Guide to the Application of Physical Security Zones

GCPSG-015 (2024)

Prepared By:
Royal Canadian Mounted Police
Lead Security Agency for Physical Security
Departmental Security
NHQ 73 Leikin Drive Ottawa Ontario, K1A 0R2

Publication Issued: 2023-08-31
Updated: 2024-06-01

Royal Canadian Mounted Police | Gendarmerie royale du Canada

Canada

Foreword

The Guide to the Application of Physical Security Zones is an UNCLASSIFIED publication, issued under the authority of the Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

This is a Government of Canada publication to serve as a guide for the application of physical security zoning for departments, agencies, and employees of the Government of Canada.

Suggestions for amendments and other information can be sent to the RCMP Lead Security Agency RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Effective Date

The effective date of GCPSG-015 (2023) Guide to the Application of Physical Security Zones was 2023-08-31; updated 2024-06-01.

Record of Amendments

Amendment No.	Date	Entered By	Summary of Amendment
1	2024-09-23	T. Murphy	Add 1.3 EDI, Appendix A and Appendix C

Note: Authority for modifications or variances is Royal Canadian Mounted Police Lead Security Agency for Physical Security (RCMP LSA).

Contents

1. Introduction

The RCMP, as the Lead Security Agency (LSA) for physical security for the Government of Canada (GC), is responsible for providing advice and guidance on all matters relating to physical security.

1.1. Purpose

The physical environments of facilities can be designed and managed to reduce the risk of unwanted events/incidents. Zoning is one such component which if implemented effectively can help reduce the risk of security events and help safeguard the confidentiality, availability and integrity of GC information, assets and people. While physical security zones are important security features, they should not be considered as a means to completely eliminate security risk, nor should it be considered as the only method to address risk. Instead, physical security zones should be viewed as an integral component of a GC department or agencies overall security risk management strategy.

1.2. Applicability

This guide is specific to the GC controlled facilities and should not be used to determine zoning for Remote/Telework location. This guide does not detail the security requirements for a remote/telework environment, for those guidelines refer to GCPSG-008 - Physical Security Considerations for Remote and Telework Environments.

All GC departments and agencies are responsible for safeguarding employees, assets, and service delivery within their area of responsibility. As it pertains to physical security zones, the Directive on Security Management (DSM), Appendix C, section C.2.3.2 "Implement measures to ensure that access to information in physical form, government facilities and other assets, including sensitive equipment, telecommunications cabling and information systems, is restricted to authorized individuals who have been security-screened at the appropriate level and who have a need for access". Similarly, GCPSG-010 - Operational Physical Security Guide (Section 6.2 - Hierarchy of Zones) states that "departments should ensure that access to and safeguards for protected and classified assets are based on a clearly discernable hierarchy of zones".

The guidance provided in this document should be considered the baseline requirements for physical security zoning. GC departments and agencies are responsible for validating these requirements against their own security needs. This guide should be used in conjunction with a Threat and Risk Assessment (TRA) in order to develop an effective physical security zoning strategy for each facility, and should be used to support decision making for zone selection. GC departments and agencies are responsible for the implementation of this guideline and may contact the RCMP LSA to discuss the content, review additional physical security guides in support of the materials discussed in this guide, and/or for assistance with safeguard suggestions above baseline threats based on the results of a TRA. Other RCMP LSA guides may be required to assess specific security situations and are available at Lead Security Agency for Physical Security - Royal Canadian Mounted Police (rcmp-grc.gc.ca).

1.3. Equity, Diversity, and Inclusion in Physical Security Systems

All employees of the Government of Canada (GC) have a responsibility to safeguard persons, information and assets of the GC. It is important that security policies and practices do not serve as barriers to inclusivity, but instead support and respect all GC personnel while ensuring appropriate security measures are maintained for the protection of GC personnel, assets, and information.

Initiatives to promote equality and inclusion among the diverse communities and heritages within the GC, should be respected in the development and maintenance of physical security systems. Departments and agencies should follow all GC legislation, policy and directives on Equity, Diversity, and Inclusion (EDI) in the promotion of a fair and equitable work environment for all persons while ensuring they meet their mandated security responsibilities.

Departments and agencies should conduct a risk management exercise to ensure, that while the dignity of all is respected, the protection of GC information, assets, and personnel is maintained. All questions on EDI policies and directives should first be addressed to your responsible departmental authority.

1.4. Information Technology Considerations

With the constantly evolving threat landscape, and the convergence of physical and information technology (IT) security, the requirement to assess the risk of any application and/or software connected to a network to operate and support equipment in Government of Canada controlled buildings is critical. Some examples of these control systems could be for items such as, but not limited to, security lighting, perimeter gates, doors, HVAC, etc.

Before implementing any applications and/or software that will control and/or automate certain building functions, your departmental security requires the completion of a Security Assessment and Authorization (SA&A). This will ensure that the integrity and availability of the components the applications and/or software controls are maintained and that any risks highlighted will be mitigated. Starting the SA&A process early is highly recommended to ensure project delivery schedules are not affected. For more information on the SA&A process, please consult your departmental Security.

