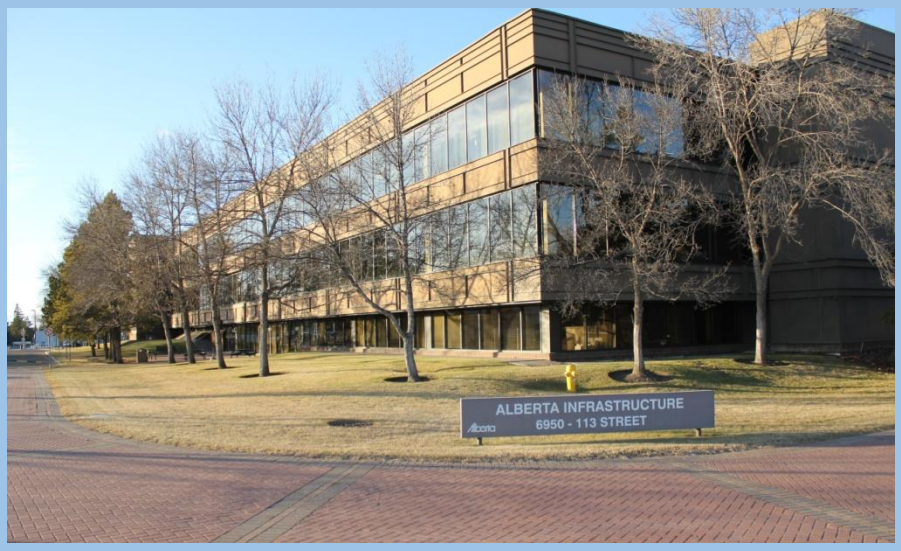
CPTED

Physical Security Guidelines & Standards for Government of Alberta Facilities



Government of Alberta

Version 2.0 – January 2018

The intent of this document is to provide guidance and discussion on Security and Safe design for facilities. National, Provincial and Municipal Codes and laws supersede this guide and shall be followed

Table of Contents

References and Acknowledgements

This document contains information gathered from many sources. We have gathered the ideas of others and applied principles of security and safety to Alberta Infrastructure standards, process and culture. The following industry leaders' body of work provides us with a basis to apply to the Government of Alberta:

- Technical Design Requirements for Alberta Infrastructure Facilities – Alberta Infrastructure
- Healthcare Security Design Guidelines – Alberta Health Services
- Technical Bulletin Issue No. 38 – Security Considerations for Secure Rooms Located in Varied Use Facilities – Alberta Infrastructure, Technical Services Branch
- Design Guide December 2010, Mental Health Facilities – Department of Veterans Affairs, Office of Construction & Facilities Management
- General Security Risk Assessment Guideline – ASIS International
- Risk Management Series, Site and Urban Design for Security, Guidance Against Potential Terrorist Attacks – FEMA 430/December 2007
- Facilities Physical Security Measures Guideline – ASIS GDL FPSM-2009
- Guide for Premises Security 2006 Edition – NFPA 730
- Guideline for Security Lighting for People, Property, and Public Spaces - IESNA G-1-03
- 21st Century Security & CPTED: Designing for Critical Infrastructure Protection and Crime Prevention, Second Edition 2013 – Randall I. Atlas

We would also like to acknowledge the efforts of many Government of Alberta staff and other industry leaders that contributed their knowledge, experiences and expertise to this Guide:

Government of Alberta
Infrastructure, Office of the Security Manager
Justice and Solicitor General, Corporate Security Services
Infrastructure, Technical Services Branch
Infrastructure, Asset Management Branch, Accommodation Planning

Document Revisions

Version	Date	Author	Revision Notes
0.1	25-April-2016	Kimberly Shaw	Draft Submitted for review
1.0	18-October-2016	Kimberly Shaw	Submitted for implementation
2.0		Kimberly Shaw	- Footnotes added to the document - Changes to the meaning and language of 4.1 - Changes and additions to 4.11 Exterior Landscaping and Wayfinding - Addition of section 5.7 Facilities in Remote Locations

Submit questions or comments to Infras.PMCSSecurityOffice@gov.ab.ca

1 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 Government of Alberta (GOA) facilities, proposed projects, and re-development. In the event that an exception needs to be made to deviate from these guidelines and standards, and or the recommendations provided by a Department Corporate Security Advisor[1], an alternate design choice should be made with a solution that meets or exceeds the recommendations. This solution should seek to eliminate, engineer or administratively control the risk/hazard.

2 Approach

The development of the guidelines and standards reflects the principles of Crime Prevention Through Environmental Design (CPTED[2]). 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 narcotic storage spaces, hazardous materials, plant utility and 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] Department Corporate Security Advisors are personnel that have the training and expertise required to complete a Physical Security Assessment Report. Final PSAR review to be conducted by Property Management Corporate Services, Office of the Security Manager (PMCS OSM)

[2] The term *CPTED* was first used by Ray Jeffrey in his book Crime Prevention Through Environmental Design (1971). According to Jeffrey, CPTED's central principle is that the proper design and effective use of the built environment can lead to a reduction in the incidence and fear of crime, as well as an improvement in the quality of life.

