BYLAW & SECURITY

PHYSICAL SECURITY STANDARDS

City of Brantford Facilities

March 2024

Table of Contents

Version History

Version #	Date Of Update	Author(s)	Approval	Revision Notes
1	March 2024	Supervisor & Coordinator of Corporate Security, SCADA Coordinator, Network Architect, Audio Visual Engineer	Director of Bylaw & Security	Implementation of a physical security design & systems standard for City of Brantford Facilities

Definitions

The following definitions apply throughout this document:

a. ACS – Access Control System
b. AHJ – Authorities Having Jurisdiction
c. CSS – City of Brantford Corporate Security Services
d. DAS – Duress/Panic Alarm System
e. DDRF – Design Deviation Request Form
f. ESMS – Enterprise Security Management System
g. IAS – Intrusion Alarm System
h. PIDS – Perimeter Intrusion Detection System
i. RFI – Request for Information
j. VMS – Video Management Software
k. VSS – Video Surveillance System
l. SCADA – Supervisory Control and Data Acquisition

1 APPLICATION

These standards apply to all space owned and leased by the City of Brantford and serve as minimum requirements. New work must comply with this document. Renovation or reconfiguration of existing space requires the upgrading of the security system(s) to the requirements of this document. Not all the systems or devices described in this standard shall necessarily be included in each project. It is the responsibility of the design team to consult and collaborate with the City client group to understand their operations, to build upon the Physical Security Standards, and develop a security design that meets the clients' functional requirements.

1.1 Purpose

The purpose of this standard is to ensure minimum requirements are established for security systems utilized within the Corporation of the City of Brantford. This documents the specific goals and objectives of City of Brantford Corporate Security (CSS) to define the major system software and hardware components that comprise the City of Brantford's Enterprise Security Management System (ESMS) and to provide design requirements for integration of the ESMS into new, existing buildings, and site development projects.

The principal goal of the document is to provide consistent design and implementation standards for physical and electronic security systems throughout City of Brantford facilities.

The ESMS is comprised of four major electronic security sub-systems:

- Intrusion Alarm System (IAS)
- Access Control System (ACS)
- Distress Alarm System (DAS)
- Video Surveillance System (VSS)

Each of these sub-systems is comprised of command/control hardware, software, and field devices. The command/control hardware and software are standardized to provide the City of Brantford with a unified operational platform for enterprise physical security management.

1.2 Design Deviation Request Form (DDRF)

All proposed deviations/exceptions to these standards require the submission of a DDRF. Do not assume that the deviation/exception is approved until the item has been specifically accepted by CSS. This form is included as Appendix E.

1.3 Mandatory Systems – Minimum Requirements

An intrusion alarm system is a mandatory minimum requirement for securing any office, building or other City of Brantford premises. Public facing locations shall also have a monitored duress alarm partition. Other systems within this standard are optional and require direction from CSS as to what is required for each location.

1.4 Scope

In close collaboration with industry leaders, these security design guidelines were developed based on functional needs and best practices. The objective in creating these guidelines is to protect staff, clients, property, and equipment; to detect an

incident, delay the incident and respond to the incident. These guidelines are applicable to all City of Brantford facilities, proposed projects, and redevelopment. In the event that an exception needs to be made to deviate from these guidelines and standards, and or the recommendations provided by a CSS, an alternate design choice should be made with a solution that meets or exceeds the recommendations. This solution should be reasonably expected to eliminate, engineer or administratively control the risk/hazard.

1.5 Approach

The development of the guidelines and standards reflects the principles of Crime Prevention through Environmental Design (CPTED). These principles, when applied early, can be integrated into any Facility design providing layers of protection for clients, visitors, and staff. CPTED defines territories and how they are controlled and managed based on the use of “concentric rings of control and protection.” Outermost rings are supported by additional inner rings of protection. Each of these concentric rings will be addressed as layers of protection within these guidelines and are intended to sequentially deter, deny access to, and slow down possible malefactors. CPTED layers include:

1. The first layer of protection should be at the perimeter of the property, which limits points of entry. The property perimeter should be defined by fences, landscape, or other barriers. At certain locations, this may include the building exterior. Property entry points should be controllable during emergency situations or heightened security levels.
2. The second layer of protection should be at the building exterior and consist of doors, windows, or other openings. Protective elements or components may include access-control hardware, intrusion detection, video surveillance, use of protective glazing materials, or personnel for control and screening at selected entrances during designated times.
3. The third layer of protection should be inside the building itself, segregating authorized and unauthorized visitors. Using physical and psychological barriers and hardware, this layer is most frequently applied in areas of higher risk such as dangerous and violent client areas, developmental disabilities and rehabilitation areas, and pediatric/youth program and treatment areas.
4. The fourth layer of protection should segregate generally accessible client areas from staff-only areas. Using physical barriers and locking hardware, this layer is most frequently applied to areas that restrict all visitors and limit access to Facility staff only in areas such as staff offices, staff locker rooms, storage and distribution locations, food preparation, and research laboratories.

5. The fifth layer of protection should further restrict staff access to highly sensitive areas. Using physical barriers and locking hardware, this layer is most frequently applied to areas that are limited to vetted and authorized staff. These areas frequently include hazardous materials, information technology infrastructure, and areas housing Personal Identifiable Information. Security design considerations for such areas should be addressed in accordance with applicable regulatory oversight, standards, and guidelines.

1.6 Security Design Process

The physical design of buildings and integration of security systems are important components of an overall facility protection plan and a positive client, visitor, and staff experience. Security design considerations must address the program requirements and services offered by the departments within. Important considerations are as follows:

1. A security project request should be submitted to security@brantford.ca.
2. The inclusion of a Physical Security Assessment Report (PSAR) conducted by a member of City of Brantford CSS; who can assess specific threats as identified by the program's unique risk factors. Including a PSAR in initial design will assist in identifying the appropriate program location within the facility and methods of control required. This may include: signage, physical barriers, direct staff observation/escort, mechanical and electronic access controls, and audible or monitored alarms.
3. The project design team—including the representative from CSS—should develop a comprehensive security plan that indicates a layered approach including zones, access control points, circulation routes, and required egress paths.
4. Security management responsibility lies with CSS and funding allocation lies with the project manager.
5. Client users, who have identified security and/or occupational health and safety (OH&S) concerns regarding their program space, should contact their OH&S representative to produce a Hazard Assessment and Control Report (HACR) to identify the hazard(s) and appropriate control(s). In the event that the hazard requires an engineering control, the client user should contact CSS for a physical security assessment. The completed PSAR will be sent to the Project/Facility Manager/Coordinator.

2 GENERAL DESIGN GUIDELINES AND STANDARDS

2.1 Fundamental Purpose

The fundamental purpose of this document is to provide expert guidance and recommendations based on best industry practice that help protect City of Brantford assets (both tangible and intangible) from potential hazards. These assets include but are not limited to staff, public, buildings, equipment and access to sensitive/personal information.

2.2 Internal Environment

The internal environment should be designed to address horizontal and vertical circulation routes that facilitate operational functions in accordance with security needs and life-safety requirements. The size, complexity, and scope of services provided within a facility can vary significantly; in all cases, the building design should be composed of defined zones of protection. Zone requirements include (See Appendix A for example):

1. *Public Zone* – this zone generally comprises of public assess areas including but not limited to a building's perimeter and elevator lobby.

2. *Reception Zone* – this is where security controls are placed at the transition of the public zone to a restricted-access area and facilitates contact between the public and company representatives. It is typically located at a building entrance or alongside as elevator lobby. Access to the public may be limited to specific times of the day or for specific reasons.

3. *Operations Zone* – this area is indicated by a recognizable perimeter and is restricted to employees and authorized contractors. Access cards and company identification are often used to authenticate personnel and provide them with access to the premises. Members of the public are not permitted into this area unless authorized and properly escorted.

4. *Security Zone* – access into this zone is strictly controlled and limited to authorized personnel within the organization and properly escorted visitors. It is also indicated by a recognizable perimeter within the operations zone, and is continually monitored. An example of this is an area where restricted information is processed of stored.

5. *High Security Zone* – assess to this zone is limited to authorized, appropriately screened and properly escorted visitors. Assess details are also recorded and audited. The area is indicated by a recognizable and specially built and controlled perimeter, and is monitored continuously. Often times, details about the zone's specific location are only provided on a need-to-know basis; for example, computer data backup sites.

2.3 Access Control

The management of access control should be consistent across the Facility as to the operating procedures and type of systems used. Electronic security systems, if used, should be integrated and standardized. Design considerations for electronic safeguards should include:

1. Designating the location of duress alarms at strategic locations where employees work alone, in isolated areas, or other areas of higher risk as identified by the PSAR.
2. Using video surveillance to capture and record images in defined security sensitive areas or other areas of higher risk as identified by the PSAR. Each camera application should have a defined policy of use that is consistent within the area being protected, recognized industry best practices, corporate policy and regulatory standards.
3. Selecting and specifying door and window hardware with specific security requirements and functionality. Hardware should be durable and appropriate for the environment.
4. Coordinating door hardware, electronic security systems, electrical, and fire alarm system specifications.
5. Installing security intrusion systems in non-24-hour facilities on all entrances and in other areas of higher risk as identified by the PSAR. The installed system should be designed to allow the independent arming of various areas of the building in support of different departmental hours of operation.
6. Developing a coordinated signage approach for wayfinding, brand identification, security, and emergency information.
7. Avoiding, where possible, stand-alone systems for individual buildings or renovation projects.
8. Implementing a single, unified or integrated system for access control, video surveillance, and when appropriate, parking access and egress, debit card functions, and time and attendance needs.
9. Expandable security systems by providing flexible infrastructure including wiring pathways and equipment locations.
10. Coordinating with other building technology systems, as appropriate.

2.3 Receptions

Description: A reception desk or counter for areas requiring public interface

Location: Separate from Operations Zone

Recommendations:

1. Controlled and restricted access in and out of the area after normal business hours or when the area is not occupied.
2. Desk or counter should be designed to obstruct access.
3. Refer to *3.1 Secure Receptions* for specific requirements.

2.4 Atriums

Description: A large open air or skylight covered space surrounded by the building

Location: Operations Zone

Recommendations:

1. Enhanced natural surveillance and sight lines.
2. Furniture should be designed to minimize the possibility of use for self-harm, as a ligature, as a weapon, or as a barricade.
3. Wall hangings, plants, fire extinguishers, or other hard objects should be securely fastened making it impossible to throw objects over the handrail.
4. Any public facing facility with an open atrium over three levels, that provides program support for violent and or unpredictable clients, should design and install a handrail system making it impossible to jump/climb over.

2.5 Shipping, Receiving and Materials Management

Description: Area(s) specifically used for the movement of materials

Location: Security Zone

Recommendations:

1. Controlled and restricted access in and out of the area.
2. Electronic access control for frequently used staff doors.
3. Hardened walls, ceiling, and doors to prevent penetration.
4. Secure storage (e.g., fencing, gates, or locked cages, for items of high value, or hazardous materials).
5. Fencing, cargo doors, or other means to secure the external loading dock area from surrounding streets.
6. Intrusion detection systems for monitoring during non-occupied hours.
7. Video intercom.

2.6 Mail Rooms

Description: A room in which incoming and outgoing mail is processed and sorted.

Location: Security Zone

Recommendations:

1. Locating mail receiving and sorting rooms away from critical building infrastructure and structural support and mission-critical building functions, if possible at an off-site central receiving facility.
2. Location on the building perimeter, near or adjacent to the loading dock.
3. Controlled and restricted access in and out of the area.
4. Electronic access control for frequently used staff doors for auditing.
5. Secure storage (e.g., lock boxes or other secure means for items of a secure nature).
6. Security mail handling where applicable.
7. Intrusion detection systems for monitoring during non-occupied hours.

2.7 Records Storage

Description: Area used for the storage, retrieval and disposal of all types of media

Location: Security Zone

Recommendations:

1. Controlled and restricted access in and out of the area.
2. Electronic access control for frequently used staff doors, maintaining an audit record of room access.
3. Hardened walls, ceiling, and doors to prevent forced entry.
4. Intrusion detection systems for monitoring during non-occupied hours.

2.8 Meeting Rooms, Interview Rooms and Conference Rooms

Description: Area used for face-to-face communications

Location: Operational Zone

Recommendations:

1. Controlled and restricted access in and out of the area after normal business hours or when areas are not occupied.
2. Appropriate circulation and egress paths.
3. Secure storage for high-value audio/video equipment, computers, and other office equipment.
4. Refer to Section 3.2 Secure Interview Rooms for specific requirements.

2.9 Call Centers

Description: Area set up to handle a large volume of telephone calls

Location: Operational Zone

Recommendations:

1. Controlled and restricted access in and out of the area.
2. Electronic access control for frequently-used staff doors, maintaining an audit record of room access.
3. Direct communication capability with security, law enforcement, and other public safety agencies.

2.10 Exterior, Landscaping, Wayfinding

Description: Clear, logical, and articulated elements and spaces of the built environment such as pathways, entries, gathering spaces and finishes.

Location: Public Zone

Recommendations:

The proper design and effective management of the external property environment can minimize violence and property crime, promote efficient resource management, and provide a welcoming environment.

1. Landscape plans should be designed to enhance facility security by, increasing natural surveillance and sight lines, and remove obstructions to lighting systems.
2. The external environment should be addressed from the outside inwards and the first point of control should be at the perimeter of the property limiting points of entry. Access control and perimeter security should be considered in the initial design stage.
    a) Physical protective barriers should be designed to help restrict or channel access. Fences are the most common perimeter barrier or control. A perimeter fence should be continuous, be kept free of plant growth, and be maintained in good condition. The number of gates and perimeter entrances should be limited to those absolutely necessary, but should be sufficient to accommodate the peak flow of pedestrian and vehicular traffic. Depending on the level of protection required, intrusion detection devices may be considered.
    b) Physical protective barriers should be placed at building entrances and walkways to minimize the likelihood of injury or damage by vehicles to pedestrians, equipment, and structures.

c) Prevent access to outdoor air intakes by placing them at the highest feasible level above the ground. Outdoor air intakes can be used to introduce chemical, biological, and radiological (CBR) agents into a facility. When air intakes are publicly accessible and relocation or physical extensions are not viable options, perimeter barriers that prevent public access to outdoor air intake areas may be an effective solution. Securing outdoor air intakes can also prevent vehicle exhaust, landscaping chemicals, and other types of contaminants from entering the building.

d) Roof access and openings, like other entrances to the building, should be secured. Ladders, skylights, and other openings should strictly be controlled through keyed locks, swipe cards, or similar measures.

e) Exterior perimeter doors should be installed so the hinges are on the inside to prevent removal of the screws or the use cutting devices. Pins in exterior hinges should be welded, flanged, or otherwise secured, to prevent the door's removal. The door should be metal or solid wood. If vision panels are to be installed, laminated security glass should be considered.

f) Natural barriers, landscaping, or security fencing should be considered to discourage persons from entering the facility grounds unobserved on foot while maintaining openness and allowing for natural surveillance.

g) Transit, taxi, and pick-up/drop-off stops should be identified and situated to maintain perimeter control, prevent unobserved pedestrian access and located in close proximity to the public entrance.

3. Way-finding signage should be used to orient and guide clients and visitors to their desired location. To be effective, signage should:

    a) Provide clear and consistent messaging.

    b) Use color coding or memory aids to help individuals locate their vehicle.

    c) Be used to enhance security awareness while serving as a psychological deterrence to criminal and other negative behavior.

    d) Not obstruct natural sight lines.

2.11 Lighting

Description: Use of light is to make our facilities and property as safe and secure during low light/nighttime hours as they are during the daylight hours

Location: All Zones

Recommendations:

The choice of lighting will greatly impact people's perception of our facilities, witness potential, and electronic surveillance (cameras) and conversely creating an environment that creates a sense of high likelihood of detection for those who wish to create an environment of social disorder.

"Lighting does not stop crime but can be effective if applied in the proper way to altering how persons perceive their space. Lighting provides users of the built environment the choice to move forward, retreat back, or stay put. Lighting helps people feel safer and reduces the opportunity for being a victim of ambush." (Atlas, 20th Century Security and CPTED, 2nd Edition, 2013).

1. Consult a CPTED trained lighting engineer or authorized security representative on light bulb and fixture specifications, locations, fixture spacing, and height.
2. Automatic light control and backup systems are recommended.
3. Lighting applications should try to avoid creating, light pollution to the sky and neighbours, shadows and blind spots.
4. Coordination with landscape plans to anticipate future landscape growth.
5. Lighting systems need to be protected with tamper-proof hardware and properly maintained.
6. Replace broken or burnt out bulbs and ballasts as soon as possible.
7. The preferred lighting systems that should be considered for security applications and environmental/energy savings are, Light Emitting Diodes (LED) and Induction Lighting Systems.
8. Refer to IESNA Standards.

2.12 Parking Facilities

Description: A building, structure, land, facility, or area intended for parking vehicles

Location: Public Zone, Security Zone or High Security Zone

Recommendations:

The security of parking facilities, including surface lots, is a significant concern for users of those facilities. The Facility should provide dedicated client and visitor parking where possible. Additional parking considerations should be provided for staff and those working during non-traditional hours.

2.13 Base Building Systems

Description: The mechanical, gas, electrical, sanitary, heating, air conditioning, ventilation, elevator, sprinkler, cabling and wiring, life-safety, roof and other service systems of the building

Location: Security Zone

Recommendations:

1. The design of utility, mechanical, and infrastructure-related space, given its critical nature, should include facilities and security expertise as well as representation from administration, safety, client departments, ITS, emergency management, and other stakeholders whose operations rely on utilities, building systems, information, and communications infrastructure.
2. The Facility should be designed and constructed to provide security protection and emergency response for critical utility systems. The Facility should:
    a) Identify and provide protective measures to areas in which utilities including water, wastewater, steam, electrical power, communications, compressed gasses, and chilled water are produced or distributed in order to minimize the opportunity for disruption of those services.
    b) Identify and provide protective measures to areas in which back-up utility systems including generators, clean steam boilers, gas canisters, and other redundant systems are located. These measures apply to areas designated for the storage of fuels used to power back-up equipment.
    c) Design for emergency response to loss of utilities and should include separate means for redundancy in the delivery of purchased utilities including gas, water, wastewater, steam, electrical power, telecommunications, and other information technology services.
        d) Allow for the alternate delivery of utilities through the construction of access points into internal distribution systems in case services are needed from portable boilers, generators, gas tanks, etc.
        e) Design access roads, driveways, etc. to allow for the delivery of fuels or alternate utility generation.
        f) Ensure that utility and infrastructure design and construction plans complement and support operations/business continuity planning objectives.
        g) Restrict access to service rooms with the following functionality:
            i. Doors that meet or exceed standard commercial grade construction.
            ii. Doors that close automatically when not in use.
            iii. Doors that automatically lock when closed.
            iv. Locking devices that cannot be manually defeated.

v. Latching/locking hardware that is barrier protected (e.g., astragals, latch guards).

vi. Access control (key or card access).

