zone Expander: DSC Neo Model HSM 2108 - 8 hardwired zone expanders.
      2.2.3. Output Module: DSC Neo HSM 2208 Low Current Output Modules complete with 8 programmable outputs.
      2.2.4. Power Supply Module: DSC HSM 2204 High Current output module (requires a DSC RL4 relay board for dry contacts).
      2.2.5. Relay Board: DSC RL4-LC Low Current 4 Relay Board
      2.2.6. Keypads: DSC HS2LCD Full message hardwired keypad for Neo.
      2.2.7. Motion detectors: DSC #BV-601 motion detectors, ceiling or wall mount, complete with built-in tamper switch and wall or ceiling mount as required (based on site conditions) – Gather more information for product to be used.
      2.2.8. Door contacts: Equal to Sentrol #SR-1078 series concealed 1" door contacts for man doors (surface mounted can be used for existing doors).
      2.2.9. PC-TAB Security Sensor: DELETED – Product discontinued.
      2.2.10. Signal horns: DSC #SD15W Siren

2.2.11. Signal strobes: DSC #F34K Amber Warning Strobe

2.3. The main intrusion alarm panel shall be installed in the main communication room. If not requiring an intrusion alarm in the building at the time of construction, the design shall allow space in the main communication room for two 24"W x 30"H custom intrusion alarm panels. Provide 4" backboxes adjacent to these panels for mounting the 120V - 16.5V transformer. The circuit can be shared but preferably from emergency or essential power.

2.4. Provide two data jacks adjacent to the main intrusion alarm panels.

2.5. Zone expanders or additional intrusion alarm panels shall be mounted in the sub-communication rooms. If there is no requirement for intrusion alarm in the building at the time of construction, allow space for two 12" x 12" custom security panels. Provide 4" backboxes adjacent to the panels in the sub-communication room for mounting the 120V - 16.5V transformer. The circuit can be shared but preferably from emergency or essential power.

2.6. Device description and associated wiring:

2.6.1. Motion Sensors: Infrared motion sensors shall be mounted at 8'-0" A.F.F., preferably at or near the corner of the room. Provide and install a single gang backbox complete with grommeted stainless steel cover plate at 8'-0" A.F.F.. Motion sensors shall be fed with a four conductor #22AWG unshielded cable. Motion sensors shall have a dedicated home run to the intrusion alarm panel.

2.6.2. Door Contacts: Magnetic door contact shall be flush mounted in door frame at top of door. Provide a 1" diameter hole in door frame for installation of door contacts. Where monitoring the door by the access control system, a second set of contacts or a two pole version of the single 1" diameter contact shall be required. The owners prefer to have only one door contact device installed at the top of the door. Coordinate with Dalhousie Facilities Management. Standard intrusion alarm door contacts shall be fed with a four conductor #22AWG unshielded cable. Each door shall have a dedicated home run back to the intrusion alarm panel.

2.6.3. Strobe: Provide and install a single gang backbox, flush ceiling mounted outside of the monitored space, generally at the door near the keypad. Alarm strobes shall be fed with a two conductor #18AWG unshielded cable equal to Belden Cat. No. 8461.

2.6.4. Siren: Provide and install a single gang backbox, flush ceiling mounted inside of the monitored space, generally above the keypad. Alarm sirens shall be fed with a two conductor #18AWG unshielded cable equal to Belden Cat. No. 8461.

2.6.5. PC Tab: For floor, desk or wall mounted equipment (monitors, computers, AV equipment, etc.) provide and install a single gang backbox at 18" A.F.F.. For ceiling mount applications (overhead projector), the single gang backbox shall be flush ceiling mounted. PC Tabs shall be fed with a four conductor #22AWG unshielded cable. Each PC Tab grouping (podium, ceiling projector, computer lab row of desks, etc.) shall have a dedicated home run back to the intrusion alarm panel location. Each home run for PC Tabs shall have a maximum of 10 PC Tabs for the home run.

2.6.6. Alarm Keypad: Provide and install a single gang backbox, flush wall mounted at 48" A.F.F. in an accessible location within the monitored space. Feed with a four conductor #22AWG unshielded cable. A global keypad shall be installed at the building main entrance to assist security personnel with locating an alarm condition as they enter the building.

2.7. All zones shall be complete with double end-of-line terminations. All intrusion alarm devices shall be connected with only one device per zone. Multiple door contacts on the same physical door system can be connected to the same zone (i.e. a double door system can have each door contact connected to the same zone).

2.8. The main panel for the building security system shall be connected to Dalhousie Security Sur-gard receiver via the ITS Network. The monitoring shall be full 24 hour monitoring and shall include a complete indication of all alarms. Provide the necessary modules in the panel to interface with Dalhousie Security. Partition outputs and general trouble outputs shall be connected to designated Mercury input modules and monitored via Genetec. Termination shall be by a Certified Alarm and Security Technician (CAST). Co-ordinate the installation with Dalhousie Facilities Management Access Control Shop.

2.9. The contractor shall complete the system programming and initial setup using the keypad or DSC downloading software. Dalhousie Facilities Management will provide the Sur-gard account number, and support for signal testing. Dalhousie FM will be responsible for user access code programming and downloading a standard DSC Neo Dal template.

2.10. Each partition has its own strobe by its associated main keypad and visible by security. Sirens shall be setup at each partition unless a siren can serve multiple partitions close together. Each partition has its own keypad or multiple keypads.

2.11. 3.11. All Neo panels shall be connected with a TL-280E communicator and a network connection to allow for updates and monitoring.

2.12. 3.12. RL4 relays, also used to control sirens and strobes, shall be used to tie partition alarm outputs from HSM2208 modules to Genetec MR16in input board.

2.13. Refer to Appendix "C" for a typical intrusion alarm riser

28 31 00.03 Duress Alarm System

This section shall be applied in conjunction with section 28 13 28.

1. Application guideline:

- All duress alarm requests must be initiated by the Security department to Facilities Management. Duress alarms requires the security department to assess the risk and help department manage this risk before implementing an engineered solution.

- All duress alarms shall be accompanied by a security camera. This provides the security department information they need when a duress alarm has been activated.

2. Technical guideline:

Hold for future versions.