3 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 ministries within.

Important considerations are as follows:

1. The inclusion of a Physical Security Assessment Report (PSAR) conducted by an authorized security representative from Alberta Infrastructure, Property Management Corporate Services or Justice and Solicitor General, Corporate Security Services; 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.
2. The project design team—including the authorized security representative—should develop a comprehensive security plan that indicates a layered approach including zones, access control points, circulation routes, and required egress paths.
3. Refer to "The Roles and responsibilities Guideline" – Alberta Infrastructure, Properties Division to determine Security Management responsibility and funding allocation.

   The Roles and responsibilities Guideline
4. Client users, who have identified security and/or occupational health and safety (OH&S) concerns regarding their program space, should contact their Ministry 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 their Client Ministry Accommodation Contact (CMAC) to arrange for a physical security assessment. The completed PSAR will be sent to the Facilities Manager/Coordinator, Infrastructure's Accommodation Planner and the CMAC. Recommendations that require significant renovations to the client space must follow the procedures for Tenant Improvements.

4 General Design Guidelines and Standards

4.1 Fundamental Purpose

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

4.2 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.

4.3 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, 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.

4.4 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 Secure Receptions for specific requirements.

4.5 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.

4.6 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[3] 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

4.7 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

4.8 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.

[3] Strategies to make it harder for a crime to be committed and reduces the gains of crime.

4.9 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 Secure Interview Rooms for specific requirements.

4.10 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.

4.11 Exterior, Landscaping and 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

4.12 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[4], 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).

[4] Designing a space, providing ample opportunity to legitimate users, engaged in their normal activities, to observe the space around them.

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[5]) and Induction Lighting Systems.
8. Refer to IESNA Standards.

4.13 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 call centre staff, and those working during non-traditional hours.

1. Concentrating pedestrian egress paths to dedicated entrances and exits.
2. Locating attendant booths, parking offices and security stations where attendants can directly observe parking activity (if appropriate).
3. Installing emergency communication devices along pedestrian walkways, on each level of the structure and in all elevators.
4. Enhancing natural surveillance and line of sight.
5. Using white concrete stain to increase general brightness and enhance illumination. Painting is discouraged as it can require increased maintenance. Anti-graffiti coatings should be considered to enable quick and easy cleaning.
6. Locating elevators and stairs on the perimeter with material that allows natural surveillance from exterior public areas. Including in the design the ability to completely shut down vehicular and pedestrian access to the parking facility when closed.
7. Features that prevent and deter entry by unauthorized persons including, but not limited to, fencing, grates, metal grills, landscaping, or other protective measures.
8. Closing off potential hiding places below stairs.
9. Avoiding dead-end parking areas, areas of concealment, and limit the number of vehicular entrances and exits.
10. Any public facing facility with above grade parking structures over three levels, that provides program support for violent and or unpredictable clients, should design and install a guard wall system making it impossible to jump/climb over.

[5] Light-emitting diode: a semiconductor that emits light when conducting current and used in electrical equipment.

11. Consider having an assessment completed to ensure the Safer Parking Initiatives (SPI[6]) guidelines and recommendations are being followed.

4.14 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, 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, 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

[6] The voluntary Safer Parking Initiative program mandate is to improve the reality and perception of safety and security in parking facilities; by implementing common sense and responsible business practices, and ensure the facility follows SPI guidelines and recommendations.

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, 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, 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 the Corporate Information Security Office (CISO) for complete directives, standards and guidelines. Corporate Information Security Office

5 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 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.

5.1 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 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.

Low Secure	
Recommendations	Typical programs
- 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 the Sheriff Operational Communication Centre (SOCC) or third party monitoring company. - 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.	Examples may include but are not limited to: Human Resources

- 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	
Medium Secure	
Recommendations	Typical programs
Low security recommendations and - Recessed Front reception counter document pass through tray (not acceptable for high secure reception)	Examples may include but are not limited to: Maintenance Enforcement Program, Commercial Vehicle Enforcement, Assured Income for the Severely Handicapped
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: Probation, Crown Prosecution Services, Adult/Youth Corrections

*Program funded

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.

5.2 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 - Recessed document pass through tray (not acceptable for high secure reception) - Millwork secured to the floor	Examples may include but are not limited to: Maintenance Enforcement

	Program, Commercial Vehicle Enforcement, Assured Income for the Severely Handicapped
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 smoked domes) and video recorder	Examples may include but are not limited to: Probation, Crown Prosecution Services, Adult/Youth Corrections

*Program funded

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

5.3 Medication Rooms

Description: Storage of drugs and other narcotics

Location: High Security Zone

Recommendations:

1. The design of medication rooms should address the unique risks presented by the storage and distribution of pharmaceuticals, narcotics, controlled and targeted drugs.
2. The design should create a secure physical separation between medication room operations and the public while integrating security systems used for access and audit functions.
3. Risks related to pharmacies are primarily related to:
    a. The products received, stored, controlled, and distributed.
    b. The potential for threats and violence involving personnel and clients.
    c. The potential for internal theft of product.