3. The Facility should integrate security measures into the design of mechanical, electrical, and critical infrastructure spaces in order to provide for a work environment in which major systems are secure from unauthorized access. The Facility should:

    a) Limit access to personnel that manage and maintain the mechanical, electrical, HVAC, and plumbing systems. This should include but not be limited to electrical vaults, elevator machine rooms, water supply systems, wastewater pumping systems, and air handler intakes.

    b) Limit access to data centers, areas that house servers and other hardware, and areas where systems are monitored, including but not limited to, information technology, telecommunications, and building automation and security systems.

    c) Limit access to rooftops in the same manner as for mechanical, electrical, and plumbing system spaces including roof access hatches as well as doors leading from secured mechanical spaces.

    d) Design storage areas within the mechanical space for use by those who have access and secure such storage facilities within the larger area.

    e) Incorporate similar security designs with regards to telecommunications, information technology, security, fire alarm, and building automation rooms or spaces throughout the building. Panels serving these systems should be secured and may be alarmed.

    f) Secure rooms or spaces storing plans allowing for access by both internal and external emergency responders.

    g) Include detailed utility and mechanical system plans within mechanical or technology rooms for use by security, facilities, or emergency response personnel from within the organization or from public responders.

4. The Facility should design and build infrastructure to provide for redundancy and potential expansion as it relates to the growth of technology and the subsequent demand on utility and mechanical systems that may require enhanced security or other building systems. The Facility should:

    a) Incorporate the design and construction of stacked technology rooms when possible to allow for the easy management of cables and wire related to security systems, telecommunications, information technology

fiber, building automation, process automation, fire alarm connections, and the efficient use of networked systems.

b) Integrate security systems infrastructure into the design and engineering of the project to ensure that there is space for current and future panels related to the systems designated above and to allow shared uninterrupted power supplies and the appropriate environmental needs as the technology evolves.

c) Provide network capabilities for current need and anticipated growth in security systems or for the future implementation of those systems.

d) Refer to City of Brantford CSS for any questions or clarifications regarding directives, standards and guidelines.

3 PROGRAM SPECIFIC REQUIREMENTS

Facility design should address the variety of settings and unique risks in providing program support for violent and or unpredictable clients. The facility should be a calm, welcoming environment, respecting privacy, with important provisions to maintain client, visitor, and staff safety. Should be designed to protect the privacy and dignity of clients and address the potential risks related to harm to self, to others, and to the environment.

3.1 Secure Receptions

Description: A reception desk or counter for areas requiring public interface with violent and/or unpredictable clients

Location: Secure Zone

Recommendations:

1. Design should address the variety of settings and unique risks in providing program support for violent and or unpredictable clients. One of the most vulnerable areas in any facility is the reception. Reception is a high traffic area and the entryway to offices and departments. Receptionists, who are often alone or isolated, are the first to encounter irate, dangerous and violent clients and visitors. The reception itself should be a calm, welcoming environment, respecting privacy, with important provisions to maintain client, visitor, and staff safety.
2. Reception room or vestibule for areas when they pose unique risks and requiring public interface, separate from Operations Zone.

3. The identified risk/vulnerability will determine the classification level: Low Secure, Medium Secure or High Secure. See table below.

<table>
<tr><th colspan="2">Low Secure</th></tr>
<tr><td>Recommendations</td><td>Typical Programs</td></tr>
<tr><td>• Reception desk should be of sufficient design to obstruct access.
• Laminated glass with 2-inch-wide vertical pass through
• Controlled and restricted access in and out of the area after normal business hours or when the area is not occupied.
• In areas that require the desk to be located behind secured doors, a video intercom (or telephone) communication from outside the unit should be provided to screen visitors, clients, and staff.
• Duress alarms at reception counter/desk monitored by City CSS and third party monitoring company specified by the City.
• The door leading into the program area should be access controlled. The door may be capable of release from the reception desk if under constant surveillance. The door release button should be concealed from view of the public. It should be a constant touch unlocking system where once the hand is removed from the unlock button, the door automatically closes and re-locks.
• Furniture should be designed and installed to minimize the possibility of use for self-harm, as a ligature, as a weapon, or as a barricade.
• Solid core security door and frame off reception area into staff inner office with automatic door closer
• Card access on solid core security door off front reception
• Panic switch located on the staff side of the secure barrier in case of emergency. All panic switches installed should be of the (operational) same design</td><td>Examples may include but are not limited to:
• Human Resources
• Building Services
• Planning Services
• Environmental Services</td></tr>
<tr><th colspan="2">Medium Secure</th></tr>
<tr><td>Recommendations</td><td>Typical Programs</td></tr>
<tr><td>Low security recommendations and
a. Recessed Front reception counter document pass through tray (not acceptable for high secure reception)</td><td>Examples may include but are not limited to:
b. Family & Income Stability
c. Customer Service at City</td></tr>
</table>

	Hall d. Parking Services
High Secure	
Recommendations	Typical Programs
Low and medium security recommendations and • Ballistic glass barrier mounted on reception counter in a metal frame and constructed to the upper slab/ceiling. No vertical or horizontal pass through is permitted. • Ballistic counter base construction on which the ballistic glass barrier is mounted. • Secure parcel pass through constructed into the wall adjacent to front counter. • Electronic voice intercom system between the public and front reception staff on either side of the ballistic glass barrier. • Video surveillance cameras (vandal resistant with smoked domes) and video recorder.	Examples may include but are not limited to: e. POA Court

4. Waiting room designed to the same security level.
5. Standard project request process is still in place.
6. See Appendix B for Secure Reception Layout options.

3.2 Secure Interview Rooms

Description: A room for programs requiring face-to-face communication with violent and/or unpredictable clients

Location: Security Zone or High Security Zone

Recommendations:

1. The design of Secure interview rooms should address the variety of factors impacting where and how programing is provided including diagnosis, gender, age, length of stay, client acuity, and risk presented to staff, themselves and or others. The level of security will vary based on these factors.
2. The prevention of self-harm should be the major factor in design by reducing potential ligature points and avoiding features that could contribute to self-harm. Recording device and microphone should be securely fastened and a clean desk policy should be followed.
3. The identified risk/vulnerability will determine the classification level: Low Secure, Medium Secure or High Secure. See table below.

Low Secure	
Recommendations	Typical Programs
• Table or desk should be placed in such a way as to not barricade staff inside the room and positioned to provide staff direct access to an exit door (safe egress). • Furniture should be designed and constructed to minimize the possibility of use for self-harm, as a ligature, as a weapon, or as a barricade. • Room should be equipped with duress alarms, access card reader, and slap-lock type locksets that require a key to lock or unlock the outer handle while the inside handle is always free. • Doors to these rooms should be designed to swing out to prevent entry being barricaded. • Duress alarm beside the door on the staff side. • The entire room should be observable from outside the room. • Light fixtures, fire system components, HVAC grilles, and equipment, and window coverings/hardware should be designed to prevent tampering, reduce the opportunity to create weapons, and eliminate aids to self-harm. • Windows should be safety glazed (laminated or film).	Examples may include but are not limited to: • Human Resources
Medium Secure	
Recommendations	Typical Programs
Low security recommendations and f. Recessed document pass through tray (not acceptable for high secure reception) g. Millwork secured to the floor	Examples may include but are not limited to: h. Customer Service at City Hall
High Secure	
Recommendations	Typical Programs
Low and medium security recommendations and • Ballistic glass barrier mounted on table in a metal frame and constructed to the upper slab/ceiling. No vertical or horizontal pass through is permitted. • Ballistic table base construction on which the ballistic glass barrier is mounted. • Electronic voice intercom system between the public and staff on either side of the ballistic glass barrier. • Video surveillance in tamper resistant housing on staff side and monitored at reception desk. • Video surveillance cameras (vandal resistant with	Examples may include but are not limited to: i. Family Income & Stability j. POA Court

smoked domes) and video recorder.	

4. See Appendix C for Secure Interview Room layout options.

3.3 Resident Facilities

Description: Facilities that provide phased based programs for clients experiencing poverty, homelessness, mental health, addictions or other challenges

Location: Should be located at a facility or site that assists clients with programming that meets their essential needs and rehabilitation

Recommendations:

1. The physical design of the facility should support a visitor reception (refer to Secure Receptions for specific requirements) during and after normal business hours. Clients and visitors presenting to the facility on foot and in vehicles should be funneled to entries with staffed reception areas where assistance, general guidance, and a psychological deterrence to wrongdoing can be provided. Ideally, the number of staffed reception areas should be minimized.
2. Designated after-hours access points for visitors should be identified. Physical controls or barriers should be provided to clearly distinguish between public areas and waiting areas.
3. Elevators available to the public should be located outside of the Operational Zone. Consider designated staff-only elevators. Provide electronic access control or other means to restrict the use of these elevators.
4. Exterior windows should be treated to prevent internal viewing from outside of the facility.
5. Client bedrooms should be designed to reduce the opportunity for self-harm.
6. Doors to client bedroom should swing out, if this can be accomplished without creating alcoves that are difficult to observe. Anti-ligature hardware should be used for client bedroom doors to prevent tampering or use as an anchor point. The door hinge should be continuous to prevent the hinge from being used as an anchor point. Doors should be equipped with classroom-type locks that can always be opened from the inside and the corridor side may be either locked or unlocked with a key.
7. Client rooms should include secure storage for client valuables and other items of higher value.
8. The bathroom should present itself as a normal environment, respecting client privacy and dignity, with important provisions to maintain client safety and reduce

the opportunity for self-harm. The external door should be fitted with a security lock that can be overridden from the outside.

9. Waiting areas should be outfitted with furniture pieces that are attached to each other or secured to the floor or a wall. Small or individual pieces should not be used.
10. Security officer, Security Guard posts, and/or police officer workstations, if applicable, should be located to maximize visibility at public entrances, waiting areas, and reception areas.
11. Staff suites and offices should be equipped with appropriate locking hardware on entry doors. Strategically located duress alarms should be considered.
12. Access to staff lockers and lounges should be controlled at all times and restricted.

3.4 Facilities in Remote Locations

Description: Large facilities located in sparsely inhabited areas

Location: Rural areas

Recommendations:

1. Constructing a fence around the perimeter can provide an adequate deterrent to entry.
2. Occasional observation by a roving guard service, depending on the sensitivity and risk of the facility.
3. Warning signs or notices should be posted to deter trespassing on government property.
4. Video surveillance could also be considered if guard services are available to monitor them.
5. Good quality and intensity of lighting should be spread throughout the property.

3.5 Cash Collection and Storage

Description: Payments received from clients, public or other sources, including cheques, cash, bank drafts or any similar items.

Location: High Security Zone

Recommendations:

1. Risks are primarily related to the collection, storage, and handling of the cash itself and can pose a risk to the Facility in the event of an armed robbery or internal theft. This includes any area within the facility that performs cash or other payment transactions.

2. Access to all doors to the main cashier area should be controlled and restricted to authorized personnel only with audit trail capability. Ideally, the dedicated entrance is limited to one single door.
3. Walls, ceilings, transaction counters, and doors to the cashier office space should be hardened to prevent penetration. The transaction counter should have a secure pass-through; an opening large enough to communicate and perform transactions only.
4. Access to the main cashier area should be restricted and provided through designated doors that feature the following functionality:
    a) Doors that meet or exceed standard commercial-grade construction.
    b) Doors that close automatically when not in use.
    c) Doors that automatically lock when closed.
    d) Locking devices that cannot be manually defeated.
    e) Latching/locking hardware that is barrier protected (e.g., astragals, latch guards).
    f) Card access.
5. Dropbox systems strategically located to facilitate centralized cash collection and protection of cash receipts. Consider the use of electronic “smart safes” to ensure large amounts of cash are not on hand in these areas at any time.
6. Cashier workstations equipped with strategically located duress alarms
7. Two-factor identification (dual level of access control)
8. Video surveillance should be used to capture and record an image with appropriate detail to identify all persons entering and leaving collection and storage areas. Additional video surveillance should capture images of:
    a) Safe or vault entry
    b) Cash counting area(s)
    c) Transaction counters
    d) Satellite cash storage areas
    e) Areas where cash is delivered or picked up
9. Consideration should be made to equipping the cash transaction counter with a video monitor displaying live camera images of transactions for public viewing and awareness.

10. Consideration should be given to the installation of video surveillance at the external perimeter of the main cash collection office such as connecting hallways and lobby areas. A video monitor should be installed inside the office for staff to view the hallway outside the entrance door.
11. In areas where cash transactions occur or cash is counted or stored, video surveillance should be installed that provides multiple angles of these activities with resolution sufficient for audit or investigation.
12. An intrusion alarm system should be installed and monitored by CSS for cash collection areas not staffed or occupied at all times. Consideration should be given to positioning alarm points for the following:
    a) Entry points
    b) Transaction counters
    c) To detect movement within the secured space
13. Primary cashier locations often require accessible services at public entrances, but based on the assessed vulnerability may be placed deeper in the facility. The facility should refrain from identifying cashier locations that do not provide direct service to the public.
14. Public cash collection areas such as cash registers at customer and parking services should include the following design considerations:
    a) Location in an open and visible area
    b) Unobstructed lines of sight to and from the cashier areas and no blind spots behind the cashier where the public can observe transactions
    c) Public interaction with cashier designed to minimize public surveillance of cash drawer achieved either through the elevation of the cashier or drawer positioning
    d) Strategically located duress alarms
    e) Recorded video surveillance of the area immediately surrounding and all transactions
15. Public cash collection areas in other areas that may be externally located or isolated within the Facility should include the following design considerations:
    a) Cashier workstation that is separated from the public and of sufficient height, width, and strength to make it difficult for someone to jump over, reach over, or physically assault an employee.

b) Unobstructed lines of sight to and from the cashier areas and no blind spots behind the cashier where the public can observe transactions, cash storage areas, or processes.

c) Strategically located duress alarms.

d) Recorded video surveillance of the area immediately surrounding and all transactions.

16. The design and construction of cash-handling spaces and cash-collection areas should include identification of regulatory and facility requirements and expectations. Procedures or systems that address access, audit, security, and the internal operations should be carefully and cooperatively planned by all those who will be involved in the operation and protection of personnel involved in cash collection, cash handling, storage, and cashier operations material and space.

3.6 Information Technology Systems

1. The design of facilities should address the multiple ways in which information can be compromised and should protect that information applying both integrated physical and electronic security systems. The design should include access and audit systems to be applied, as appropriate, to areas including—but not limited to—storage facilities, computer training rooms, data closets, server rooms, water & wastewater stations, and communication rooms.
2. The design of areas housing Information Technology Systems (ITS) should start with the outer barrier to the space and include forced-entry protective measures that extend from slab to slab. This design should prevent access above suspended ceilings, through air ducts, cable or utility infrastructure, roof hatches, skylights, unprotected external windows, and doors.
3. Access that is restricted within a Security Zone and with the following functionality:

    a) Doors that meet or exceed standard commercial grade construction

    b) Doors that close automatically when not in use

    c) Doors that automatically lock when closed

    d) Locking devices that cannot be manually defeated

    e) Latching/locking hardware that is barrier protected (e.g., astragals, latch guards)

    f) Card access with multi-factor authentication

4. Areas should have security safeguards designed for external monitoring. An intrusion alarm system should be installed and monitored by CSS to address alarms, including but not limited to the following:
    a) Breach of an exterior entry point, via door position switches
    b) Breach of exterior openings (exterior or service windows), via glass break or shock sensors
    c) Activity within the secured space, via motion sensors
    d) Door(s) held open, via door position switches
5. The Facility should implement the design of integrated security systems to assist in the protection of ITS and the management of a safe and secure environment, considering the following:
    a) Access Control systems should be installed at entrances used by authorized staff.
    b) Video surveillance should be installed with the specific purpose of digitally archiving in accordance with regulatory requirements, facility policy, and recognized industry best practices. Facility's should consider locating video surveillance at the following locations:
        i. Main perimeter access points
        ii. Internal areas
        iii. Consideration should be given to the installation of video surveillance at the external perimeter of areas that are used primarily for the storage of ITS

3.7 Court Programs and Services

The Province of Ontario's Architectural Design Standards for Court Houses, last revised in 1999, sets building standards for security. Such standards include the need for secure screened entries for the public, separate secure entries for the Judiciary, and the separation of corridors to be used by the Judiciary, the accused, and the public. These standards have been applied for newly built court locations and for retrofit projects of existing courthouses. The design solution and use of materials should be carefully considered to meet future requirements, generated by legislation or the continued evolution of court house operations.

The design shall include:

1. Separate and secure corridors
2. Secure parking for the Judiciary

3. Sufficient holding areas
4. Security checks at public entrances which should all be monitored
5. All entrances monitored and including electronic access controls
6. Video camera surveillance in all areas accessible to the public
7. Sufficient panic buttons, monitored by CSS and alarm monitoring company specified by CSS
8. Buttons by local police and court staff

3.7.1 Duress Alarms

Placement of duress alarms should be in a discreet yet easily accessible location, often just below the desk of counter work area. In open office staff areas, they may be wall-mounted in an easily accessible location. Duress alarms should be integrated with other security systems (e.g., when a duress activates, an image on the appropriate camera should activate on a monitor in the command center).

Locations of duress alarm buttons shall include, but are not limited to:

1. In the in-custody transportation sally port
2. At all circulation areas through which an in-custody defendant may be escorted (i.e., staging areas, hallways, and elevators)
3. In the courtroom at the bench and clerk's station
4. In each chamber, reception area, and chambers conference rooms
5. At public screening stations
6. At staff screening stations
7. At public service transaction counters
8. In staff offices and work areas
9. In police/security offices and work areas
10. In interview and meeting rooms where staff meet with the public
11. For staff who have cause to come into contact with the public outside of their immediate office space (mobile duress alarms)
12. In each drug testing room provided
13. In the loading dock area
14. In the jury assembly room and in each jury deliberation room
15. In the mailroom

3.7.2 Security Cameras

Courts should ensure that security cameras have sufficient and appropriate functional capacity to meet the security requirements of the court building. Security cameras should be installed in the following locations:

1. In the sally port
2. In holding cells
3. At all circulation areas through which an in-custody defendant may be escorted (i.e., staging areas, hallways, and elevators)
4. In each courtroom
5. In hallways that access chambers
6. At security screening stations
7. At access points to critical rooms and areas such as electrical supply, roof, data centers, maintenance areas/shops, water utilities, and other building systems
8. At judges and staff entrances
9. At public service transaction counters
10. In secure waiting areas used by victims and witnesses, protective order petitioners and respondents, and other court visitors who might be at risk of assault
11. At dedicated interview areas for staff to meet with members of the public or clients who may have the potential for violence
12. In judges' parking areas
13. At the court building perimeter
14. Overlooking the inside and outside of all exterior doors
15. In staff, juror, and general public parking lots
16. At the loading dock
17. At the driveway used for transporting in-custody defendants
18. In public hallways
19. In elevators and stairwells
20. In the mailroom

3.7.3 Security Command Center

A security command center, as referenced in this document, refers to a physical location where all security activities for the court building are controlled and all security infrastructure is monitored. The building security control room serves as headquarters during any emergency. From here personnel would be dispatched in response to emergencies and external agencies would be summoned or notified. A security ”command center” has a different function than an in-custody defendant ”control room”, which is used to manage the transport and housing of in-custody defendants. In some court buildings, the command center and control room are combined into a single facility to gain building and staffing efficiencies. A command center shall be included, which will be staffed by Brantford Police Service as the provider of facility security for the court.

1. Construct a dedicated command center within the court building. The security control room should be centrally located near the main public entrance, or it may be located near or in the central holding area close to secure circulation.
2. The size of the security control room will vary with the size of the court facility. A minimum of 100 square feet should be provided, with larger units being 400 to 500 square feet.
3. Make sure that access to the command center is carefully restricted. No unauthorized persons should have access to the security control room. Access to the life safety equipment panel should be limited to building management. Also located with the central security control room is the protective equipment such as security and duress alarms, fire alarm, emergency elevator control, public address system, fire alarm enunciator panel, etc.
4. Configured to permit continuous monitoring of monitor duress alarms and security cameras at the command center. Install control panels and monitoring equipment for security surveillance cameras, duress alarms, fire alarms or alerts, intrusion detection systems, and telephone and radio communication and dispatch. As noted above, all
5. Provide alarm panels or posted diagrams at the command center. Control panels should clearly identify locations in the court building to include rooms clearly and logically numbered to aid in emergency response.
6. Establish telephone/radio communication points between the security desk and potentially vulnerable areas of the court building, such as courtrooms and chambers.
7. Establish telephone/radio communication between the security desk and local law enforcement, and/or emergency dispatch entities.