Note: Refer to the Alberta Health Services – Healthcare Security Design Guidelines 2014 Edition for complete design guidelines.

5.4 Records and Information Management

Description: The creation, receipt, maintenance, use and disposal of records.

Location: Security Zone or High Security Zone

Recommendations:

The design should address the multiple ways in which this information can be compromised and should protect that information utilizing integrated physical and electronic security systems. The design should include access and audit systems to be applied, as appropriate, to electronic and hard copy document locations in areas including—but not limited to—human resources, registration, interview, clinical, health records, storage, and waste areas as well as within data systems. All areas should practice a clean desk policy.

1. During the planning and conceptual design phase, the level of security classification should be identified. The four levels of security classification include:
    a) Unrestricted – Public Information (including information deemed public by legislation or through a policy of routine disclosure). Available to the public, all employees, contractors, sub-contractors and agents.
    b) Protected – Information that is sensitive outside the Government of Alberta and needs to be protected. Authorized access (to employees, contractors, sub-contractors and agents) on a "need-to-know" basis for business-related purposes.
    c) Confidential – Information that is sensitive within the Government of Alberta and is available only to a specific function, group or role.
    d) Restricted – Information that is highly sensitive and is available only to specific, named individuals (or specific positions).
2. When designing areas that are primarily used for storage including warehouses, record rooms, data centers, or other such locations, design should address all points of entry from Public Zones as well as adjacent spaces and should include:
    a) The design 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, doors, and dumbwaiters.
    b) Access through designated doors 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. Card access.
    c) Staff should have a clear and unobstructed view from reception desk of persons requesting entry and access.
    d) Areas that are not staffed on a 24/7 basis should have security safeguards designed for internal and external monitoring. An intrusion alarm system should be installed and monitored by SOCC to address alarms, including but not limited to the following:
        i. Breach of an exterior entry point, via door position switches.

ii. Breach of exterior openings (exterior or service windows), via glass break or shock sensors.

iii. Activity within the secured space, via motion sensors.

iv. Door(s) held open, via door position switches.

5.5 Developmental Disabilities and Rehabilitation Facilities

Description: A diverse group of chronic conditions that are due to mental or physical impairments. Client may be violent and/or unpredictable.

Location: Security Zone

Recommendations:

1. The design should address the need for a safe environment for those who may present unique challenges and risks, while protecting the privacy, dignity, and health of clients and address the potential risks related to client elopement, harm to self, to others, and to the facility.
2. Design should address the variety of Facility settings that may be used, as well as, a number of factors impacting where and how care is provided including diagnosis, gender, age, length of stay, client acuity, and risk presented to themselves or others.
3. Facilities should be designed with a secure perimeter so as to control access to and egress from the facility or work unit. Perimeter design should address the following:
    a) Fencing or another type of barrier should surround any external activity areas and these areas should be designed to prevent access to roof areas and climbing of the fence or building, and limit landscaped areas that may be used for hiding or concealment. A buffer zone of at least 15 feet should be considered around the perimeter. These areas should be designed to provide good observation for staff. Activity areas housed in courtyards should follow the same principles although fencing and buffer zone requirements many not be applicable.
    b) All exterior doors should be locked at all times. These doors, if locked, will be connected to the fire alarm system and may stay locked when the fire alarm is activated (fail secure) or release on the activation of an alarm (fail safe) based on the client population and the authority that has jurisdiction. Alternate entry points to the unit should be available through exit doors for authorized responding personnel only by way of strictly controlled key or card access.
4. The internal space of the facility should be designed to provide a safe and secure environment and should consider the following design elements:
    a) There should be one primary secure entry to the work unit. A video intercom for communication to reception from outside the unit should be provided to screen visitors, clients, and staff. The door should preferably be controlled by an electronic access system utilizing an electric strike. The door may be capable of release from the reception desk if visible from that location. The door release button should not be exposed or available to a client. It should be a constant touch unlocking system where once the hand is removed from the unlock button the door re-locks.
    b) Client visiting areas designed in a location in close proximity to the main entrance and exit, including a secure area for screening separated from client treatment areas. Lockers may be provided for visitors' packages, purses, etc.
    c) Circulation routes within the work unit should be designed for staff observation, avoiding deep recesses, blind corners, and long. The corridors should provide sufficient width so that

three people could walk side by side, ideally with high ceilings and constructed with robust slab to slab walls and tamper resistant fixtures.

d) For areas not under constant observation, 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.

e) Security of unattended staff and service areas such as maintenance and housekeeping closets, and conference rooms should be designed to have the ability to be locked at all times.

f) Windows should be safety glazed or equipped with metal screening on the outside and have an opening limited to less than six inches.

g) Furniture should be designed to minimize the possibility of use for self-harm, as a ligature, as a weapon, or as a barricade.

h) Fire alarm pull stations and fire extinguisher cabinets throughout the area should be lockable and keyed so that all staff on duty are able to access these normally locked devices and cabinets with clearly identifiable keys. As an alternative, pull station covers that have a loud local audible alarm when the cover is pulled off may be considered. Consistent with fire regulations.

i) Sprinkler valves should be designed to prevent a ligature point or intentional damage resulting in water damage/evacuation.