8. Command center staff should have access to mass notification systems (e.g., public address systems, telephone notification systems, email, text, social media, etc.) installed in the court building to be able to communicate with building occupants in the event of emergencies. Staff should receive ongoing training on mass notification protocols and procedures
9. The individuals staffing the command center should not be the physical responders to a crisis. Removing them from the command center to be physically present at the scene of the crisis could result in the loss of a critical element providing situational awareness to emergency responders and staff. The situational awareness provided by the command center allows responders to make the best tactical decisions and staff to decide whether to shelter in place or run.
10. The command center should be staffed at all times when the court building is open the public. Assign a court security officer to the dedicated command center.
11. A push to lock button shall be included in location(s) specified by CSS, which would lock all electronically controlled access points (i.e. lockdown).
12. Cameras should be integrated with duress and access control (door) alarms. When a duress or access control alarm activates, an image on the appropriate camera should activate on a monitor in the command center. The command center staff should not only have the ability to view the monitor but also to communicate via audio with staff activating the alarm.
13. Provide additional monitoring capacity for critical court building infrastructure including elevators, mechanical systems, emergency generators/generator fuel levels.
14. In court buildings where the command center is situated in a vulnerable area (e.g., in the main entrance/lobby area with windows facing the exterior) and as justified by a threat assessment, provide ballistic-resistant protection over the command center’s doors, windows, and other areas subject to attack.
15. After-hours monitoring of intrusion alarms and cameras should be provided. This may be accomplished through network linkage and coordination with local law enforcement, and/or emergency dispatch entities.
16. Appropriate power and cabling should be provided for the security equipment and monitors. Multiple phone lines should include those dedicated for internal courthouse use and dedicated external lines to supporting agencies.
17. The security command center shall contain a combination desk and control panel, a lockable file cabinet, and a storage locker. The security stations are open workstations consisting of a desk and chair.

18. The security command center should have proper thermostatic and ventilation conditions, as this improves the concentration of the officers on duty. High-density lighting should be used, but not so high that it creates a glare on the television monitors.
19. All power and lighting for this room should be from the building's emergency electrical service. All equipment should be on an uninterruptible power supply and all electricity should be conditioned.
20. The security control room should have an equipment room and toilets for staff.
21. The control units and toilets should be accessible to persons with disabilities.
22. Establish the security command center as the designated safe room(s) in the court building where judges and staff can seek safety in case of a negative event. Retrofit the locking mechanism on the safe room door so that it can be locked and unlocked from the inside. Reinforce the door jamb to protect against the door being kicked in. Install a duress alarm in the safe room. Make sure that room has adequate ventilation, communication equipment, and supplies (e.g., food and water) to support a reasonable length of stay.

3.7.4 In-Custody Defendants

1. Establish one or more dedicated holding cells where in-custody defendants may be held while waiting for their court hearing.
2. Provide sight and sound separation, as required or appropriate, of different in-custody populations within secure in-custody holding and transportation areas (e.g., male, female, and juveniles). The design of these areas should prohibit unauthorized access by the public and escape by in-custody defendants.
3. Install security cameras (with tamper-resistant housings) in holding cells.
4. Install security cameras along the entire in-custody defendants' escort route including staging areas, hallways, and elevators.
5. Install duress alarms in circulation areas through which an in-custody defendant may be escorted (i.e., staging areas, hallways, and elevators).
6. Establish a secure sally port for in-custody defendants entering the court building. The sally port should be equipped with a security camera and duress alarm.
7. Provide remote video and audio linkages (and supporting infrastructure) to allow for reliable connectivity between the court and the detention centers for both adult and juvenile populations. Alternatively, establish a courtroom in the detention center(s) for advisements/arraignments and other hearings. From a security perspective, either measure minimizes the number of in-custody

defendants brought into the courthouse and is a preferred solution to bringing in-custody defendants back and forth to the court buildings, particularly for arraignment settings and non-evidentiary hearings.

8. The presence of in-custody defendants poses inherent security risks for those who work in and visit court buildings. During the COVID 19 Pandemic many state courts took steps to reduce and minimize the number of in-custody defendants brought into court buildings on a regular basis. These steps included:
    a) Providing technology tools connecting courtrooms remotely to detention centers and jails (for both adult and juvenile populations) to minimize the number of in-custody defendants brought into the court building.
    b) Providing suitable and adequate space to efficiently conduct remote proceedings at detention centers and jails.
    c) Limiting the number of transportation events to necessary in-court hearings for individuals in custody or receiving services pursuant to court order, including combining hearings (subject to maximum gathering size and to minimize the mixing of populations to eliminate avoidable quarantines when such individuals are returned to custody following court hearings). Continuing to implement such steps, even in the aftermath of the Pandemic, will have a beneficial impact on the safety and security of court buildings.
9. Establish a control room to manage the transport and housing of in-custody defendants. The control center should include monitoring capacity and control of all doors, elevators, cameras, and alarms within the secure in-custody defendant circulation area.
10. The control room should be staffed at all times when in-custody defendants are present in the court building.
11. Establish and maintain complete separation between areas used for the transportation of in-custody defendants and all other areas of the court building. This includes secure circulation for a defendant from the transport vehicle, through the sally port, through secure elevators, to the holding cell, and to the courtroom to avoid crossing the path of judges, jurors, staff, or the public.

3.7.5 Courtrooms

1. Install duress alarms6 in the courtroom at accessible locations:
    a) On top of or under the working surface of the bench, plainly marked
    b) At the clerk’s station
2. Secure or remove items inside the courtroom that can be used as weapons (e.g., scissors, staplers, metal water pitchers, water glasses). As substitutes for these

items, use Styrofoam or paper products. Use snub nose scissors, bendable pens for defendants, and smaller staplers. There should be no drawers in plaintiff's or defendant's tables. Secure or remove all moveable furniture. (Moveable or folding chairs can be secured by fastening them together with secure ties around their legs.)

3. Install and then regularly test emergency lighting/fire equipment in courtrooms.
4. Install door scopes (i.e., peepholes) for the judge's entry into the courtroom.
5. Keep presentation tables and podiums a safe distance away from the bench.
6. Install two security cameras in all courtrooms:
    a) One camera should be installed on the wall behind the bench facing the litigation area and public seating as described in a previous Step.
    b) A second camera should be installed in the back of the public seating area facing the litigation area. Establish separate entrance approaches and appropriate access controls into courtrooms for judges and court staff, jurors, in-custody defendants. Attorneys, witnesses, and the general public should enter courtrooms only through the main public entrance doors.
7. The courtroom door nearest the bench should allow the judge to quickly leave the courtroom in case of an emergency or security event and should lock behind the judge to thwart the pursuit by a potential assailant. If the door is required for public exit in the event of an emergency, a delayed egress device should be installed in accordance with local building codes.
8. Provide holding cells adjacent to courtrooms where matters involving the presence of in-custody defendants are regularly scheduled. Holding cells for the courtroom should be properly constructed, safe for the in-custody defendants, and escape-proof.
9. Install bullet-resistant materials at the bench and workstations inside courtrooms. Opaque ballistic-resistant material that meets UL Standard 752, Level III, should be installed behind the vertical surfaces on the three sides of the benches and stations that are visible to the public. Bullet-resistant fiberglass panels are a cost-effective material that can be field cut or factory cut to specific dimensions and installed on the backside of existing courtroom millwork.
10. Provide remote video and audio linkages (and supporting infrastructure) to allow for reliable connectivity between the court and the detention center(s).
11. Install an automatic electronic lock-down mechanism on the public entrance to the courtroom in case there is a security incident in the public area outside of the courtroom.

3.7.6 Chambers

1. Establish a video intercom and remote-controlled magnetic door strike system to control access into chambers areas.
2. Install blinds, preferably vertical, as interior window coverings in all chambers. Keep blinds positioned at all times so as to prevent a view into chambers from the outside.
3. Position furniture in chambers with security in mind. For example, the judge's access to the exit door should not be blocked by a visitor's chair. Also, the judge's chair should be positioned, where feasible, to avoid a direct line of sight from the outside.
4. Install a sound and light (i.e., strobe) system in the hallways by chambers to alert judges and staff when in-custody defendants are about to be escorted through the hallway.
5. Install duress alarms in chambers conference room(s).
6. Install security cameras in chambers hallways that lead to chambers areas.
7. Establish a secure path (horizontally and vertically) for judges to go from chambers to courtrooms. A separate secure path for escorting of in-custody defendants from holding cells to the courtroom without going through chambers hallways should also be established.
8. Install reflective glass or reflective film on the outside of chambers windows so that the public cannot see into these areas. Install security film on the inside of such windows. Reflective glass and film does not prevent a view into interior spaces at nighttime and does not preclude the need for window coverings. Security film is not ballistic rated but may prevent the shattering of large pieces of glass in the event of an assault.
9. Consider installing ballistic-resistant windows in areas deemed to be exposed to a specific significant threat or vulnerability (e.g., windows at ground level offices for judges and/or elected officials, presence-adjacent structures, and/or vulnerable geographic features associated with the location of the office). The recommended ballistic-resistant material for severe risk applications should meet UL Standard 752, Level IV (designed for high powered rifles).

3.7.7 Access of Public into Court Building

1. Establish only one main entrance through which the public can enter the court building.
2. Install appropriate signage at the main entrance to alert the public to what items cannot be brought into the court building and that all persons are subject to

search by security personnel. Additionally, signage should be conspicuously placed:

   a. To inform the public of any health and safety requirements in force; and
   b. To inform the public that security cameras are operating and recording activity throughout the building

3. Emergency exit crash bars should be installed on all exterior exit doors. All exit doors should be alarmed, with a ten second delay consistent with local codes. Establish signage that explains the “Exit Only” requirement. Alarms should sound at the command center and also in the immediate area of the door..
4. Ensure that sight lines from the screening station and the building entrance/exit are unobstructed to allow for appropriate visual assessment and security response.
5. Install a magnetometer at the main door (public entrance) to the court building.
6. Install an x-ray imaging system at the public entrance screening station.
7. Install a security camera at the main door (public entrance) to the court building.
8. Add a duress alarm, telephone, and lockers/lock boxes at a secure location adjacent to the screening station.
9. Install ballistic-resistant barriers at the screening station to protect screening staff.
10. Provide an appropriate number of screenings stations based on the volume of traffic regularly entering the court building.
11. Design the screening station to allow screening staff to observe the public as they enter the court building, throughout the main entrance, screening area, and lobby.
12. Provide adequate space in queuing areas to avoid overcrowding and congestion.
13. Provide re-dressing tables for visitors to organize their personal effects and belongings after going through screening. These should be located away from the screening station(s) to not interrupt the screening process for other visitors.
14. Establish clear and separate court building exit lane(s). These may be separated from the screening/queuing area with glass partitions to allow for security to observe the area. The exit lane(s) should be equipped with turnstiles for one way traffic.
15. Install reflective glass or film so that the public cannot see into the front entrance screening area but the screening station staff can see outside. Install security film on the inside of the main entry and exit doors to the court building. Such film is

not ballistic rated but may prevent the shattering of large pieces of glass in the event of an assault.

3.7.8 Access to Secure Areas within Court Building

1. Where staff are not required to use the main public entrance, designate one of the exterior doors to the building as a restricted entry for designated personnel (preferably staffed by a court security officer). Access should be controlled with an access card or key. Lawyers and jurors should not be permitted to use this door but should enter through the public entrance.
2. The VSS shall detect and allow operators in the security command center to monitor “Tailgating” events through secured doors, which should never be allowed. Tailgating is when an individual(s) enters a court building by following a person who is authorized to properly gain entry with an access card or key.
3. Establish, as feasible within the court building, the concept of circulation zones to maintain complete separation between public, restricted, and secured areas and routes within the court building. Circulations zones include the following:
    a. **Public Zone:** The public circulation system provides access from the main entrance to all publicly accessible areas of the court building. All areas that require access by the public should be accessible within the public circulation zone including courtrooms, public counter areas and court service functions, court administration, public restrooms, public elevators, and chambers reception areas.
    b. **Restricted Staff Zone:** The restricted circulation corridors, elevators and stairwells provide access for court staff, judges, escorted jurors, and security personnel to courtrooms, chambers, offices, and jury deliberation rooms. Judges and court staff should be able to move into work areas or courtrooms through private corridors and a private elevator without going through the public area.
    c. **Secure In-Custody Defendant Zone:** This zone includes in-custody defendant transport and holding areas throughout the building. The configuration of these areas should prohibit unauthorized access by the public and escape by in-custody defendants.
4. Prevent unauthorized access to critical rooms and areas such as electrical supply, roof, data centers, maintenance areas/shops, water utilities, and other building systems. Install cameras at access points to critical areas.
5. Eliminate metal keys and migrate toward electronic access devices. Only maintenance staff and emergency responders should retain keys. Where keys

are required in specific instances, issue double-cut, non-duplicate keys for use in emergencies or building maintenance purposes.

6. Prevent unauthorized access to secure storage areas containing dangerous objects and substances (e.g., weapons, toxic substances, and flammable materials). When dangerous objects and substances are maintained in the court building, they should be stored in a secure area to which access is limited to those specifically identified to have access. There should be adequate ventilation, temperature controls, and fire suppression systems as required to ensure safe storage.
7. Where applicable, establish a video intercom and remote-operated magnetic door strike system to allow permitted visitor access into secure areas.
8. Establish a universal screening policy. Universal screening means everyone entering the building is screened. (However, if there is not a separate entrance with a screening station for judges, then judges ought not to wait in a screening line at a public entrance.)
9. Install a magnetometer, x-ray imaging system, duress alarm, and security camera at the judge/staff entrance. Consider allowing jurors to use this entrance.
10. For after hours, create a single access point into the court building that is secured by a court security officer, who checks identification and signs in all people entering the building after regular hours. As time permits, the CSO should periodically patrol the interior and exterior of the court building.
11. Install delayed egress units in all doors that lead from public areas to secure areas where public transit is required through the secure area in the event of fire or other emergency. The delay should be set at 15 to 30 seconds as required by local building code officials to allow time for security personnel to respond to the access breach. The units should sound an alarm at the command center and also in the immediate area of the door to alert those inside the secure area.

3.7.8 Offices and Work Areas where Staff Interact with Public

1. Install one or more duress alarms at each work area where staff interact with the public.
2. Keep window coverings in work areas (e.g., drapes, blinds) drawn or install privacy film to restrict observation from outside.
3. Install Plexiglas-type enclosures at counters where cash is handled.
4. Ensure all public transaction counters are designed with adequate height and depth dimensions to discourage and limit attempts to jump or climb over.

5. Ensure that sensitive items such as court stamps or seals are not in reaching distance of the public standing at public transaction counters.
6. Install polycarbonate (e.g., Plexiglas barriers over all public counters. If there is no weapons screening at the court building, or if screening is materially deficient, provide ballistic rated barriers at public counters. Ballistic-rated barriers should be installed below the counter as well as above the counter.
7. Install duress alarms strategically in the office areas behind counters.
8. Install duress alarms in all interview and conference rooms where staff meets with the public (e.g., mediation rooms and assessment interview rooms). Position furniture in these rooms with security in mind. For example, staff's access to the exit door should not be blocked by a visitor's chair.
9. Provide mobile duress alarms to staff who have cause to come into contact with the public outside of their immediate office space (e.g., in common meeting rooms, restrooms shared with the public, etc.). Mobile duress alarms should have location tracking technology that will allow command center staff or other first responders to be able to immediately identify the location of the alarm.
10. Install doors with glass panes and sidelight windows in all mediation and conference rooms.
11. Install security cameras at the back of all public counters to capture the faces of members of the public conducting business at the counter.
12. Provide safe and secure waiting areas for use by victims and witnesses, protective order petitioners and respondents, and other court visitors who might be at risk of assault.
13. Install Voice over Internet Protocol (VoIP) handsets that include emergency notification features to supplement duress alarms (e.g., push-button emergency alarm notification, two-way hands-free communication with security personnel, and audible public address notification capabilities).
14. Create dedicated interview areas for staff to meet with members of the public or clients who may have the potential for violence (e.g., those on probation) rather than having staff meet with such clients in their own staff office spaces. Interview areas should include with meeting rooms/interview booths which should be accessed separately from public and staff areas. Duress alarms should be provided in individual meeting rooms/booths. The interview area should be equipped with security cameras and monitored and patrolled by a CSO.
15. Where applicable, create separate secure drug testing areas for clients who are required to give urine samples. Public or staff restrooms should not be used for this function. Install a duress alarm in each drug testing room provided.

16. Install reflective glass or film on ground floor office windows and in any offices where there may be a higher level of threat to specific staff so that the public cannot see into these office areas. Install security film on the inside of such windows. Consider installation of ballistic rated glazing in areas deemed to be exposed to an especially high threat. NOTE: Reflective glass and film does not prevent a view into interior spaces at nighttime and does not preclude the need for window coverings. Security film is not ballistic rated but may prevent the shattering of large pieces of glass in the event of an assault.
17. Consider installing ballistic-resistant windows in areas deemed to be exposed to a specific significant threat or vulnerability (e.g., windows at ground level offices for judges, presence-adjacent structures, and/or vulnerable geographic features associated with the location of the office). The recommended ballistic-resistant material for severe risk applications should meet UL Standard 752, Level IV (designed for high powered rifles).

3.7.9 Judges Parking

1. Install good quality lighting quality and intensity covering the parking lot.
2. Use reserved signs with numbers and not names.
3. Install security cameras with protective environmental housings in the judges' parking lot.
4. Install emergency call boxes in the judges' parking lot.
5. Fence-in the judges' parking lot using opaque materials such as brick or stone. If this is not feasible and instead a chain-link fence is used, install privacy slats in the chain-link.
6. Make sure that in-custody defendants are never afforded a view of judges getting in or out of their vehicles.
7. Provide sturdy vehicle access gates or overhead doors accessible by electronic devices. Install a video intercom connected to the command center.
8. Calibrate the timing of doors or gates to secure parking areas so that the doors or gates close in a timely fashion after entry of authorized vehicles to limit opportunities for tailgating.
9. Provide a secure parking area, preferably covered, for judges where they can proceed directly from their car, through dedicated elevators and through screening, and to their chambers without traversing any public areas or main court building entrance areas.
10. Consider installing a security booth checkpoint for access to secure parking in high-risk areas or have a court security officer patrol/monitor the lot.