5. Bathrooms should be designed and constructed to reduce the opportunity for self-harm. The external door should be fitted with a security lock and occupancy indicator bolt that can be overridden from the outside.

5.6 Temporary Resident Facilities

Description: Facilities that provide phased based programs for violent and or unpredictable clients. Length of stay can vary between days and months.

Location: Should be located at a facility or site that assists clients with program 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.
5. 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.
8. 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.
9. 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.
10. Staff sleeping rooms and suites should be equipped with appropriate locking hardware on entry doors. Strategically located duress alarms should be considered.
11. Access to staff lockers and lounges should be controlled at all times and restricted.

5.7 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.

5.8 Correctional Programs and Services

Description: Programs responsible for the incarceration and rehabilitation of convicted criminal offenders such as Alberta Crown Prosecution Service offices.

Location: High Security Zone. The youth justice system must be separate from the adult system (Youth Criminal Justice Act (YCJA) (2003-present)).

Recommendations:

1. Adult and youth correction programs should not be located in the same facility that provides programs and/or services for minors.
2. Careful consideration should be made to ensure correctional programs and services are not located within the same facility as vulnerable programs and services.
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. Bathrooms should be designed, 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.
5. Refer to Secure Receptions and Secure Interview Rooms, for design requirements.

6. 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.
7. Secondary staff egress/access to and from the office space. The secondary access should include:
    a. A solid core security door and frame with automatic closer.
    b. A door viewer system to allow the staff to ensure the security of the office when opening the doors to exit.
    c. A panic alarm mounted in proximity to the door in case of an incident in relation to that entry point.
8. The demising walls between this suite, adjacent tenant space and public spaces (i.e. hallways) must be slab to slab construction.
9. Staff should have access to secure, dedicated staff washrooms to ensure staff security.
10. Exterior windows should be treated to prevent internal viewing from outside of the facility and the following elements:
    a. Glass break sensors connected to an office intrusion security system.
    b. Security laminate applied to improve the ability of the glass window to mitigate the impact of force. If transparent glazing is used then drapes, blinds or other means need to be used to prevent access to classified material.
    c. Where possible should be designed to create a standoff distance between the windows and the public's access proximity to the windows.
11. The physical design of the interior offices should include:
    a. Door locks. This allows for the securing of confidential material within the office when necessary as well as to act as a temporary secure room if a security incident were to occur within the office.
    b. Offices with window panels should be coated with opaque security film designed to offer penetration resistance and a measure of concealment from view if a security incident were to occur within the office.

5.9 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 at SOCC 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 in the cafeteria, gift shop, and store front 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 parking facilities and booths, Temporary Resident Facilities, and 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.

5.10 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, 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.

    a) Refer to the Corporate Information Security Office (CISO) for complete directives, standards and guidelines. Corporate Information Security Office (CISO)

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 the SOCC 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:

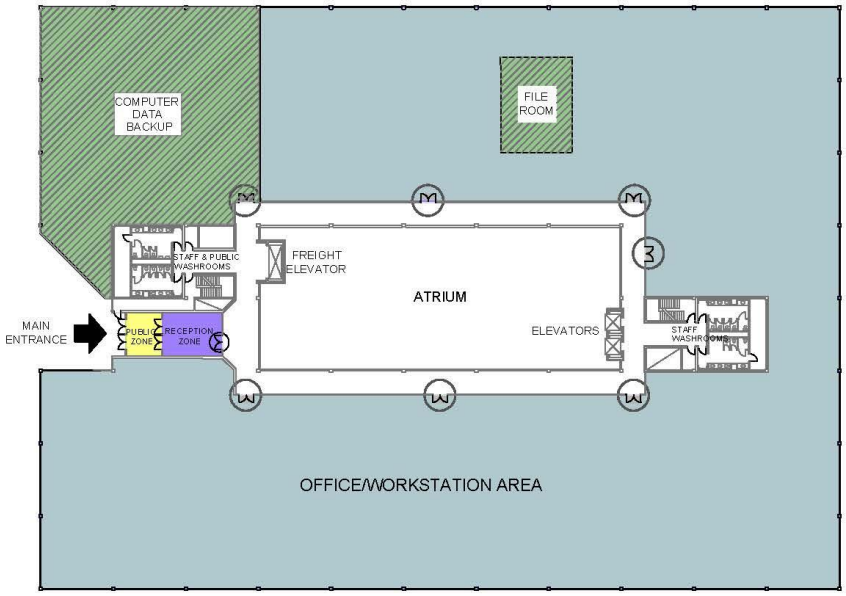
      i. Main perimeter access points.

      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.