3.7.10 Perimeter Issues

1. Provide for sufficient lighting around the building perimeter, including parking areas. Lighting should be sufficient to provide a reasonable level of safety for judges and staff going to and from the court building during hours of darkness.
2. Keep landscaping trimmed and neat to limit areas of concealment and reduce opportunities for undetected property damage and/or undetected access.
3. Make sure that there are clear, open, and non-congested lines of sight for all areas around the perimeter of the court building.
4. Make sure that there is adequate and unobstructed space for evacuation of the court building and for unfettered access by first responders.
5. Relocate all trash receptacles, newspaper kiosks, and any other items that could be used to conceal weapons or hazardous materials to a safe distance away from the court building.
6. Keep doors locked after hours and allow access only via appropriately authorized electronic access devices or keys (for back-up emergency only).
7. Install signage to indicate any areas that are restricted to public access.
8. Install exterior security cameras overlooking the inside and outside of all exterior doors. Cameras should be positioned to capture the face of all persons entering and exiting the building and recordings should be kept allowing CSO's, law enforcement, and court officials to review footage of building ingress/egress. Install exterior security cameras overlooking the inside and outside of all exterior doors. Cameras should be positioned to capture the face of all persons entering and exiting the building and recordings should be kept allowing CSO's, law enforcement, and court officials to review footage of building ingress/egress.
9. Install exterior security cameras around the perimeter (at each corner of the court building). Make sure that security cameras have a clear line of sight around the entire perimeter of the court building.
10. Install duress alarms and security cameras at the loading dock.
11. Install a security camera covering the driveway, the port and exterior areas leading to the sally port.
12. Install bollards or heavy landscape features outside main entrance doors, large ground floor windows, shipping and delivery docks, and other vulnerable or critical areas.
13. Enclose and secure all exposed gas, electric, and other utilities from public access or tampering. Secure air ducts, intakes or other openings from physical intrusion and from the introduction of any toxic substance.

14. Prohibit unauthorized motor vehicles from parking or accessing areas adjacent to or within “blast-proximity” of the court building. NOTE: the presence of unoccupied law enforcement vehicles parked around the perimeter of the court building can serve as a deterrent to unlawful activity.
15. Install emergency call boxes in both staff and public parking areas around the court building.

3.7.11 Emergency Equipment

1. Install an emergency, battery-generated lighting system in courtrooms, offices, and public areas to allow occupants to exit the building safely in the event of a power outage.
2. Ensure that proper and effective fire detection and suppression equipment, including, for example, alarms, sprinklers, hoses, and extinguishers, are properly installed and maintained, and are secured from tampering, vandalism, or sabotage.
3. Install automated external defibrillators (AEDs) located accessibly in main areas of the court building. Ensure staff are properly trained on the use of AEDs and related medical response procedures.
4. Install an emergency generator system that is properly secured and protected.
5. Install uninterrupted power supplies (UPS) for critical systems.
6. Provide basic medical/first aid supplies for all offices.
7. Install a public address system and public information display systrem for the court building to notify occupants of emergency situations and provide instructions in case of events such as building evacuations, bomb threats, medical emergencies, in-custody defendant escapes, and unruly litigants or visitors.

3.7.12 Intrusion Detection Systems

1. All exterior doors and interior doors into secure areas should have basic intrusion alarm devices, that are remotely monitored by an off-site alarm monitoring service, on-site at the security command center, and sounds locally, covering:
    a. Building ingress/egress during business and after-hours.
    b. Emergency exit doors during business and after-hours.
2. Install either glass-break or motion sensor intrusion devices that sound locally on all accessible windows. This can be accomplished with a passive infrared motion detector (PIR) in each room (or combination of rooms) that has an accessible window or by attaching a motion sensor to each window.

3. Integrate the intrusion alarms described above into the command center (or appropriate monitoring agency during after-hours) so that triggered devices sound an alarm that clearly identifies the area intruded at the court building. Alarms triggered during business hours should alert the court building's command center; when the court building is closed, the alarms should alert the command center of the appropriate responding law enforcement agency (e.g., the 911 dispatch center).
4. Integrate security cameras into the intrusion detection system described above so that cameras will be activated within the command center (or appropriate monitoring agency during after-hours) in the area(s) of intrusion.

3.7.13 Public Lobbies, Hallways, Stairwells, and Elevators

1. Provide emergency lighting in the court building, including backup generator powered lighting and lighted emergency egress signage.
2. Establish, as feasible, open hallways and lobbies with clear site lines and with no hiding spots.
3. Post floor diagrams in the hallways of the court building. Floor diagrams should be highly visible, legible, and should clearly indicate available emergency exit routes.
4. Establish egress/ingress standards regarding stairwells. For most court buildings, there should no re-entry for persons exiting into stairwells. Entry from the stairwell-side should be by controlled access only.
5. Install security cameras in court building lobbies, hallways, stairwells, elevators, and at elevator landings.
6. Provide adequate waiting space for court visitors outside of the courtrooms so that opposing parties are not kept in close proximity.
7. If there are easily lifted furniture or chairs provided in public seating areas, make sure that the furniture is fastened to the floor or tied together securely.
8. Install adequate barriers over open atriums or stairwells to prevent someone from jumping or falling.

3.7.14 Juror Security and Circulation

1. Screen jurors as they enter the court building.
2. Install a duress alarm in each jury deliberation room and in the jury assembly room. A duress alarm may be need should a medical emergency or a violent altercation among jurors occur during deliberation.

3. Juror deliberation rooms should be located within a secure area of the court building.
4. Provide restrooms for juror use only, with no public access.
5. Provide secure ingress and egress for jurors to the court building and to their vehicles to avoid the threat of intimidation or attempt to influence.

3.7.15 Cash Handling

1. Install protective barriers and duress alarms at cash counters.
2. Install security cameras in offices where cash is handled and overlooking safes.
3. Use a securely installed office safe for money storage.
4. Install appropriate alarms and sensors (i.e., security, smoke, fire, extreme moisture, and motion) on safes.

3.7.16 Screening Mail and Packages

1. Install a duress alarm in the mailroom.
2. Install a security camera in the mailroom.
3. Require all mail and packages to be processed through an x-ray imaging system.
4. Require everyone delivering mail or packages to pass through the magnetometer.
5. Delivery people and contractors should enter through the main door and be verified by an authorized representative requesting the delivery or service. Delivery people and packages should be screened through a magnetometer and x-ray machine respectively. The same procedure should be followed after verification at the main door to the court building for delivery people and contractors needing to use other external doors for service or delivery.
6. Establish a single and separate offsite screening station or location for all mail and packages delivered to the court building.

4 CONDITIONS

4.1 General

1. Items covered within this document shall not be cut and pasted as components of a consultant’s specifications. It must be referenced as a complete document and not altered in any way.

2. Compliance with these standards does not imply a completely secure environment. Instead, these requirements shall be integrated into a comprehensive site security plan.
3. Security systems for municipal government leased/owned space shall be managed solely by the City of Brantford. The use of landlord owned, and/or managed security systems is acceptable for common areas of buildings only and must not provide access to government leased space.
4. The City of Brantford shall have complete control of the operation of the system(s) while the space is occupied by the government and/or its tenants.
5. Equipment shall remain the sole property of the City of Brantford and the installing company shall not retain any ownership, access to and/or control of the system(s).
6. Hardware, software, and operating systems required for operation, including programming, shall be provided. Hard copies of all required licenses/keys shall be provided.
7. Contractors shall take necessary measures to maintain security and prevent unauthorized access to government space, assets, and information during the performance of any work.
8. Remote access to security systems is not permitted. All considerations require acceptance by CSS through the completion of a Design Deviation Request Form (DDRF).
9. All equipment work that connects to the city network must be scheduled with City IT Services before starting.
10. All network devices must have a static IP assigned using a form provided by City IT Services. The form must be completed to include the MAC, serial number and model ID of the device associated with the static IP and provided to City IT Services.

5.2 Licensing

1. The consulting, design, engineering, and commissioning of electronic security systems for the City of Brantford shall be by qualified personnel that hold professional designations applicable to the specific project.
2. Security contractors shall maintain all current licenses required to provide the specific work efforts of the project.
3. Contractors shall be certified by the manufacturer to procure, install, program, maintain, and service the acceptable system components.

4. The Contractor must have permanent full-time certified staff available in the project area to perform all necessary project cycle installation functions, including service and maintenance work following system acceptance.
5. Have staff and be able to supply information to support that their current installation and service technicians are competent factory trained and certified personnel capable of maintaining and servicing the proposed system.
6. Have a proven record of experience with similar supply and installation of equivalent systems.
7. Have been a factory certified representative for the security system products indicated, for a minimum of three years entailing design, installation, configuration, and maintenance.
8. Have comprehensive local service and support facilities in the project area for the total security systems as provided.
9. Maintain local supplies, or have access to a factory authorized organization that shall carry a complete stock of essential and expendable parts.
11. Security contractors shall utilize installation and service technicians holding an applicable security systems certification and are competent, factory trained, industry certified, and capable of installing, maintaining the system(s), and providing reasonable service. For example, technicians working on the following systems shall carry the associated technical certifications:
    a) Milestone Certified Integration Technician (MCIT)
    b) Milestone Certified Integration Engineer (MCIE)
    c) Genetec Security Center 5.x Enterprise (advanced) technical certification
    d) Genetec Security Center 5.x Omnicast™ advanced configuration and troubleshooting technical certification
    e) Genetec Security Center 5.x Synergis technical certification
    f) DMP Advanced Technician

5.3 Design Requirements

It is the responsibility of the systems design team to identify (as part of the security drawings and specifications) the City's functional requirements specific to each project, through documented communication with City client group representatives.

Security items shall be shown on dedicated drawings (Div. 28). The following items are required for review:

1. Specifications identifying the City clients' desired systems and functional requirements specific to the project.
2. Details about any infrastructure requirements, including but not limited to power or network drops.
3. Floor plans, demolition plans, riser diagrams, and detail drawings
4. Project phasing plan (where applicable)
5. All end devices and controls (e.g., card readers, motion detectors, control panels, strobes, chimes, annunciators, signal extenders, antennas, duress switches, etc.) identified.
6. Intrusion alarm, access control, door, and video surveillance hardware schedules as applicable.
7. Relative Field-of-View (FOV) drawings for all video surveillance applications.
8. IAS and ACS partitioning.

4.4 Material Substitutions

Whenever materials, equipment or processes are specified or described in this standard by using the proprietary name of an item, or the name of a manufacturer, the naming is intended to establish the type, function, standard of quality, and performance required. It is not the intent of City of Brantford CSS to exclude other materials, equipment, or processes.

Therefore, unless the proprietary named device referred to in the standards is a major system component and is followed by the words "no equal" (indicating that no substitution is permitted), materials or equipment of other manufacturers shall be considered by CSS for substitution. Major system components are manufacturer specific, and substitution shall not be permitted.

1. Consideration will be given to a proposed substitute when enough information is submitted to CSS through the Design Deviation Request Form (DDRF) to determine that the proposed material, equipment, or process is in fact equivalent (or better) in all respects to the materials, equipment, or process defined in these standards.
2. Substituted materials, equipment, or processes are not approved as equal until the item has been specifically accepted by CSS.

4.5 Training

1. Training shall be provided for two (2) hours per individual system (unless otherwise agreed) and be conducted at a time that is agreeable to both the security contractor and the City client.

2. The security contractor shall provide a list of individuals trained via an attendance sign-off sheet. This sheet shall identify the site, time, date of training, and items trained.

4.6 Warranty

1. Warranty shall be included on all components furnished, and maintenance/repair/ replacement during the warranty period.
2. The Warranty Period for all components of the new system and labour involved in their installation shall be a minimum of two (2) years from the date of Substantial Performance. The date of Substantial Performance shall be the date when all components have been certified by the Consultant, if applicable, and accepted by COB to be complete in accordance with the definition of Substantial Performance.
3. All components and their installations shall be free from defects. Any defective material or workmanship and any resulting damage to work of other trades shall be replaced or repaired as directed during the Warranty Period. The security contractor shall agree to repair or replace any components of the system that have failed within the warranty period.
4. Replace or repair all supplied defective installations. Respond and be on site within 24 hours. Provide replacement components within 24 Hours. The Contractor shall guarantee to COB that the delivery of replacement components will be provided within 24 hours.
5. Defective equipment shall be repaired onsite within 24 hours and failing this, a suitable replacement unit shall be supplied (at no additional cost and within 24 hours) to keep the system fully operational until the original unit is returned.
6. The contractor shall maintain an inventory of commonly replaced components in the local office for the replacement of failed components. Larger components shall be readily available within the North America for overnight courier shipping response.
7. Warranty certificate(s) shall include all company contact information including emergency after-hours support.
8. Schedule repair work with the Owners representative to prevent interference with normal building activities.
9. Base Tender prices shall include the cost of all replacement parts during the warranty period and all of the associated installation costs and all of the costs associated with the repair of components during the warranty period but shall not include the cost of labour for routine maintenance during the warranty period.

The cost of labour for routine maintenance shall be at the Owners request based on published labour rates provided as part of applicable pricing submissions.

10. Any software modifications or upgrades that become standard product offerings from the Contractor or equipment vendors during the warranty period shall be brought to the attention of the COB, at the discretion of COB, may be requested and, if so, shall be provided at no additional cost to COB.

4.7 Handover/Closeout Documentation

The security contractor shall provide the following minimum documentation for each system:

1. User/Installation Manuals
2. Addendums and RFI's
3. As-built drawings (CAD and PDF) showing locations of all devices, controls, panels, keypads, strobes, sirens, and demarcation points. Zones and partitions shall be clearly identified in the drawings
4. Monitoring company activity report verifying system testing
5. All installer passwords, switch configurations, serial numbers, IP, and MAC addresses
6. Warranty Certificate(s)
7. Completed Letter of Conformance (Appendix D)
8. Any completed Design Deviation Request Forms (Appendix E)
9. Electrical schematic drawings detailing connections to peripheral devices.

4.8 Reference Standards

Materials, workmanship, installation practices and/or other activities, shall meet or exceed the following reference standards:

1. CAN/ULC-S302-14 Standard for the Installation, Inspection and Testing of Intrusion Alarm Systems
2. CAN/ULC-S316-14 Standard for Performance of Video Surveillance Systems
3. CAN/ULC-S318-96 Standard for Power Supplies for Burglar Alarm Systems
4. CAN/ULC-S319-05 Electronic Access Control Systems
5. CAN/ULC-437 Standard for Key Locks
6. ANSI/TIA-568/569 Standards for Commercial Building Cabling
7. Ontario Building Code and Local Building Bylaws

8. Ontario Health and Safety Act
9. Freedom of Information and Protection of Privacy Act
10. Guidelines for the Use of Video Surveillance, Information and Privacy Commissioner of Ontario
11. City of Brantford Network Cabling Specifications.
12. City of Brantford Vertical Standards.
13. City of Brantford SCADA Standards (where applicable).
14. All other applicable Federal, Provincial and Municipal laws, regulations, and bylaws.

5 EXECUTION

5.1 Collaboration

1. Coordinate and cooperate with other trades for timely completion of the work.
2. The security contractor shall coordinate work with CSS and their appointed representatives to ensure systems are installed, programmed, tested, commissioned, and verified fully operational to the satisfaction of CSS.

5.2 Installation

1. System(s) shall be installed in a manner that is consistent with the provisions and intent of the project specific Specifications and Drawings, the referenced Codes and Standards, and in accordance with equipment manufacturers' written Specifications and Instructions.
2. Whenever systems are being installed, or upgraded, all abandoned cabling and devices shall be removed.
3. Installation and service workmanship shall be accomplished in a neat and professional manner to meet best industry standards. The security contractor is responsible for the cleanup and disposal of all garbage and debris resulting from their work.
4. The security contractor shall repair at no cost to the City any surfaces, finishes, equipment, or structures damaged by the execution of their contract, to the original condition.
5. Configuration and programming of all panels and devices associated with a specific project shall be included as a requirement within that project. All

configuration and programming shall be coordinated with City clients and match existing naming and classification schema.

6. Security contractors shall test and commission systems as fully operational and functional prior to handover. CSS reserves the right to verify the security contractor's test results to determine if system operation is satisfactory. The security contractor is responsible for correcting any deficiencies at no additional cost.
7. Cables shall be permanently identified and listed on as-built drawings as follows: cable number / source / destination.
8. Where wiring penetrating any horizontal or vertical assembly is required to have a fire-resistance rating, the rating shall be in accordance with the local AHJ. Conduits or cables shall be tightly fitted, and fire-stopped where necessary to maintain fire rating.
9. Proposed exterior installations of security equipment require landlord acceptance prior to installation, as applicable.
10. Security systems control panels, servers, storage arrays, etc. shall be wall mounted and/or installed within their own rack in the secure telecom room.

5.3 Pathways

Wiring shall be concealed unless otherwise authorized by CSS:

1. Armoured, electric metal tubing, flexible metal conduit, impact resistant PVC, or other approved conduit type specified by CSS shall be used when:
    a. Cabling is accessible to the public.
    b. Cabling may require mechanical protection.
2. Security cabling may be concealed within drop ceilings for:
    a. Staff areas
    b. Staff supervised areas (e.g., waiting room, program room)
3. Conduit connecting to field devices such as camera enclosures shall be terminated and secured up to the enclosure to conceal all wiring and connections.
4. All pathways, including but not limited to any conduit, enclosures, junction boxes, connections, and fittings must utilize security screw fasteners requiring security bits for driving or removal.
5. When applicable, the security contractor shall coordinate installation of conduit and raceways with electrical contractor to meet these requirements.

6. Where ceiling pathways are utilized, cabling and installation shall comply with ANSI/TIA 568/569 Standards.
7. All network cabling shall comply with the City of Brantford Network Cabling Specifications.

5.4 System Conductors & Cables

1. Provide cabling as required for all components as per manufacturers' requirements.
2. The security contractor shall be responsible for ensuring that all conductor types and gauges are sufficient to meet requirements for power and control on all equipment being installed for use with the system. The security contractor shall provide any related calculations on request.
3. Network cabling shall be supplied, installed, terminated, and tested to fully meet ANSI/TIA 568 Transmission Performance Specifications. Test report shall be included with the O&M Manual.
4. Cables placed in underground ducts and conduit outside of buildings shall be rated for outdoor use with water blocking membranes.
5. Ground all security equipment as per manufacturer's and AHJ requirements. Bonding conductor shall be green PVC jacketed, stranded copper and soft conductor unless otherwise noted.
6. Where fiber cable length is less than 300m, use a minimum of OM3.

5.5 Change Management

1. All changes to a system's configuration shall be logged and associated with the individual making the change.
2. System changes, updates, and patches shall be tested prior to installation in the production environment if a test environment is available. If a test environment is not available, this lack of testing shall be communicated to CSS.
3. Any other systems/processes that may be dependent on the system shall be identified and communicated to CSS.
4. A recovery plan shall be in place to restore the system should things not go as planned.
5. Post change testing is required to ensure the changed system, and any dependent systems, function as intended.

5.6 Commissioning

1. The consultant/engineer is responsible for performing an independent commissioning of the system. This shall cover functionality testing of all components within the system.
2. The consultant/engineer signs off that the system meets the full requirements of the design and standards by submitting a completed Letter of Conformance (Appendix D).
3. On-site commissioning and provision of all personnel and equipment necessary to perform these tests shall be inclusive of each project referencing work included in this standard.
4. Commissioning shall include operational verification and testing of all new and existing devices installed, modified, or associated with the scope of the project.
5. Commissioning shall include verification that all alarm signals have been received by the monitoring station.

6 GENERAL REQUIREMENTS

6.1 Operational

1. Electronic security systems shall operate 24 hours a day, 7 days a week.
2. Daylight Savings Time (DST) shall be enabled.

6.2 Products

1. Products being delivered shall be from reputable industry recognized manufacturers regularly engaged in the production of models and types of equipment used in the electronics security, computer, and telecommunications industries. Products shall be quality control tested and verified for the intended operation prior to installation at site.
2. Products shall comply with the Canadian Standards Association (CSA) or recognized approved equivalent.
3. All materials, including the hardware and software being supplied, shall be new and of the latest version or production model unless otherwise specified.
4. Foreign state-owned company products are not permitted.