Appendix A – Zones

EXAMPLE FLOOR PLAN



PUBLIC ZONE

RECEPTION ZONE

OPERATIONS ZONE

SECURITY ZONE (OFFICE/WORKSTATION)

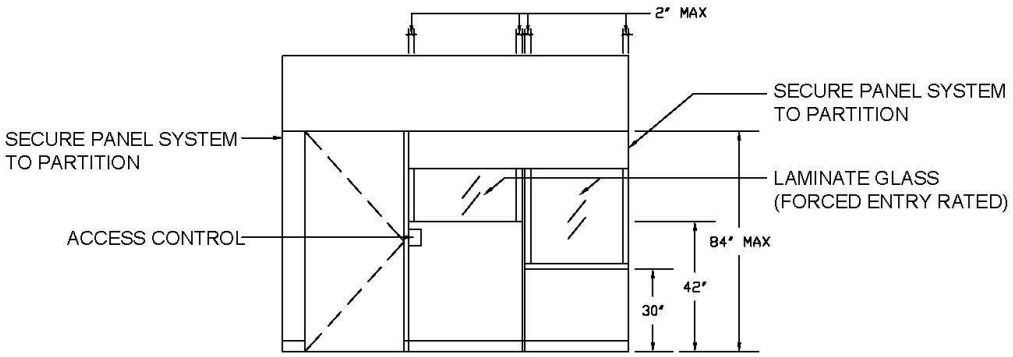
HIGH SECURITY ZONE (FILE ROOM/COMPUTER DATA BACKUP)

ACCESS CONTROL

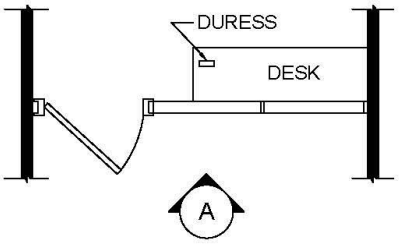
Government of Alberta
Infrastructure

EXAMPLE FLOOR PLAN
SCALE: N.T.S

Appendix B – Secure Receptions



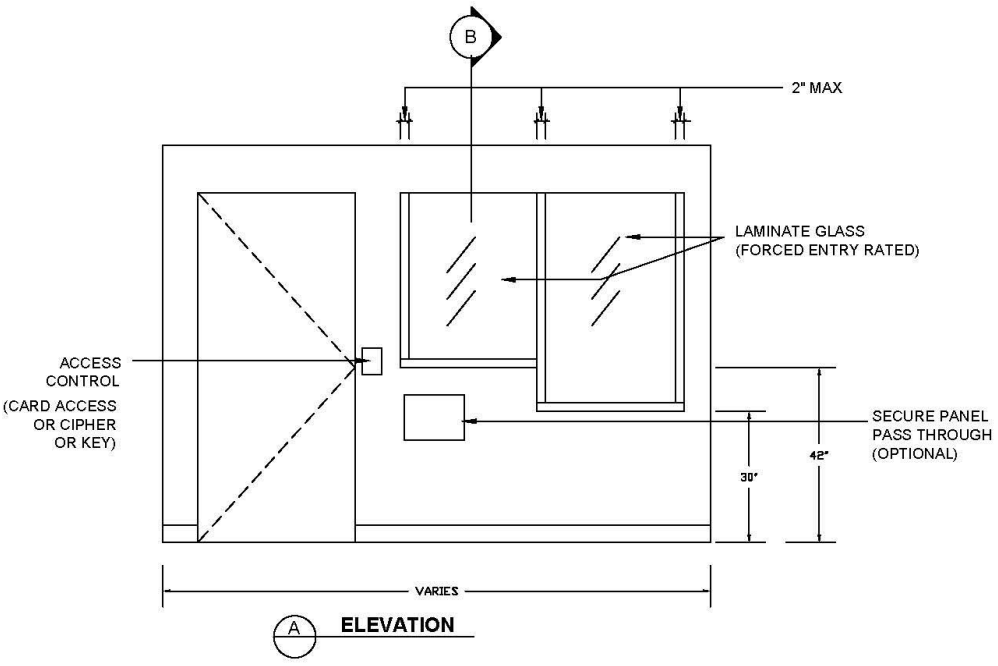
A **ELEVATION**

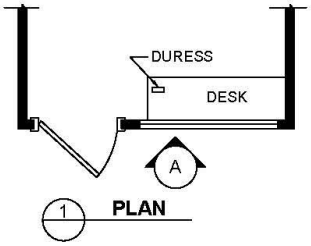


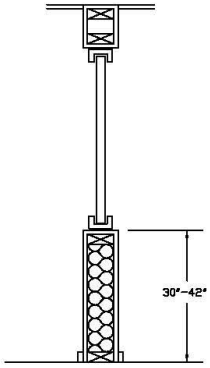
NOTE:
NO TRANSACTION TOP ON CLIENT SIDE.
MAX 2" WIDE VERTICAL PASS THROUGH.
HORIZONTAL PASS THROUGH IS NOT PERMITTED.
VERTICAL PASS THROUGH LOCATION CAN BE IN THE MIDDLE, EITHER END ONLY OR MIDDLE AND BOTH ENDS.
SYSTEM FURNITURE SOLUTION.
ENTIRE ASSEMBLY TO BE FORCED ENTRY RATED.