6.3 Power

1. Security equipment shall be hard-wired to dedicated non-switched electrical circuits. The circuit numbers shall be clearly identified on both the electrical panel directory and security controller's (inside) panel cover.
2. Electrical breakers that control security systems equipment shall be identified as such and secured against tamper (e.g., non-padlock-able "lock dogs").
3. Each system shall have enough power supply to operate the system. The manufacturers' recommended power for the system shall be less than 80% of the power supply rated power output.
4. Security systems shall be protected by batteries and/or uninterruptable power supply (UPS) to provide a minimum of thirty minutes (30min) backup power to all security devices, when not protected by a generator. When protected by a generator, backup power shall be supplied until the generator comes online.
5. UPS equipment shall be integrated to signal the attached equipment to shut down properly in the event of a power failure.
6. Control panels shall have labels attached to their inside front covers indicating the equipment, electrical circuit, and date the battery was installed or last maintained.
7. All security systems shall be designed/installed with surge and lightning protection.
8. All surveillance cameras shall be powered over Ethernet unless power requirements exceed the maximum POE power requirements or capabilities of the connected network equipment.
9. Cameras mounted on the building exterior, landscape exterior, and PTZ:
    a. Exterior camera and associated pan/tilt/zoom drives shall be powered by POE+, or dedicated Power Supply Equipment (PSE) when:
        i. For PTZ camera and when the camera's power requirements exceed the maximum POE power requirements.
        ii. When the electric power requirement for camera's device and camera's location exceeds the maximum permissible distance of the POE switch or injector.
        iii. When the ambient temperature is below the minimum ambient operating temperature requirements for the camera.
    b. Provide exterior-rated POE injectors where necessary at camera locations to suit the installation. Provide Axis T8123-E (30W), Axis T8213-E (60W),

or approved equal, or provide dedicated PSE 24VAC or 28VAC power supply at camera locations where required. PSE shall be NEMA 4/IP66 rated when installed outdoor, or

c. Provide Centralized 24VAC or 28VAC power supply with sufficient battery backup to maintain camera's operation for a period of 8 hours upon main power failure. Located in IT telecom rooms and as indicated by CSS.

d. For multiple exterior cameras, Provide purpose manufactured VSS power supplies meeting, at minimum, the following requirements:

    i. Separate outputs for up to 16 cameras per enclosure.

    ii. Individual fuses for each camera output.

    iii. Outdoor NEMA 4 /IP66 rated for outdoor applications.

    iv. Utilize supply voltage of 120 VAC, 60Hz (105 to 130 VAC).

    v. Selectable 24 VAC or 28 VAC outputs for long wiring runs. Voltage drop shall be calculated.

    vi. AC power indication and On/Off switch.

    vii. Built-in charger for sealed lead acid or gel type batteries with automatic switchover to stand-by batteries when AC fails.

    viii. Steel powder coated enclosures.

    ix. Surveillance camera power supplies shall be Altronix or approved equal.

10. Electrical contractor shall provide 120V AC circuit on UPS at injector's and all dedicated power supply locations that are required.

11. Security Contractor shall provide all required wiring, conduits, and terminations from the camera devices, power supply units and the electric power supply circuit.

6.4 Passwords

All passwords for ESMS systems shall comply with the City of Brantford Complex Password requirements:

a. Contain a minimum of ten characters.

b. Contain characters from three of the following categories:

    i. English upper-case characters (A to Z)

    ii. English lower-case characters (a to z)

iii. Numerals (0 to 9)

iv. Non-alphanumeric keyboard symbols (e.g., ! $ # %); and,

c. Not contain the username or any proper names of the employees, City departments, entities or facilities.

d. Access/account/administrative credentials and passwords must be submitted to CSS. There shall be no passwords or access/account/administrative credentials configured without consent of the City of Brantford.

6.5 Network Connectivity

1. Intrusion alarm, video surveillance, access control, and other security systems require a connection to the City of Brantford network. No other external network connectivity shall exist.
2. Network connectivity requires an IT Service Ticket to be created by the City client group.
3. Contractor shall contact IT Service Desk (either via email itservicedesk@brantford.ca or telephone 519-759-4150 X.5555) to schedule an installation appointment. At time of appointment, technician shall be onsite and call into the IT Service Desk to provide IT Services Staff with the MAC address of the connected device(s) and confirm connectivity.

6.6 Backups

1. Administration of systems shall include backups conducted per the following requirements:
    a. Accomplishes information system backup by maintaining a redundant secondary system that is not collocated with the primary system (offsite storage or cloud-based storage) that can be activated without loss of information or disruption to operations.
    b. Onsite backup storage must be authorized by CSS following a design deviation request.
    c. System back-up procedures shall be part of initial systems training.

6.7 Telecom Rooms

Telecom rooms shall be included in the main office intrusion alarm partition when located within this protected space. Telecom rooms that reside outside of this protected space (e.g., common areas, etc.) shall be protected by a dedicated partition of the intrusion alarm.

1. Each telecom room requires:

a. Entry doors equipped with door position sensors
b. A minimum of one (1) motion detector. Additional motion detectors may be required as determined by space.
c. Intrusion alarm keypad (if required to be on its own partition)
d. Door closers for all doors that directly access the room. No door hold devices shall be installed or utilized.
e. Telecom rooms shall not be identifiable (including signage/graphics).

6.8 Door Hardware

1. Locks
    a. Grade 1 hardware is required.
2. Security Astragals
    a. Exterior doors require full-length astragals (to protect locking mechanism and deter against prying).
    b. Suite entry/exit doors and other interior doors that separate secure staff and client space, shall utilize form fitting astragals (to protect the locking mechanism only).
3. NRP (non-removable pin) Hinges
    a. NRP hinges are required when exposed, for all exterior, suite entry/exit, and other doors that separate secure staff space from client space.
4. Closers
    a. Door closers for all controlled access doors. No door hold devices shall be installed or utilized.

6.9 Key Control

1. Whenever possible, a complete keying protocol should be organized for the facility (e.g., perimeter doors locks should be keyed separately from other locks).
2. Keys, and any information needed to reproduce keys, should not be stored together. Master keys should remain in the building. Higher security areas/rooms should require dedicated keys.
3. Keyways shall use a “restricted” format at minimum and be engraved with “Do Not Copy”.
4. Where a higher level of security is required, keying shall be compliant with UL437 and be registered.

6.10 Physical Hardening

For locations that require a higher level of security, the following may be considered:

1. Doors
    a. Heavy duty 16 ga. solid core steel door (with steel stiffeners). Perimeter doors shall be fitted with a full-length steel astragal.
    b. Door and sidelight glazing may include heavy duty laminated glass or “attached” security window films installed to manufacturers specifications.
2. Windows
    a. Accessible windows (e.g., within 3 meters (10ft) of grade), may be protected with laminated glass or “attached” security window films installed to manufacturers’ specifications
3. Walls, Roofs and Floors
    a. Interior demising walls shall be full height (slab to slab/roof) as required by technical standards. To increase the level of security, the following options may be considered:
        I. Walls, roofs, and floors may be constructed with 3.5mm (10 ga.) expanded metal mesh as a secure material layer where required.
        II. Construct the wall with a material designed to resist penetration (e.g.,13mm (1/2”) plywood or particle board) as a backing to the outer layer of gypsum board wall finish.
        III. Construct the wall in the following order (from the exterior inwards):
            i. 16mm (5/8”) gypsum wall board (or as per AHJ requirements)
            ii. 3.5mm (10 ga.) expanded metal mesh
            iii. 19mm Plywood or OSB
            iv. Framing
            v. 16mm (5/8”) gypsum wall board
            vi. Where openings cannot be avoided at the ceiling plenum area, the area shall be completely enclosed with 3.5mm (10 ga.) expanded metal mesh.

6.11 Systems Hardening

1. Controller, expander, power supply and other security systems related enclosures shall be serviceable and have tamper-protection monitored as a supervised zone on the intrusion panel.
2. Systems shall be set up in a protected network environment, or by using a method that assures the system is not accessible via a potentially hostile network, until it is secured.
3. Access to systems shall be controlled and restricted to authorized personnel only. CSS approval is required for access to be given, changed, or removed.
4. Services, applications, and user accounts that are not being utilized shall be disabled or uninstalled.
5. Methods shall be enabled to limit connections to services running on the host, to only authorized users of the service. Software firewalls, hardware firewall, and service configuration are a few of the methods that may be employed.
6. Methods shall be taken to disable the network, USB, and other ports that are not being utilized.
7. Systems shall provide secure storage for data as required by confidentiality, integrity, and availability needs. Security can be provided by means such as, but not limited to encryption, access controls, file system audits, physically securing the storage media, or any combination thereof deemed appropriate.
8. Security devices shall have the default user/password changed. The changed user/password shall be documented and submitted as per this document. Passwords should be unique to each device and compliant with Section 6.4.

7 INTRUSION ALARM SYSTEMS (IAS)

7.1 General

1. A monitored intrusion alarm system (IAS) is a mandatory minimum requirement for securing any office, building or other City of Brantford space. The IAS is designed to detect unauthorized entry into protected spaces. Locations that provide services directly to the public shall also have a monitored duress alarm that complies with the requirements of this document.
2. Installation must be fully compliant with applicable standards for a security alarm system, including but not limited to UL 681 Standard for Installation and Classification of Burglar and Holdup Alarm Systems as well as UL 827 Standard for Central Station Alarm Services.

3. Installation includes the provision of all field equipment, mounting hardware, wiring, cable, terminations, expansion devices, and I/O modules required to support the various alarm points and/or systems. Installation also includes any related programming, setup, and testing of system functionality.
4. The IAS control panel shall have enough zone inputs so that each device shall be connected to a single zone (double doors may be grouped as a single zone) and be home-run to the intrusion panel. Do not gang, daisy chain, or group devices.
5. The IAS may be divided into separate partitions (areas) as required.
6. Configuration shall include integrated functionality and communication between the City's VSS and ACS as specified by CSS, including but not limited to monitoring and tracking movements of individuals throughout a facility, monitoring status and alerts for intrusion alarm being disarmed, armed or triggered, and displaying critical information from all systems in a single interface.
7. Once the system installation is deemed substantially completed, the security contractor shall not access the system either physically or electronically without CSS consultation and written permission.
8. Intrusion protection shall be provided by way of hardwired door and window position sensors, with dual technology motion detectors (Note: glass break detectors shall only be used as an additional layer to motion detection for high security areas).
9. Each partition of the IAS shall have at minimum, the following devices:
    a. Keypad
    b. Door/Window Position Sensors (all entry/exit points)
    c. Motion Detectors (covering all accessible perimeter windows, entry/exit doors, and main pathways)
    d. Interior Siren
10. Control panels shall have labels attached to their inside front covers indicating the applicable zone descriptors.
11. Devices shall be supervised with End-of-Line Resistance (EOLR). EOLR shall be installed at the end device, not within the panel.
12. If used, terminal strips shall be mounted securely within an approved enclosure.
13. Upon completion of programming, the installer shall initiate an upload of the panel programming to the monitoring station.

14. Confirmation of all alarm signals received, with a report detailing the system's programming and configuration, shall be provided by the security contractor as part of the project document submittals.
15. IAS shall include all associated equipment for a fully-functional system, including but not limited to:
    a. Keypad at main entrance(s)
    b. Network control panel
    c. Transformer(s)
    d. Batteries
    e. Tamper switch
    f. Enclosure with lock and key
    g. Network alarm communicator with LTE cellular communicator backup
    h. Wireless receiver(s)
    i. Power supply, transformer
    j. Cable plus cable covers (i.e. raceway ducts and joint covers)
    k. PIR sensors
    l. Door contacts
    m. Glass break sensors
    n. Remote access and management interface to be included and configured
    o. Card reader for arm/disarm function
    p. Wireless PIR sensors, including, but not limited to distribution in the following areas:
        i. Lobby of main entrance(s)
        ii. Vestibule(s)
        iii. Interior of entry/exit doors, including emergency exits
        iv. Corridors
        v. Other high-traffic areas
16. Standard of Acceptance:
    a. DMP Aqualite 7073A
    b. "No Equal"

7.2 Auto-Arming and Cancellation

Intrusion alarms shall auto-arm at multiple times (minimum 4) during evenings and weekends. The auto-arming schedules shall be performed by the IAS.

1. Recommended auto-arming times are 6pm, 8pm, 10pm, 12am (M-F) and 10am, 2pm, 6pm, 9pm (S-S).

    a. Consult City Client to develop a schedule that compliments the operational requirements of each location. The intention is to start auto-arming shortly after the space is typically vacant.
    b. The annunciation and cancellation methods enable easy management of this process should the operational needs change intermittently.
2. Users shall quick-arm intrusion systems upon exit, with the auto-arming serving as a backup to this process.
3. An interior audible warning shall be provided for three (3) minutes whenever the system is arming, whether manually or automatically. The warning tone shall be different from an alarm siren sound (siren pulse is not permitted) and shall be heard (minimum 10dB above average ambient sound level) throughout the protected space. The security contractor shall supply any additional sound devices if the space requires them to meet this stated criterion.
4. Notification requirements include offices and/or rooms with doors that can be closed. Ensure notification (dB) levels are compliant within these spaces.
5. A method of canceling arming during the audible warning period shall be provided within 15m of any potentially occupied area(s). A momentary switch shall be used to provide this method of cancellation.
    a. Momentary switches shall only provide cancellation during arming delay and shall not be capable of disarming alarm once armed.
6. Annunciators and cancellation devices shall be located within logical proximity to one another to facilitate ease of use.
7. IAS must be connected with the ACS and VSS to enable integrated functionality, such as enabling access card credentials to be used to arm/disarm, integrated logging, monitoring as well as allowing operators to see information from all systems in a single interface.
8. Standard of acceptance:
    a. Momentary Switch: Camden CM-7000 Series (w/ green button and labelled, “hold for 2 seconds to cancel auto-arm”)
    b. Annunciator: Flush Mount Single Gang 3 Tone Chime – W Box Technologies

7.4 Programming

1. The security contractor shall be responsible for all programming of the system. This includes user codes, zone definitions, and establishing a connection to the monitoring station.

2. CSS shall supply the security contractor with all user codes to be programmed into the alarm system.
3. The panel shall be programmed in SIA or CID format.
4. The security contractor shall program the following:
    a. Multiple monitoring stations receiver addresses for redundancy.
    b. User code required to bypass zones (no forced bypass). Auto-arming may use a code with forced bypass privilege.
    c. Daily test transmission (after 00:01 – 5:00, but not on the hour)
    d. Bell/VoIP time-out shall be set at 4 minutes. Notification strobe to latch until reset.
    e. Automatic arming: multiple attempts (at least 4) throughout the unoccupied times (see Section 7.2).
    f. Automatic disarming is not permitted under any circumstance.
    g. Remote download access enabled.
    h. Intrusion panel upload code shall be changed from default and provided to the monitoring station.
    i. Installer code shall be changed from default and provided as part of the handover documentation.
    j. The security contractor shall not enable an installer's lockout.

7.5 Door/Window Position Sensors

1. Every door which leads to the protected space shall be fitted with a commercial grade steel door position sensor.
2. Grade level or accessible windows that provide a large enough opening for a person, shall be equipped with a window position sensor.
3. Door position sensors shall be installed on the top, opening side of the door. Sensors shall be capable of initiating an alarm signal when the protected door is opened a maximum of 1" on the latch side.
4. Door and window sensors shall be "wide gap" type to align with false alarm reduction strategies.
5. Door and window sensors shall be a minimum of 3/8" diameter. Sensors shall be recessed unless otherwise required. If installed in wood or similar material, allow for expansion. Fill all voids with RTV silicone or equivalent.

6. Surface mount sensors shall be mounted to the door header with the associated magnet mounted to the door. Exposed cabling shall be protected.
7. Overhead door sensors shall:
    a. Have aluminum housing and be equipped with an armored cable jacket.
    b. Be floor mounted with associated magnet surface mounted to the overhead door.
8. When door position sensors are used to monitor position for both the IAS and the ACS, sensors shall be minimum double-pole-single-throw (DPST) to provide single circuit operation, suitable for end-of-line supervision and connection to both systems.

7.6 Motion Detectors

1. Motion detectors shall be used to provide internal area alarm detection covering all accessible perimeter windows, entry/exit doors, and main pathways.
2. Motion detectors shall utilize both microwave and passive infrared technology to reduce false alarms.
    a. Wall mounted motion detection preferred.
    b. 360° detectors may offer multiple modes of false alarm reduction versus dual technologies but must be suitable for the environment and application.
3. Motion detectors shall be installed, and field adjusted as per the manufacturer's specifications for appropriate coverage of the protected space.
4. Motion detectors shall have LED's disabled after initial testing is complete.
5. Standard of Acceptance:

    One of the following, as approved by City of Brantford CSS:

    a. Bosch ISC-BDL2-W12G Blue Line Gen 2 Tritech
    b. Bosch DS9370 Ceiling mount

7.7 Glass Break Detectors

1. Glass break detection shall only be used as an additional layer to motion detection, for high security areas.
2. Glass break detectors shall provide low and high frequency detection to reduce the likelihood of false alarms.
3. Devices shall be installed, calibrated, and field adjusted as per manufacturer's specifications.

4. Standard of Acceptance:
    a. Bosch DS1101
    b. ‘No Equivalent’

7.8 Keypads

1. No global operations permitted for keypads. Each partition shall have at least one (1) dedicated keypad.
2. Keypads shall be full alpha numeric.
3. Emergency buttons on an IAS keypad shall be disabled, unless otherwise directed by CSS.
4. Keypads shall have “Quick Arming” enabled. For example: (* then 0)
5. Keypads should be mounted so that the top of the number touchpad is no more than forty-eight (48”) above the finished floor with no obstructions in locations where wheelchair access is available only from the front.

7.9 Sirens

1. A separate interior siren shall be installed within each partition.
2. An exterior siren may be installed where possible.
3. Sirens shall be programmed for a four-minute (4 min) duration.

7.10 Alarm Notification Strobes

1. A strobe (red) shall be installed to notify returning staff that an intrusion event may be in progress and to assist responding authorities in identifying the location. The strobe shall activate until the alarm is reset by an authorized user.
2. The strobe shall be visible from the exterior of the secure space by arriving persons (e.g., viewable from window). An exception is made for sites that employ 24/7 security officers, providing for an immediate response.

7.11 Environmental Alarm Sensors

Where required, environmental alarm sensors may be installed and connected to the intrusion alarm system.

1. Environmental alarms shall be programmed as 24-hour zones and activated for continuous monitoring.
2. Environmental alarm sensors include:
    a. Low/High Temperature
    b. Water Detection

c. Carbon Monoxide / Smoke Detection

d. Process Control Faults (wastewater devices)

7.12 Network Alarm Communicators

1. The security contractor shall provide a network alarm communicator connected to the IAS for reporting alarms over the City network as per Chapter 6.5.
2. Network alarm communicator connections to the BUS/HSBS require an IT Order completed by the City client group.
3. Communicator minimum specifications:
    a. 128-bit AES encryption
    b. Compatible with 10/100BaseT networks
    c. Full duplex
    d. Reports events to at least two (2) different receiver IP addresses

7.13 Cellular Backup

1. Cellular units shall be installed in locations where there is a moderate to strong cellular signal. If an acceptable signal level cannot be found within the premise, an exterior antenna solution may be required. Exterior locations require landlord approval if applicable.
2. If a cellular back-up unit is installed, it shall be equipped with its own power supply sized to meet the maximum power requirements of the unit.
3. The cellular unit shall monitor all signals from the intrusion system. These zones shall be identified as coming from the cellular communicator.
4. The cellular unit shall be capable of connection to the monitoring station.
5. Please see Section 7.14.5 for information on cellular SIM.

7.14 Monitoring

1. The City of Brantford retains the right to monitor alarm systems in a manner of their choosing and shall not be locked into any other monitoring arrangements because of alarm system installations.
2. Security contractor shall provide connectivity (hardware & software) with monitoring station:
    a. Typical Application:
        i. Primary network connection shall be through the City of Brantford corporate network, with secondary cellular backup.

b. High Security Application:

i. Primary network connection through the City of Brantford corporate network, secondary cellular backup, and tertiary telephone line backup.

3. Backup communicators shall operate as secondary and tertiary paths if the primary communication fails.
4. If a telephone line is to be used as a communication path, the demarcation point shall be marked “Intrusion Alarm – DO NOT DISCONNECT”.
5. Monitoring is arranged with CSS’s Service Provider, who will issue all relative information including receiver addresses and cellular radio SIM.

7.15 Perimeter Intrusion Detection Systems (PIDS)

1. Perimeter Intrusion Detection Systems (PIDS) may be installed when required by the City client. The system shall comply with the requirements of this document.
2. PIDS are highly susceptible to false alarm and should only be considered for controlled environments (e.g., maintained fence and easement).
3. The security consultant/contractor is responsible for ensuring the proposed solution is suitable for the environment where it is being installed (e.g., fence type/condition, controlled easement, existing vegetation management).
4. PIDS may consist of the following:
    a. Fence Cut, Climb, Tamper Detection Systems
    b. Perimeter Beam Systems
    c. All other PIDS considerations require CSS’s acceptance through the completion of a Design Deviation Request Form (DDRF).

7.16 Fence Cut, Climb, Tamper Detection Systems

1. The fence-mounted system shall detect vibrations from cut, climb or tamper attempts to the fence fabric and subsequently identify the point of intrusion to within 3 meters (10 ft.).
2. The fence cable system zone configurations shall be based on the design criteria listed below:
    a. Zones shall not extend around corners in perimeter fencing.
    b. Considerations for zoning shall include the reduction of nuisance alarms and assessment advantages for patrol personnel.

3. The fence system shall:
    a. Detect climbing intruders with a weight of 34 kilograms (75 lbs.) with a Probability of Detection (Pd) of 95% at a 99% confidence level.
    b. Detect cuts to the fence fabric with a Probability of Detection (Pd) of 95% at a 99% confidence level.
    c. Be monitored by a dedicated partition of the intrusion alarm.
    d. Be on a dedicated AC circuit, with circuit number identified at the system control panel.
4. Fence vibration detection zones shall be monitored by a dedicated partition of the intrusion alarm.
5. Designated zones may be shunted as required by operational conditions.
6. AC power for the fence vibration detection system shall be a separate circuit, and circuit number shall be identified at the perimeter beam system control panel.

7.17 Perimeter Beam Systems

23. Unless otherwise specified, beam towers shall be:
    a. Configured in a “crossfire” pattern.
    b. Equipped with thermostatically controlled heaters.
    c. An individual alarm zone (not ganged). Designated zones may be shunted as required by operational conditions.
    d. Mounted and bolted directly onto security contractor supplied 305mm (12”) diameter concrete pedestals (sunk minimum of 813mm - 32” into the ground).
    e. On a dedicated AC circuit with circuit number identified at the system control panel.

8 DURESS ALARM SYSTEMS (DAS)

8.1 General

1. Public facing offices shall have a monitored duress alarm.
2. Duress alarms shall not be installed within unsupervised areas accessible to members of the public.

3. Duress alarms shall be installed at locations where staff interact with and provide service to the public, including, but not limited to, interview/meeting rooms and customer service counters.
4. Alarms shall be activated by hardwired devices only. Wireless duress alarm considerations require CSS's acceptance through the completion of a Design Deviation Request Form (DDRF).
5. Devices located on movable furniture shall be connected using an RJ12 wall jack and a telephone patch cord to the jack.
6. Devices (and any associated wall jacks) shall be clearly identified by a machine printed label or other professional method.
7. Duress alarms shall be connected to a dedicated, monitored partition of the intrusion alarm and be programmed as a "24 Hour Duress" alarm.
8. When the alarm is activated, a flashing blue light and chime shall sound in designated staff areas. Signals shall not be heard/seen from duress initiating location to mitigate the potential for escalation.
9. In larger offices (where direct line of sight does not exist) and in higher security environments, duress alarms shall be shown on appropriately sized graphic annunciators) to simultaneously display all activated alarms.
10. Duress partitions require a dedicated keypad for the display and resetting of alarms.
11. All equipment must be included for a fully-functional system, including but not limited to:
    a. Wireless repeater(s)
    b. Control panel
    c. Batteries
    d. Battery harness
    e. Keypad
    f. Network zone expansion modules
    g. Panic buttons
    h. Power supply, transformer
    i. Wireless receivers
    j. Cable plus cable covers (i.e. raceway ducts and joint covers)
12. In each general area, a network expansion module will be installed, which will allow all of these panic buttons to be brought back to the main control panel to be located in the telecom room.
13. Panic buttons must additionally be connected to an external 24/7/365 alarm monitoring service, which will include real-time monitoring of alarm signals and

system troubles, and alerts provided to designated recipients through phone calls from the monitoring service. The selected monitoring service must be approved by CSS.

14. The security contractor shall provide network alarm communicator that meets the requirements outlined in Section 7.12 Network Alarm Communicators.
15. The security contractor shall ensure that cellular units are installed in accordance with the requirements outlined in Section 7.13 Cellular Backup.
16. The security contractor shall ensure that the DAS is monitored in accordance with the requirements outlined in Section 7.14 Monitoring.
17. Standard of Acceptance:
    a. Audible Annunciator: 3 Tone Chime – W Box Technologies
    b. Duress Devices: Magnasphere MK-3045 (under counter / wall mount applications)

9 ACCESS CONTROL SYSTEMS (ACS)

9.1 General

1. Access Control Systems (ACS) may be installed when required by the City client. The system shall comply with the requirements of this document.

24. User information may contain business contact information (name, email, department, phone) only. The collection of photos or other personal information requires a Privacy Impact Assessment (PIA) to be accepted by CSS prior to implementation.
25. Card readers, electric locking devices, door position, request-to-exit sensors, security astragals, and NRP (non-removable pin) hinges shall be installed at all designated entry doors to the protected space (including stairwells).
26. The ACS shall include all new computer hardware, peripherals, and software necessary to operate the system as designed, including the recording of system event history. Materials shall meet or exceed the manufacturer’s requirements.
27. The security contractor is responsible for providing and maintaining all security-related devices including workstations, servers, networking hardware, etc. for the ACS.
28. The ACS shall not be dependent on the workstation/server for its operation; the access control panels shall continue to operate 24 hours a day, 7 days a week without any degradation in the operation of the system, even if the computer

hardware and software are completely disconnected from the access control panels.

29. The ACS shall have the number of cards immediately required by the tenant plus 25%.
30. For low security applications:
    a. The ACS shall be integrated with the IAS to disarm when a valid access credential is presented. Systems shall continue to operate independently in the event of integration failure.
31. For medium to high security applications:
    b. The ACS shall not be integrated with the IAS to disarm when a valid access credential is presented. For these applications users shall enter with access card and then utilize a unique code on the intrusion keypad to disarm the alarm (multifactor authentication).
32. Whenever accessible door operators are installed on an access-controlled door, the door operator shall be integrated to activate only when the door is in the “unlocked state”.
33. Communications between readers and controllers shall be OSDP V2 (Open Supervised Device Protocol Version 2).
34. A wired network security intercom is required if there is a need to remotely identify and authorize individuals requesting access to the premises.
35. A push to lock button shall be included in location(s) specified by CSS, which would lock all electronically controlled access points (i.e. lockdown).
36. Standard of Acceptance:
    - Genetec Synergis – Security Center 5.11 (or higher)
    - Genetec LP1501, LP2500, or other Genetec Controller approved by the City, depending on appropriate support for the number of managed card readers plus additional capacity requirements stipulated in this standard
    - Axis Communications I8016-LVE /A8207-VE Mk II/I8116-E network intercom with 2N® IP PHONE D7A
    - “No Equal”

9.2 Scheduling

1. Scheduling shall not be used to control the state of doors except in the following circumstances:

a. May be used to secure the door as part of the Remote Door Control solution identified within this standard.
b. May be used for multi-tenant common building entrances, when in conjunction with “first-person-in” rules.
c. May be used to control the state of a vestibule door (when other door is managed by Remote Door Control) and “first-person-in” rules are utilized.

2. All other door state scheduling considerations require CSS’s acceptance through the completion of a Design Deviation Request Form (DDRF).

9.3 Readers

The City of Brantford is migrating towards HID Corporate 1000 as the preferred access control credential format. As part of this transition path, the following requirements shall be implemented within each project:

1. New Systems:
    a. When a new system is installed, readers shall be HID Signo Seos profile, and a multi-technology credential may be used to bridge suite and base building systems.
2. Existing Systems:
    a. When an existing system requires a reader, the readers shall be HID Signo Seos multi-technology, capable of reading existing credentials.
3. Certain reader configuration changes may require authorization through HID Reader Manager Portal. All considerations require CSS’s acceptance through the completion of a Design Deviation Request Form (DDRF).
4. Bi-color LED shall provide the following minimum visual feedback: (RED = access denied, GREEN = access granted).
5. All readers shall be installed at an accessible height (48”) above the finished floor, unless otherwise directed. All wall-mounted readers shall be installed on a standard single-gang electrical back-box.
6. Exterior card readers shall be weatherproof, designed for outdoor applications, and installed on watertight boxes.
7. Readers shall be cabled according to manufacturer recommendations and for serial communications (OSDP) between controller and reader. All cables shall be sized appropriately for length and application.
8. Combination keypad/readers shall only be used for dual authentication (e.g., pin only not permitted).

9. Standard of Acceptance:
    a. HID Signo Seos:
        - Reader: 20TKS-T1-00C1W3 (mullion)
        - Reader: 40TKS- T1-00C1W3 (wall)
        - Keypad/Reader: 20KTKS- T1-00C1W3 (mullion)
        - Keypad/Reader: 40KTKS- T1-00C1W3 (wall)
    b. HID Seos/Prox (multi-technology):
        - Reader: 20TKS-00-00C1WC (mullion)
        - Reader: 40TKS-00-00C1WC (wall)
        - Keypad/Reader 20: 20KTKS-00-00C1WC (mullion)
        - Keypad/Reader 40: 40KTKS-00-00C1WC (wall)
    c. All other considerations require RPD's acceptance through the completion of a Design Deviation Request Form (DDRF).
    d. "No Equal"

9.4 Credentials

The City of Brantford is migrating towards HID Corporate 1000 as the preferred access control credential format and HID Seos credentials, as specified in the standard of acceptance below. The following requirements shall be implemented within each project:

1. New Systems:
    a. Whenever a new system is installed, credentials shall be HID Seos. A multi-technology card may be used to bridge suite and base building systems where possible.
2. Existing Systems:
    a. Whenever an existing system requires additional credentials, the existing credential type may be continued.
3. Credentials shall not have any identifying information (e.g., photo, address, department name, etc.) included or attached.
4. The standard form of credential shall be a card type unless a key fob or other form of credential is specified by CSS and a DDRF has been authorized for an exception.

5. Standard of Acceptance:
    a. HID Credentials:
        - Seos/iCLASS/Prox Card: 52064PSPGGANAN
        - Seos Key Fob (if approved by CSS): 5266PNNA
    b. Credential Formatting:
        - Corporate 1000 Format: H2007745
        - Facility Code: 7791
    c. Certain groups may utilize other Corporate 1000 formats if approved by CSS.
    d. All other considerations require CSS's acceptance through the completion of a Design Deviation Request Form (DDRF).
    e. "No Equal"

9.5 Request-to-Exit (REX) Sensors

1. REX devices shall be configured to permit egress through monitored doors by shunting door position sensors upon activation. REX device shall not unlock door(s).
2. The REX shall have a built-in buzzer to locally annunciate "door forced" and "door held open" alarms.
3. Standard of Acceptance:
    a. Bosch DS160
    b. 'No equivalent'

9.6 Electronic Locks

1. Locks shall be electrified mortise, cylindrical, strike, rim and/or exit device. All locking devices shall meet the building, fire, and electrical code requirements of all AHJ.
2. Locks shall be provided with appropriate wire transfer or electrified door hinge, which shall be cabled on the secure side of the door.
3. Electric locks shall fail-secure and be powered by 12/24VDC (unless AC is required for annunciation). Locks to be hard wired and receive power from a dedicated power supply.
4. Magnetic and wireless lock solutions are not approved for use. All considerations require CSS's acceptance through the completion of a Design Deviation Request Form (DDRF).

9.7 Door Position Sensors

1. A door position sensor is required for all access-controlled doors.
2. When door position sensors are used to monitor position for both the ACS and the IAS, sensors shall be minimum double-pole-single-throw (DPST) to provide single circuit operation, suitable for end-of-line supervision and connection to both systems.
3. Sounders shall be installed to provide local alert of delayed egress.

   Standard of Acceptance:

   a. Rutherford Controls 903 Series

   b. ‘No Equivalent’
4. Overhead door contacts shall be installed on all exterior doors and doors separating public from staff access.

   Standard of Acceptance:

   a. GE 1078 Series

9.8 Remote Door Control

Certain doors may require the ability to be locked and unlocked remotely (typically waiting rooms with client entrance doors). This is to facilitate open/close, lunch hours, and security incidents where a quick method of locking facility doors may be required.

1. A momentary switch shall be used to provide control over any and all doors specified by CSS. The switch shall be integrated with the ACS to provide control, status, and permit authorized card holders to enter even when in the “locked” state.
2. The status of the momentary switch light indicator shall follow door state (i.e. lit when locked, unlit when unlocked).
3. Accessibility buttons must shunt the door sensor to ensure free egress.
4. The relocking of doors, in the event they are accidently left unlocked, shall be protected by the following methods:

   a. Schedule to lock the door(s) at end of business hours.

   b. Integration with the IAS to lock the door(s) when the system is arming.
5. Doors shall not automatically unlock by schedule or otherwise.
6. Standard of Acceptance:

   a. Camden CM-30 Series (w/ red button and labelled “Push to Lock, Locked when Lit”)

9.9 Remote Door Release

Certain doors may require the ability to be momentarily released remotely:

1. A momentary push button switch shall be used to provide control over these doors.
2. The push button shall be integrated with the ACS for control of the door(s).
3. The push button shall be clearly labeled as to which door is controlled.
4. Standard of Acceptance:
    a. Camden CM-7000 Series (w/ red button and labelled faceplate, “Push to Open”)

9.10 ACS Servers/Workstations

1. Servers and workstations shall meet or exceed the minimum requirements specified by the ACS.
2. Servers shall be cabled directly to the access control systems and be located within the secure telecom room.
3. Workstation(s) shall be located within the secure suite space as required for administration.
4. All ACS workstations shall include a monitor, keyboard, mouse, and latest version of software (including operating system and ACS application) supported by the ACS manufacturer.

9.11 Programming

1. The security contractor shall be responsible for all programming of the system. This includes, but is not limited to, user profiles, user groups, credentials, access rules, and establishing a connection to the existing ACS and necessary configuration for centralized management.
2. CSS shall supply the security contractor with all user profiles, groups, access rules, and system information to be programmed into the ACS.

10 VIDEO SURVEILLANCE SYSTEMS (VSS)

All instances of video surveillance require an accepted Privacy Impact Assessment (PIA) prior to installation, as defined by the Office of the Information and Privacy Commissioner of Ontario. PIAs must be completed for each camera and monitor device, and must be approved by CSS prior to installation of VSS.

10.1 General

1. Video Surveillance Systems (VSS) may be installed when required by the City client and supported by an accepted Privacy Impact Assessment. The system shall comply with the requirements of this document.
2. The VSS shall not violate the rights of privacy and other legal rights of persons under observation. Signs shall be provided where routine surveillance is conducted, advising that the space is under video surveillance. Signage shall be in the languages spoken in the area. Cameras shall not be installed where there is a reasonable expectation of privacy, e.g., washrooms, changing rooms, or other similar spaces.
3. Where a VSS is being provided, co-ordinate the equipment size and mounting with the electrical consultant and City IT Services as required to ensure proper sizing of the telecom room.
4. Required camera resolutions shall be identified in drawings as Story Board, Recognize or Identify as shown in Table 11.5.4.
5. Where the manufacturer requires a camera in the system to be licensed, these licenses shall be specified within each project to accommodate the cameras specified within that design.
6. The VSS shall include all equipment necessary for a fully functioning system. The security contractor is responsible for providing and maintaining all security-related devices including workstations, servers, networking hardware, etc.
7. The VSS shall include all necessary licensed software (including operating system).
8. The VSS shall have the ability to switch frame rates on event without experiencing any loss in video recording.
9. The VSS shall have the ability to output to a DVD/R or USB drive and be complete with all programs and equipment required to view images. This may include, but is not limited to, workstation(s), kvm(s), keyboard(s), monitor(s), and mouse/mice.
10. The security consultant/contractor shall perform all calculations to ensure the systems, hardware, and networks meet the operational requirements including, but not limited to, recording parameters, throughput, number of cameras, streaming, workstations, etc.
11. Signage shall be conspicuously placed to inform the public that security cameras are operating and recording activity throughout the facility

10.2 Video Surveillance Network

1. The VSS network shall be a dedicated, isolated LAN and not be connected to other City of Brantford networks, an ISP, or any other 3rd party network.
2. The network components and performance shall meet or exceed the requirements specified by the VSS manufacturer.
3. The network shall support an IP Video Surveillance System. This includes bandwidth, throughput, QoS, security, network services, and virtualization.
4. All servers, cameras, encoders, and workstations on the network shall be configured to use the static IP addresses prescribed by the City of Brantford IT Services.
5. The host name shall be configured to match the host name prescribed by the City of Brantford IT Services.
6. Access to the NVR shall be coordinated with City of Brantford IT Services to ensure that the system is configured on the City's active directory and that City staff requiring access to the system are able to connect through the City's active directory service.
7. The network shall be physically connected and not utilize any wireless technology. All wireless considerations require CSS's acceptance through the completion of a Design Deviation Request Form (DDRF).
8. Data and other ports shall be disabled if not in use.
9. All security network cabling must meet the specifications outlined in the current version of the City of Brantford's Data Cabling Standard.
10. The VSS network shall utilize Cat 6A cabling at minimum, terminated on RJ-45 data jack receptacles at each location and modular jack patch panels in telecom room. Provide patch cords as required to connect cameras and interconnect switches at patch panels.
11. The maximum length of cable run shall not exceed 90 meters. Where cabling exceeds 90 meters, fiber optic cabling shall be used instead.

10.3 Cameras

1. Cameras shall utilize IP communications and be POE capable.
2. Cameras shall incorporate vandal/tamper resistant hardware. Level of resistance shall be appropriate for intended mounting location.
3. Color, finish, and form factor shall be coordinated with the project architect to balance the use and function while maintaining the desired aesthetic.