Government of Alberta ■
Infrastructure

LOW SECURE RECEPTION
SCALE: N.T.S



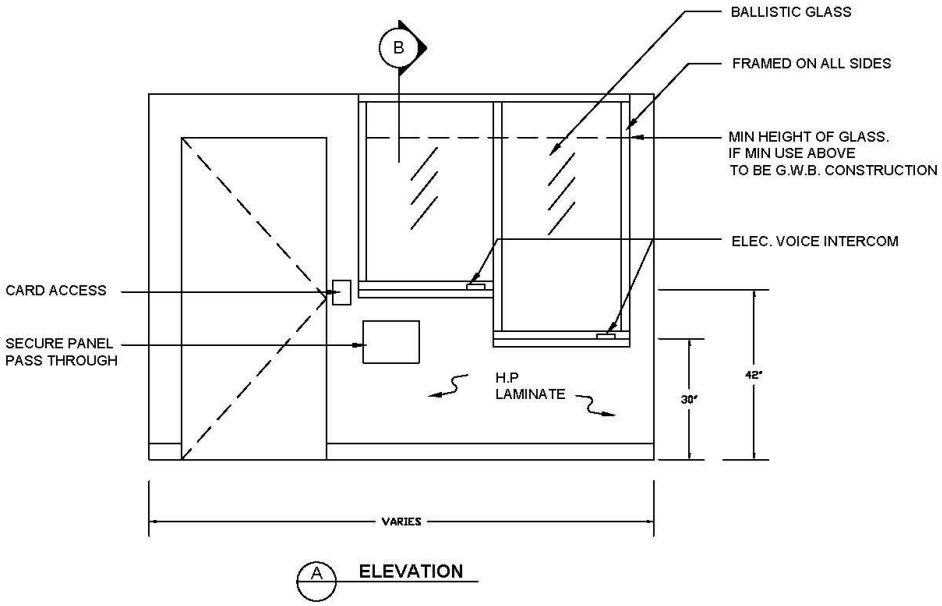


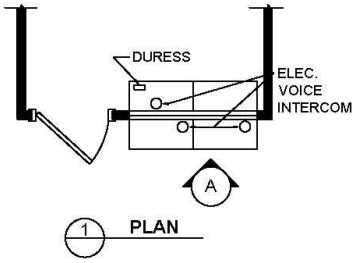


NOTE:
NO TRANSACTION COUNTER ON CLIENT SIDE.
VERTICAL PASS THROUGH.
HORIZONTAL PASS THROUGH IS NOT PERMITTED.
PARTITION CONSTRUCTION TYPE - DEMOUNTABLE OR MOVEABLE WALLS.
ENTIRE ASSEMBLY TO BE FORCED ENTRY RATED.

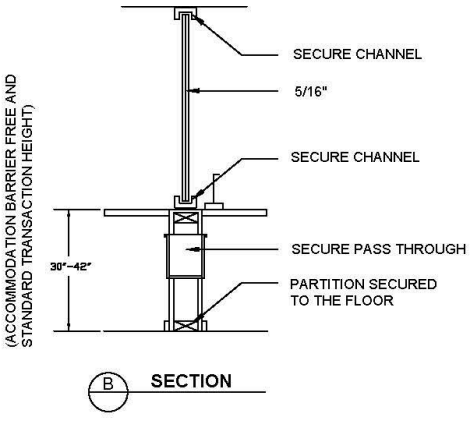
Government of Alberta ■
Infrastructure

MEDIUM SECURE RECEPTION
SCALE: N.T.S





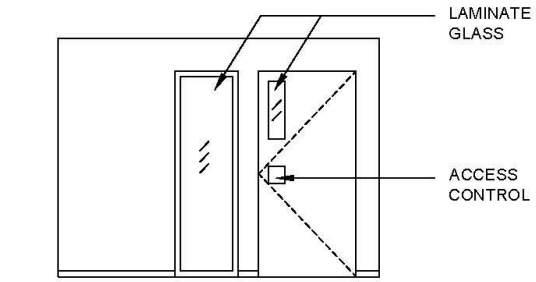
NOTE:
NO TRANSACTION COUNTER ON CLIENT SIDE.
VERTICAL AND HORIZONTAL PASS THROUGH(S) ARE NOT PERMITTED.
PARTITIONS CONSTRUCTED OF G.W.B.
ENTIRE ASSEMBLY TO BE BALLISTIC RATED.
SECURE PARCEL PASS THROUGH SURVEILLANCE SYSTEMS (PROGRAM FUNDED).