4. Interior cameras shall be suitable for interior installation environments.
5. Exterior cameras shall be suitable for exterior installation environments and provided with integral heaters, blowers, and seals necessary to operate within -40° to 50° Celsius (-40° to 122° F).
6. IR illumination shall be used as required to ensure that the area of interest is lit to the camera's requirements and is suitable for the scene type.
7. Cameras shall be mounted at suitable height for the required field of view and for clear unobstructed surveillance.
8. Cameras shall offer H.265 (or newer) compression.
9. Provide surveillance cameras complete with protective housings, which shall meet the following minimum requirements:
    a. Complete with all mounting hardware and brackets. Refer to security drawings for mount.
    b. Accessible, removable and lockable access doors to allow for maintenance.
    c. Allow for the adjustment of the controls without removing the camera.
    d. Power and signal cable harnesses and connectors to allow for the removal or replacement of a camera.
    e. Tamper resistant.
    f. Dome with captive shroud to conceal camera position.
10. Provide exterior mounted surveillance cameras with housings which are non-corroding and weather proof along with integral fans, powered heating elements and controls to maintain the functional operation of the cameras and controls in exposed ambient temperatures.
11. Provide appropriate camera mounts in accordance with the following requirements and are approved by CSS:
    a. All exterior camera mounts, metal tubes, brackets and accessories shall be of sufficient strength and diameter to defeat any detectable camera shake in up to 65 km/h (40 MPH) winds. All components and mounting bolts shall not rust or deteriorate and shall be designed for the surface to which the camera is mounted. All mounts shall allow for complete pan and tilt positioning achieving the required field of view with positive locking position bolts. Cameras mounted over heights greater than 6 meters (20 feet) shall be completely swiveled to a safe location for servicing.
    b. Hard-ceiling mounted fixed units shall not be J hook mounted.

c. Where electronics do not fit in camera housing coordinate imbedding an IP65 locking electronics box in base of pole or in nearest electrical ground vault. Surface boxes attached to pole are not acceptable.

d. For ceiling or wall mounted cameras, when necessary provide all required accessories (wall bracket, extension pipes) in order to install cameras below any obstructions and/or allow complete pan and tilt positions.

12. Lenses for each camera shall meet the following requirements:

    a. Provide surveillance camera lens facilities for each camera. Camera lens shall meet, at minimum, the following requirements:

        i. Glass lens appropriate for camera type, lens mount, sensor size, and camera resolution (i.e. megapixel cameras should use megapixel quality lens).

        ii. Utilize spot filters only for extreme light conditions.

        iii. Fixed cameras shall have manual varifocal lenses, which shall be auto focusing (except pinhole cameras). The lens size is identified within the camera housing types.

13. Installation of cameras in elevators shall meet the following requirements for:

    a. Cabling contractor to provide POE injector, Media converter, and Ethernet over copper extender in each elevator machine room.

    b. Security contractor to provide module boxes, and all required auxiliary VSS devices in each elevator machine room.

    c. Electrical contractor to provide 120V receptacle on emergency circuit in each elevator machine room for auxiliary VSS devices.

    d. Costs associated with electrical/cabling contractor or an elevator technician shall be included in any bid pricing.

14. Resolution of cameras shall meet or exceed the minimum requirement for each type of scene as identified in the table below:

    Storyboard: used to provide overall context and view of a larger area.

    Recognition: used to determine if movement is from a person, animal, or object.

    Identification: used to identify a person.

Scene Type	Resolution (pixels per foot)	Horizontal Resolution (pixels)	Vertical Resolution (pixels)	Maximum Horizontal Field of View (feet)	Maximum Vertical Field of View (feet)

Story Board	20 20 20	2592 3840 4000	1944 2160 3000	32 51 64	24 38 48
Recognize	40 40 40	2592 3840 4000	1944 2160 3000	16 26 32	12 19 24
Identify	80 80 80	2592 3840 4000	1944 2160 3000	8 13 16	6 10 12

15. Standard of Acceptance:

Subject to compliance with these specifications, surveillance cameras, mounts, and related components shall be manufactured by:

a. Hanwha Vision

Description	Approved Model(s)
Single-lens Dome	XNV-9083RZ
Single-lens Mini Dome	QNV-C9011R
360° Fisheye	XNF-9013RV
License Plate Recognition Single-lens Dome	PNB-A9091RDPH
180° Panoramic	PNM-C9022RV
Elevator	TNV-8011C
Dual-lens	PNM-C12083RVD
Quad-lens	PNM-C32083RVQ
Quad-lens plus PTZ	PNM-C34404RQPZ

b. “No Equal”

10.4 Video Management Software (VMS)

1. Configuration and programming of all cameras and devices associated with a specific project shall be included as a requirement within that project. All configuration and programming shall be coordinated with City clients, match existing naming and classification schema, and approved by CSS.
2. Configuration shall include various views with video feeds from specific camera devices on the VSS, as specified by CSS.

3. Configuration shall include analytics that are specified by CSS, including but not limited to license plate recognition, object detection and subject recognition.
4. Configuration shall include integrated functionality and communication between the City's VSS and ACS as specified by CSS, including but not limited to monitoring and tracking movements of individuals throughout a facility, monitoring and alerts for doors forced or held open, and displaying critical information from both systems in a single interface.
5. Configuration shall include VMS system alerts, including system health alerts, to keep users updated about any issues or problems in the VMS, including but not limited to cameras going offline and changes in status for cameras or other devices.
6. Configuration shall include collaboration with City of Brantford IT Services to connect the VMS to active directory, which is a requirement to help the City centralize and monitor user permissions, access controls and various applications within the VSS.
7. Standard of Acceptance:

   Subject to compliance with these specifications, video management software must be manufactured by:

   a. Genetec Omnicast – Security Center 5.11 (or higher)*
      *Version to be confirmed by City of Brantford
   b. "No Equal"

10.5 Servers & Workstations

16. Cameras shall have the default login information changed and passwords shall comply with Section 6.4 and be documented and submitted as per this document.
17. Cameras shall be capable of being controlled and programmed through VSS.
18. Under NO circumstances shall an empty housing or non-operational (dummy) camera be installed.
19. The selected VSS server and workstation shall support optimal function of all cameras and functionality immediately required plus 25% in consideration of system expansion and growing demands.
20. The selected VSS server shall include a minimum of RAID5 storage.
21. All systems shall include an IPMI interface for remote headless connectivity.
22. Standard of Acceptance:

Subject to compliance with these specifications and approval of CSS, the following line of security infrastructure appliances shall be utilized based on the system design, performance and capacity requirements, and equipment specifications of the following:

a. Scalable rackmount solution:
    i. Streamvault SV-2000E
    ii. Streamvault SV-4000E
    iii. Streamvault SV-7000E
c. All-in-one security:
    iv. Streamvault SV-100E
    v. Streamvault SV-300E
    vi. Streamvault SV-350E
d. Workstations:
    vii. Streamvault SVW-300E
    viii. Streamvault SVW-500E
e. Analytics Appliances:
    ix. Streamvault SVA-100E
    x. Streamvault SVA-1000E
    xi. Streamvault SVA-2000E
f. “No Equal”

10.6 Monitors

1. Monitors shall meet or exceed the minimum requirements specified by the VSS.
2. Spot monitors shall be connected to digital video decoders for their associated streams.
3. Monitors may be wall or desk mounted. Mounting hardware to be provided as part of project.
4. Monitors shall function normally without impact from radio frequencies.

10.7 Recording and Retention

1. New video surveillance systems shall utilize a NVR for recording.
2. Cameras shall record at the required resolution for scene type, with a minimum of 30 fps continuous recording 24/7/365. If motion-based recording is authorized

by CSS through an authorized DDRF, 30 seconds of pre and post event recording is required.

3. Video recordings shall be retained for a period of no less than thirty (30) calendar days. VSS shall be fully programmed to provide suitable recording times (as per City client requirements).
4. The VSS shall have the ability to record all images in a proprietary file format with forensic digital watermarking features.
5. The VSS shall be capable of extracting video in AVI format as well as the native file format with watermark. Native file format shall include an embedded player. Player shall not require installation or user privileges to play video.
6. The storage hardware shall be mounted in the secure telecom room. Security contractor shall coordinate final mounting location at site prior to installation.

10.8 Landlord Owned Systems

Landlord owned video surveillance systems should comply with the following:

1. Not be located within or provide direct views of municipal tenant space.
2. Not utilize covert methods of video surveillance without municipal tenant consultation.
3. Clearly identify purpose of video surveillance, landlord ownership and contact information, with appropriate signage for any potential video surveillance related concerns from staff or members of the public, as per the Freedom of Information and Privacy Protection Act (FIPPA).

10.9 Programming

1. The security contractor shall be responsible for all programming of the system. This includes, but is not limited to, naming devices, camera views, device settings, user groups, credentials, access rules, system alerts, system integration, analytics, and collaboration with IT Services for establishing a connection to the City’s Active Directory.
2. CSS shall supply the security contractor with all user profiles, groups, access rules, and system information to be programmed into the ACS.

11 SECURITY ANNOUNCIATION

11.1 General

1. All required annunciation means shall be readily accessible to responding personnel and shall be located as required by the AHJ to facilitate an efficient response to the event.
2. The annunciation system shall be integrated with the City's VOIP phone system.
3. Standard of Acceptance:

Subject to compliance with these specifications and approval of CSS, the following annunciation devices shall be utilized based on the application requirements:

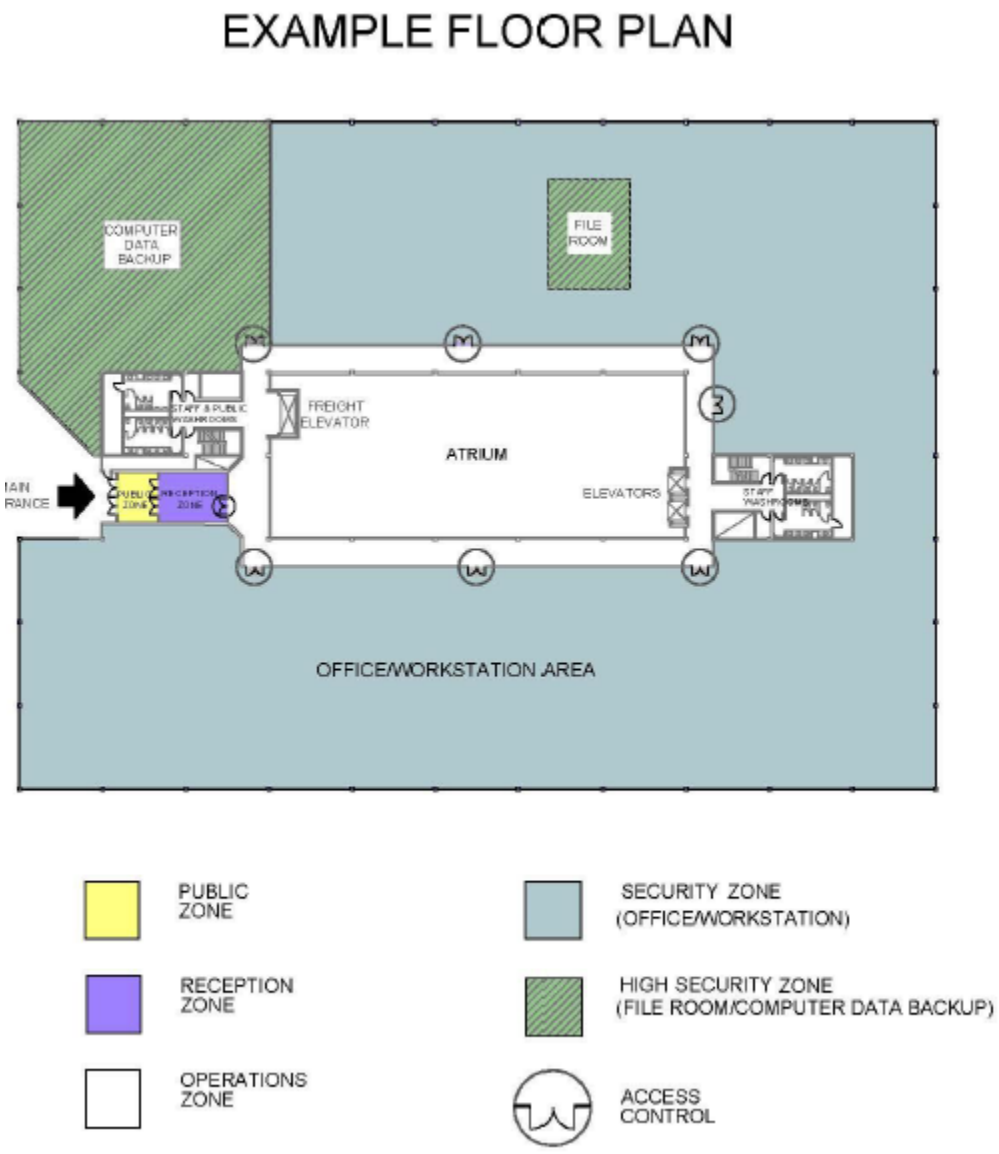
a. Axis Communications

xii. C1004-E
xiii. C1310-E
xiv. C1410
xv. C1510
xvi. C1511
xvii. C1610-VE
xviii. C1210-E
xix. C1211-E

b. "No Equal"

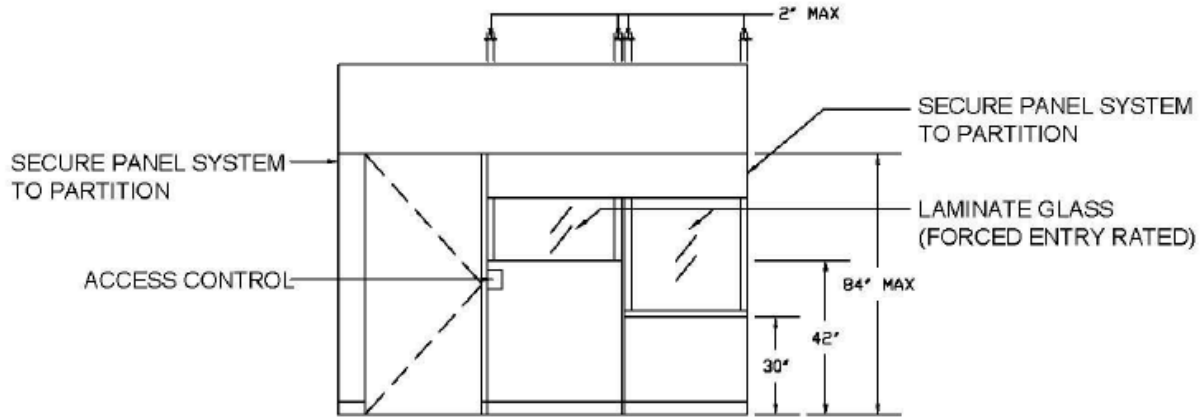
APPENDICES

Appendix A – Zones

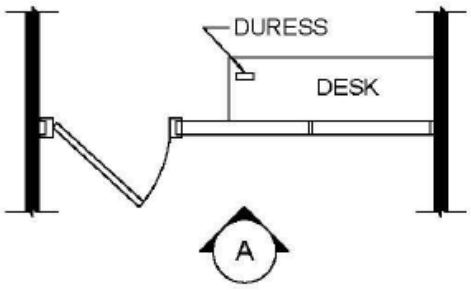


Appendix B – Secure Receptions

Low Secure Reception:

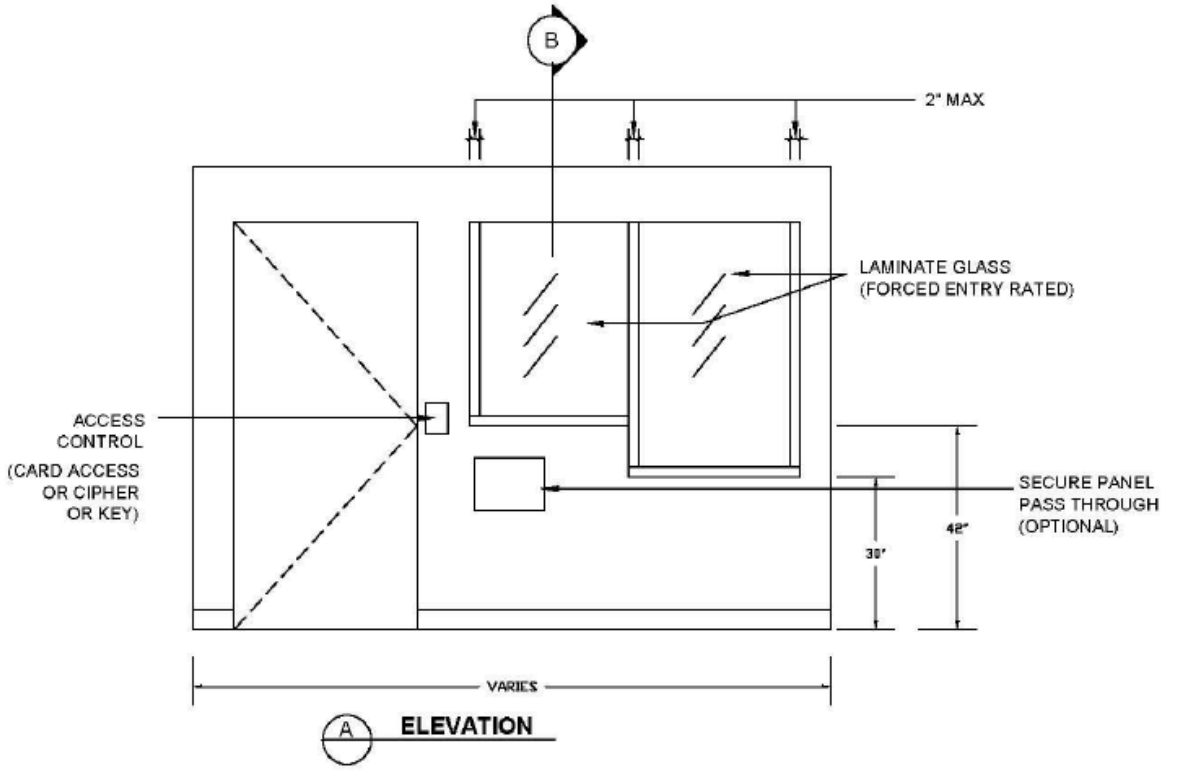


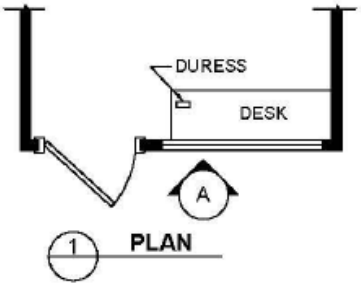
A **ELEVATION**

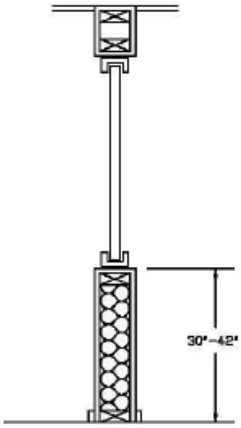


NOTE:
NO TRANSACTION TOP ON CLIENT SIDE.
MAX 2' WIDE VERTICAL PASS THROUGH.
HORIZONTAL PASS THROUGH IS NOT PERMITTED.
VERTICAL PASS THROUGH LOCATION CAN BE IN THE MIDDLE, EITHER END ONLY OR MIDDLE AND BOTH ENDS.
SYSTEM FURNITURE SOLUTION.
ENTIRE ASSEMBLY TO BE FORCED ENTRY RATED.