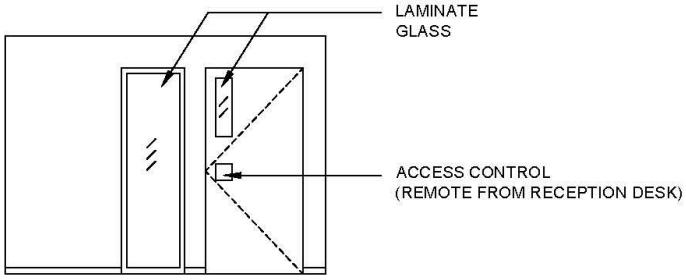
Government of Alberta ■
Infrastructure

HIGH SECURE RECEPTION
SCALE: N.T.S

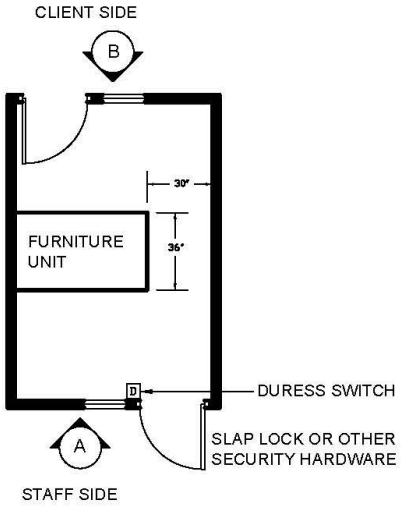
Appendix C – Secure Interview Rooms



A **STAFF SIDE ELEVATION**



B **CLIENT SIDE ELEVATION**



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

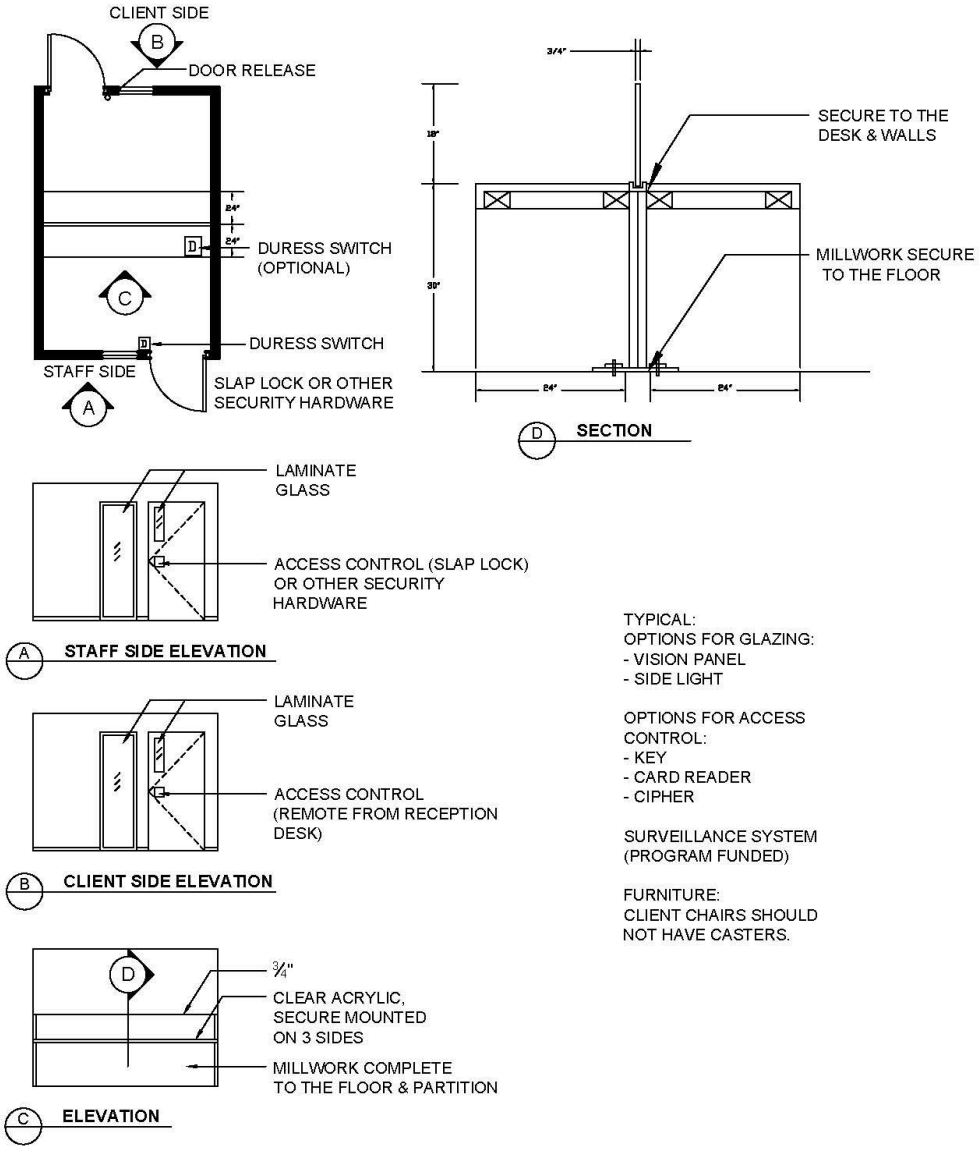
OPTIONS FOR ACCESS CONTROL:
- KEY
- CARD READER
- CIPHER

SURVEILLANCE SYSTEM
(PROGRAM FUNDED)

FURNITURE:
CLIENT CHAIRS SHOULD NOT HAVE CASTERS.

Government of Alberta ■
Infrastructure

LOW SECURE INTERVIEW ROOM
SCALE: N.T.S



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

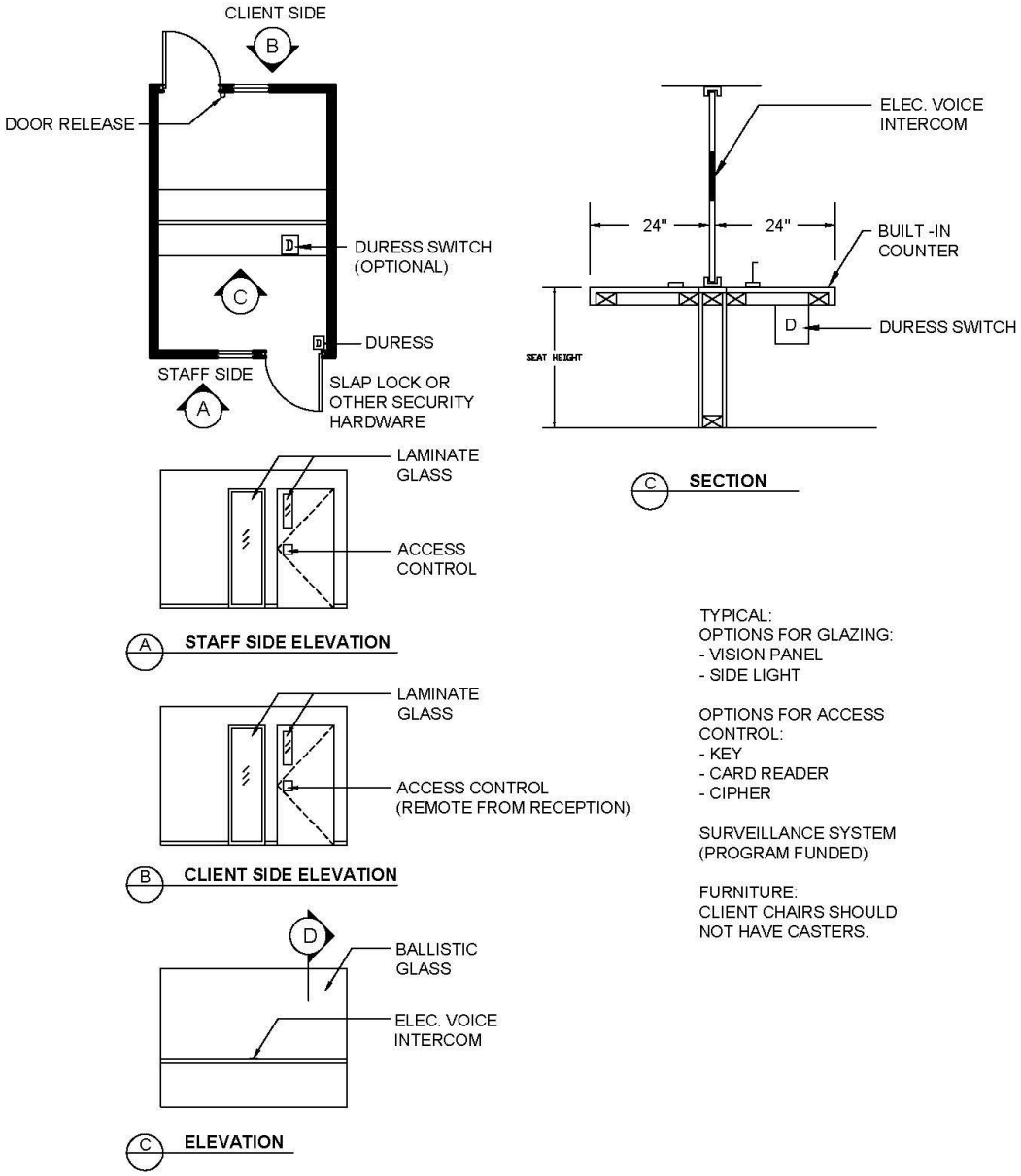
OPTIONS FOR ACCESS CONTROL:
- KEY
- CARD READER
- CIPHER

SURVEILLANCE SYSTEM
(PROGRAM FUNDED)

FURNITURE:
CLIENT CHAIRS SHOULD
NOT HAVE CASTERS.

Government of Alberta ■
Infrastructure

MEDIUM SECURE INTERVIEW ROOM
SCALE: N.T.S



Government of Alberta
Infrastructure

HIGH SECURE INTERVIEW ROOM
SCALE: N.T.S