Medium Secure Reception:

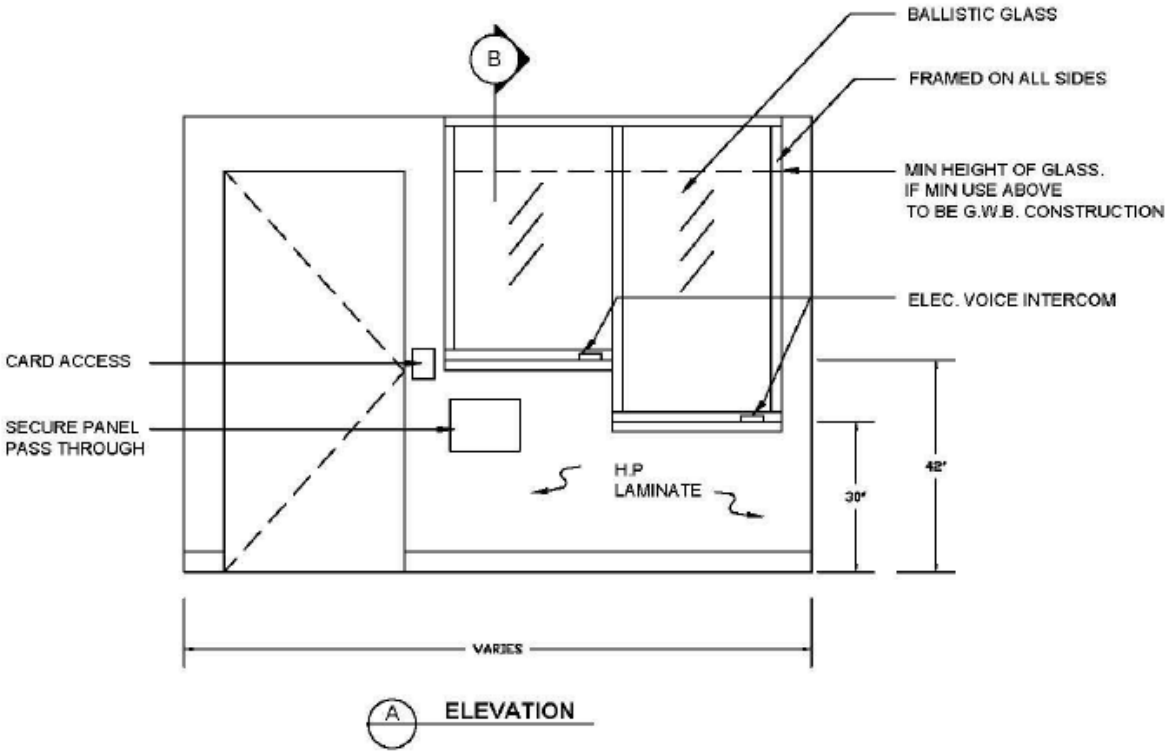


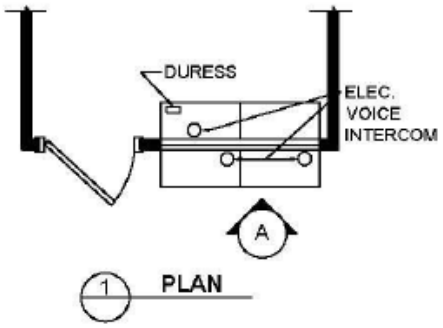




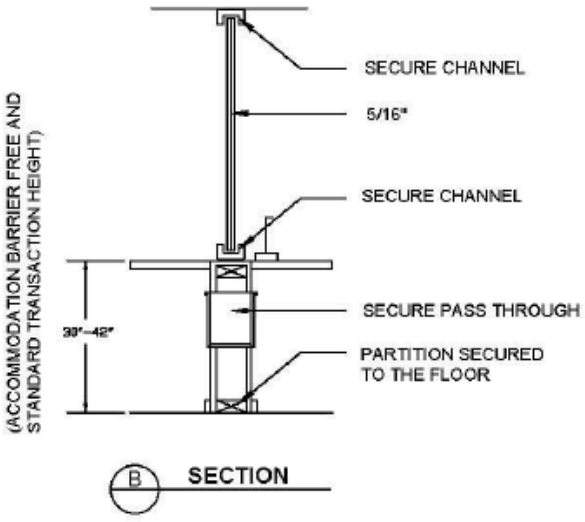
NOTE:
NO TRANSACTION COUNTER ON CLIENT SIDE.
VERTICAL PASS THROUGH.
HORIZONTAL PASS THROUGH IS NOT PERMITTED.
PARTITION CONSTRUCTION TYPE - DEMOUNTABLE OR MOVEABLE WALLS.
ENTIRE ASSEMBLY TO BE FORCED ENTRY RATED.

High Secure Reception:



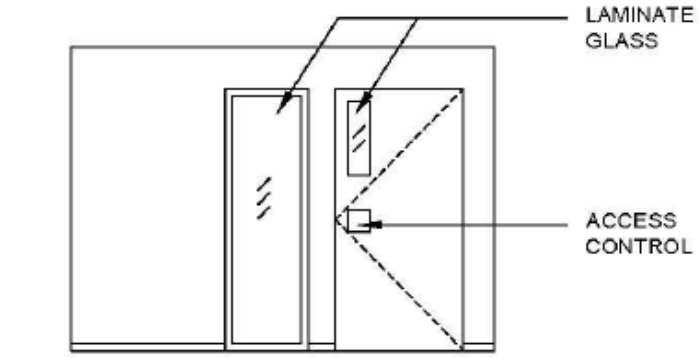


NOTE:
NO TRANSACTION COUNTER ON CLIENT SIDE.
VERTICAL AND HORIZONTAL PASS THROUGH(S) ARE NOT PERMITTED.
PARTITIONS CONSTRUCTED OF G.W.B.
ENTIRE ASSEMBLY TO BE BALLISTIC RATED.
SECURE PARCEL PASS THROUGH SURVEILLANCE SYSTEMS (PROGRAM FUNDED).

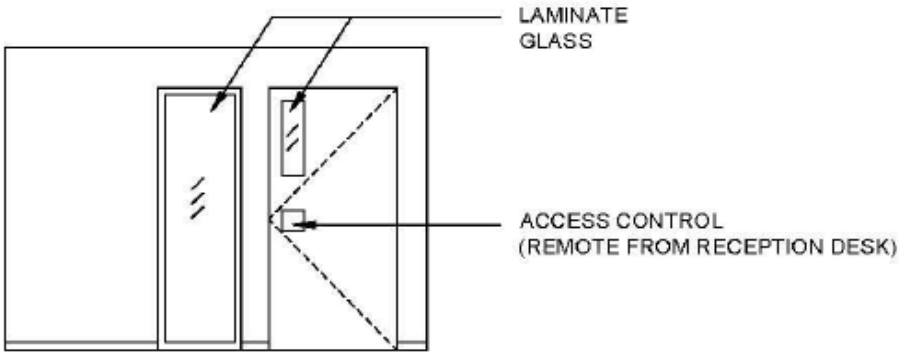


Appendix C – Secure Interview Room

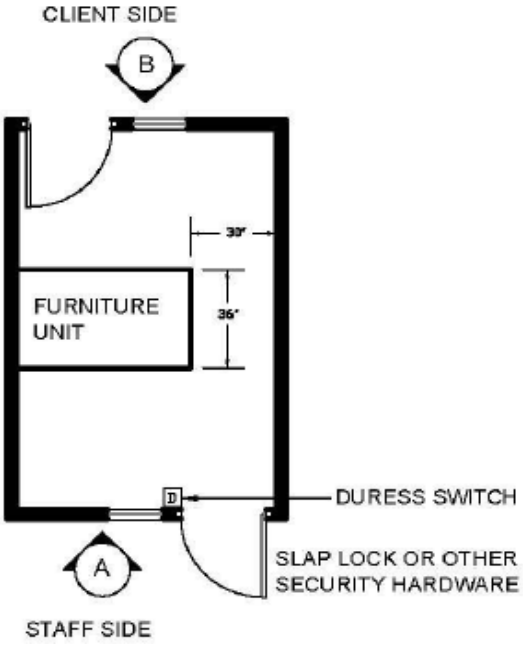
Low Secure Interview Room:



A **STAFF SIDE ELEVATION**



B **CLIENT SIDE ELEVATION**



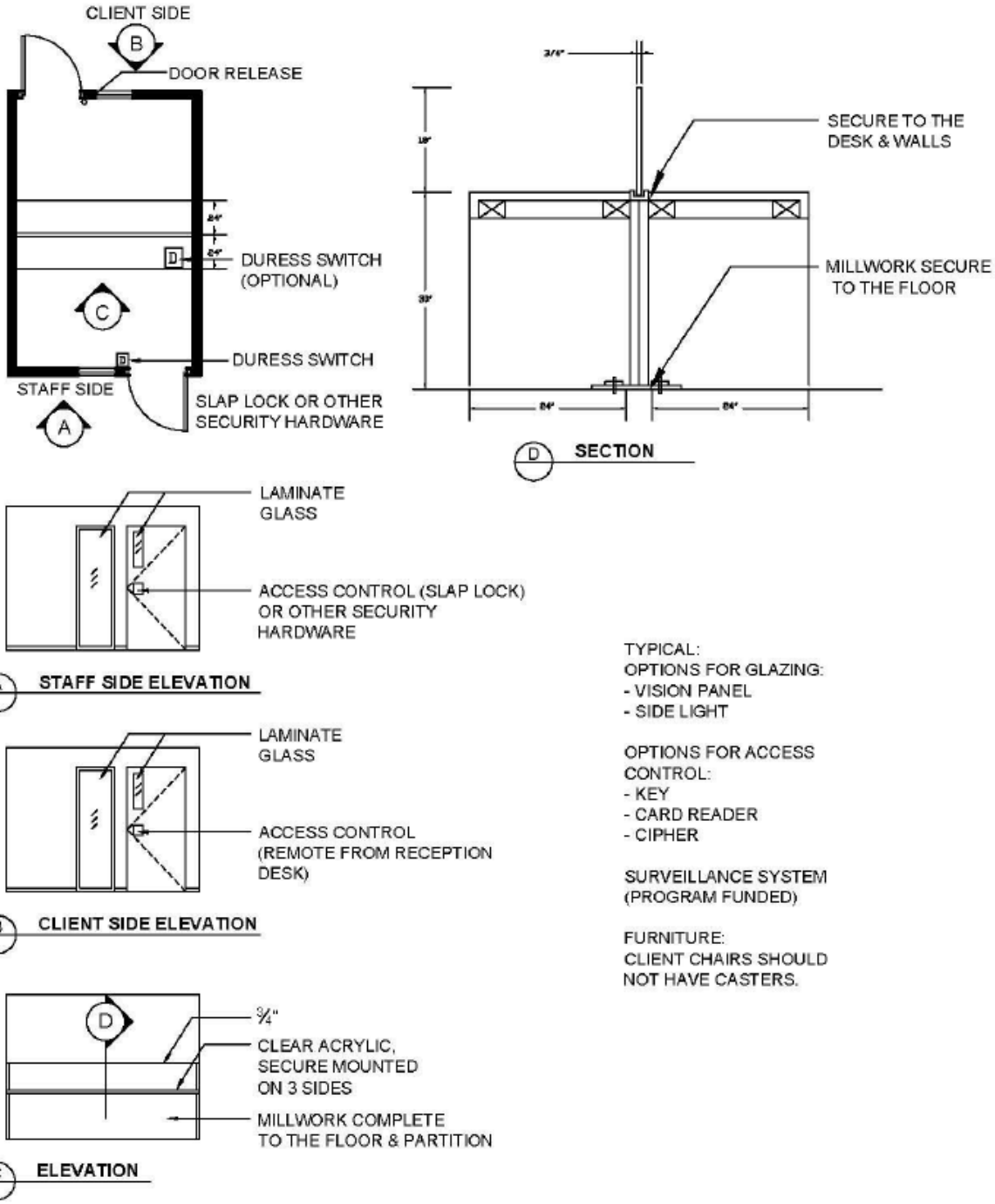
TYPICAL:
OPTIONS FOR GLAZING:
- VISION PANEL
- SIDE LIGHT

OPTIONS FOR ACCESS CONTROL:
- KEY
- CARD READER
- CIPHER

SURVEILLANCE SYSTEM (PROGRAM FUNDED)

FURNITURE:
CLIENT CHAIRS SHOULD NOT HAVE CASTERS.

Medium Secure Interview Room:



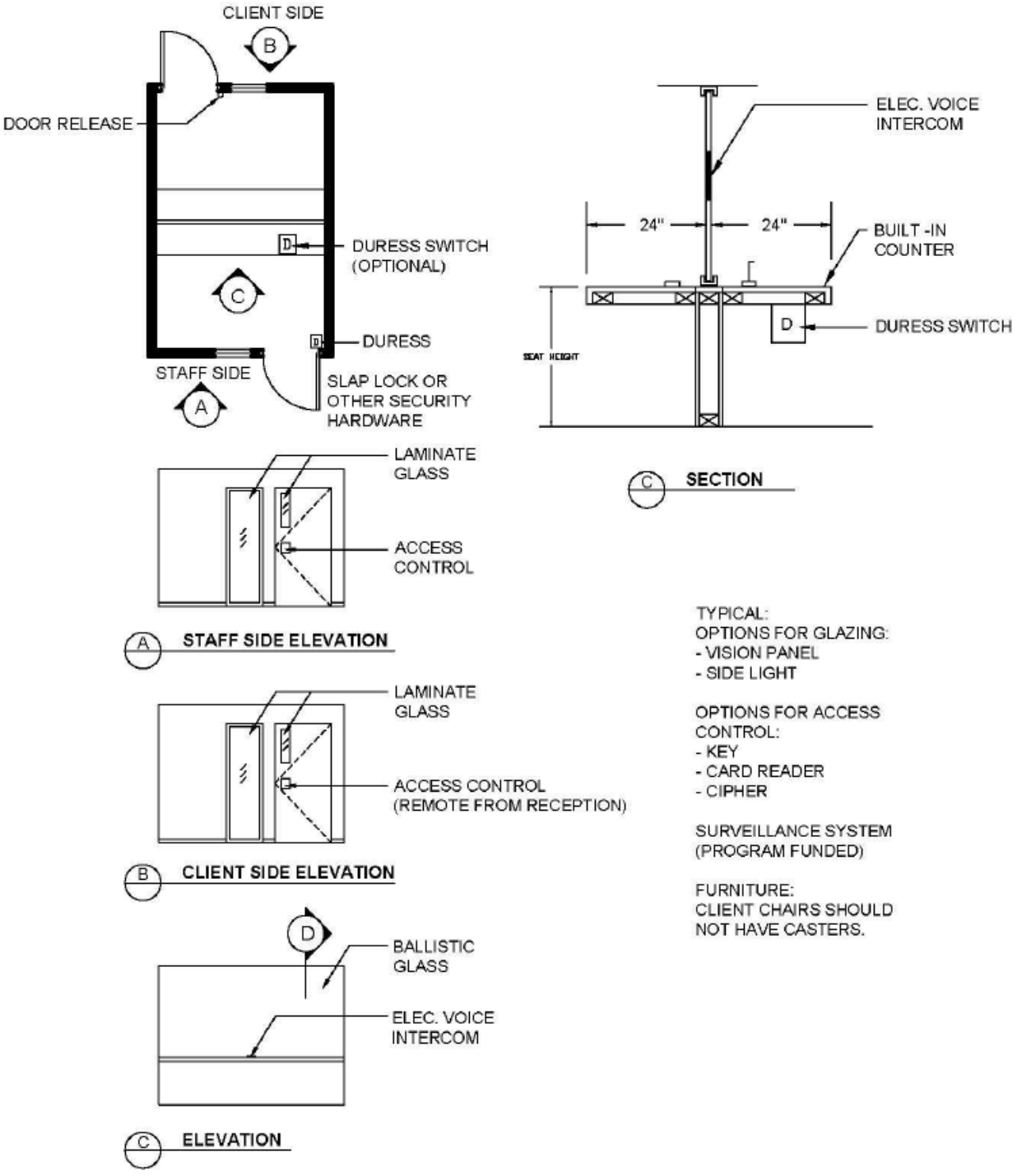
TYPICAL:
OPTIONS FOR GLAZING:
- VISION PANEL
- SIDE LIGHT

OPTIONS FOR ACCESS CONTROL:
- KEY
- CARD READER
- CIPHER

SURVEILLANCE SYSTEM
(PROGRAM FUNDED)

FURNITURE:
CLIENT CHAIRS SHOULD
NOT HAVE CASTERS.

High Secure Interview Room:



TYPICAL:
OPTIONS FOR GLAZING:
- VISION PANEL
- SIDE LIGHT

OPTIONS FOR ACCESS CONTROL:
- KEY
- CARD READER
- CIPHER

SURVEILLANCE SYSTEM
(PROGRAM FUNDED)

FURNITURE:
CLIENT CHAIRS SHOULD NOT HAVE CASTERS.

Appendix D – Letter of Conformance

BYLAW & SECURITY

Project Name:		
Instructions: The Person of Record (e.g., security engineer, designer, consultant) shall complete and sign this document. For each relative section, circle the corresponding answer below to confirm general compliance for the project. Person of Record shall complete and sign this document indicating conformance.		
Section A:		
A.1	YES / NO	Security systems are compliant with the Physical Security Standards for City of Brantford facilities and any deviations/exceptions have been identified, recorded, and accepted by CSS. Identify all deviations/exceptions in Section B.
A.2	YES / NO	Complete intrusion alarm system (including any duress alarms) has been tested and all signals have been received by the monitoring station.
A.3	YES / NO	Complete video surveillance system has been tested and all camera views have been verified and approved by CSS.
A.4	YES / NO	Complete access control system has been tested and functionality meets the requirements of the Physical Security Standards, contract documents, and CSS.
A.5	YES / NO	Record drawings have been received, reviewed and are complete. Documents have all been submitted to CSS.
A.6	YES / NO	Training has been provided as per contract documents and City requirements.
A.7	YES / NO	Security systems products and installation are in conformance with contract document and shop drawings.
Section B: Deviations as per A.1 above (attach additional sheet if required)		
B.1		
B.2		
B.3		
Person of Record:		
Name:		Company:
Signature:		Date:

Appendix E – Design Deviation Request Form (DDRF)

BYLAW & SECURITY

It is CSS's expectation that when projects are being designed and implemented, the relevant technical standards shall be followed. However, it is understood that on some projects there may be justifiable reasons to deviate from a standard (e.g.: site constraints, landlord building standards, client requirements, etc.).

Under such circumstances and in conjunction with the Project Charter, the Design Deviation Request Form (DDRF) must be completed by the consulting team and submitted by the Prime Consultant to the CSS staff assigned to the project. Submit a separate DDRF for each deviation request. Upon receipt, the completed DDRF will be reviewed by CSS for acceptance, and signed off by the CSS staff assigned to the project.

Do not assume that the deviation/exception is approved until the item has been specifically accepted by CSS. It is CSS's expectation that any design deviations would be identified during the project schematic design phase however, it is understood that there may be exceptions that may require deviations during other phases including construction.

Project Number:	Date:	DDRF Number:
Project Name:	Project Address:	
Deviation Subject Title:		
Reference Clause Number(s) from Technical Standard: (list all clauses affected and version of Technical Standard used)		
Deviation Description: (include any proposed options and supporting documentation)		

Rationale for Deviation:	
Schedule Impact:	
Budget Impact:	
Applicant Name and Company:	Applicant Signature: Date Signed:
Review Comments: (include BTA technical review comments and Consultant responses)	
Deviation Approval (CSS Use only): __ APPROVED __ NOT APPROVED CSS Representative Name: Justification: Date:	

The completed form shall be attached to the Project Charter and added to the applicable CSS Project Folder