2. Contact Information

For more information, please contact:

Royal Canadian Mounted Police
Lead Security Agency for Physical Security
73 Leikin Drive, Mailstop #165
Ottawa, ON
K1A 0R2
Email: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronyms

Acronym/Abbreviation	Meaning
CSO	Chief Security Officer
GC	Government of Canada
HSZ	High Security Zone
LSA	Lead Security Agency
OZ	Operations Zone
PSPC	Public Services and Procurement Canada
PZ	Public Zone
RAA	Restricted Access Area
RZ	Reception Zone
SBDA	Scientific Based Departments and Agencies
SOPs	Standard Operating Procedures
SPS	Special Purpose Spaces
SRCE	Scientific Research Collaborative Environment
SZ	Security Zone
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment
USB	Universal Serial Bus

4. Glossary

Term	Definition
Asset	Tangible or intangible things of the Government of Canada. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation.
Baseline Security Requirements	Mandatory security provisions of the GC Policy on Government Security and its associated policy instruments.
Classified Assets	Assets, whose compromise would reasonably be expected to cause injury to the national interest.
Classified Information	Information, whose compromise would reasonably be expected to cause injury to the national interest.
Continuous Monitoring	Uninterrupted observation on a continuous (24/7) basis to confirm there has not been a breach of security. Examples include electronic intrusion detection systems, CCTV, or someone guarding a particular point on a constant basis.
Control of Access	A process to restrict access to assets within a facility or restricted access areas. This can be accomplished through various means including the screening of visitors and material at entry points by personnel, guards or automated means and, where required, monitoring the movement within the facility or restricted access areas

	through access control systems.
Defence-in-Depth	This is the principle where security zones are implemented in a progressively restrictive manner, proceeding from the least restrictive zone to the most restrictive.
Escort or Escorting	An appropriately security cleared person who is responsible for the continuous supervision of non-security cleared people in areas where a security clearance or status would normally be required to work.
Facility	Something that is built, installed, or established to serve a particular purpose. A facility may include a specific building (whole or part) or the site or land it is located on.
Insider Risk	A person with knowledge of, or access to, an organization's infrastructure (both physical or computer networks) who maliciously, or by chance, misuses their trusted access to harm the organization's employees, customers, assets, reputation or interests.
Integrity	The accuracy and completeness of assets, and the authenticity of transactions.
Need-to-Access	The principle that there is a need for the person to access the area or zone in order to perform their duties. This is not to be confused with the need-to-know the content of the information contained or processed within that area or zone.
Need-to-Know	The principle that there is a need for someone to access and know information in order to perform their duties.
Periodic Monitoring	Monitoring on a periodic but regular basis. For the purposes of physical security, the frequency and diligence of periodic monitoring is determined by a department organization based on a TRA.
Protected Asset	Assets, whose compromise would reasonably be expected to cause injury to other than the national interest.
Protected Information	Information, whose compromise would reasonably be expected to cause injury to other than the national interest.
Restricted Access Area (RAA)	A work area (site or building) within a department where access is limited to authorized individuals. This includes Operations Zone, Security Zone, and High Security Zones as defined in Ref: G1-026 Guide to the Application of Physical Security Zones.
Tenant	An organization occupying federal real property that is under the administration of another GC department, agency or crown corporation.

5. Design Implementation

Physical security zones, when appropriately integrated, should enhance the overall security environment of a facility. Physical security zoning should promote a sense of ownership or territorial reinforcement, provide opportunities for natural surveillance, and establish a clearly defined sequence of boundaries through which an appropriately screened visitor or employee may pass through.

Before a person moves from one physical security zone to another, they should perceive the zoning boundary (implied or actual) and understand the rules / limitations associated with crossing it. Departmental functional space requirements should also be taken into consideration when establishing zoning boundaries.

Physical security zoning should not be implemented by simply adhering to the prescribed technical requirements for zones (refer to Section 5.3 for baseline zone requirements), nor by integrating zones into the plan based solely on functional space requirements. If physical security measures that demarcate zones are excessive, inappropriate, or have not considered the functional space requirements, these measures will eventually be bypassed and could become ineffective. Incentives for unauthorized personnel to cross zoning boundaries (i.e., washrooms, cafeteria, etc.) should be avoided or removed.

5.1. Need-To-Know / Need-to-Access

A fundamental requirement of the Policy on Government Security (PGS) is to limit access to sensitive information and areas. The PGS further restricts access to those who have the need-to-know, or a need-to-access in order to perform their duties. While security screening levels permit access to certain information or areas, the application of the need-to-know and need-to-access principles restrict that access to those with a need to see specific information or to access specific areas. Personnel are not entitled to access merely because it is convenient nor because it is commensurate with their security clearance level, status, rank, or office. GC departments and agencies are responsible for reviewing access privileges and should revoke access when it is no longer required (i.e., if an employee no longer requires access to an area, accepts a position with another department or agency or when they retire).

An effective way of implementing and maintaining the need-to-know or need-to-access principle consists of segregating and controlling access to sensitive GC information and assets through the effective use of physical security zones. Given that individuals within an GC department or agency can pose a threat to the availability, confidentiality or integrity of GC information or assets (often referred to as insider risk); limiting access only to those with the appropriate need-to-know / need-to-access can reduce insider risk and help safeguard GC information and assets.

5.2. Zone Selection

To determine the appropriate zone(s) for the processing, storage, or destruction of sensitive assets, it is first necessary to establish the minimum baseline security requirements. RCMP LSA guide GCPSG-010 - Operational Physical Security Guide designates physical security zones based upon the security categorization and the corresponding injury that would result from the unauthorized disclosure, destruction, removal, modification, interruption or misuse of the information or assets contained within. These categorizations and injury levels can also be found in the DSM Appendix J.

ZONE SELECTION			
Categorization *(see Note 1)*	**Injury level** *(see Notes 1, 2)*	**Baseline Zone** *(see Note 3)*	**Enhanced Threat**
Protected A	Limited or moderate injury	Operations Zone	Operations Zone
Protected B	Serious Injury	Operations Zone	A TRA should be completed to determine the safeguards
Protected C	Extremely Grave Injury	Security Zone	
Confidential	Limited or Moderate Injury	Operations Zone	
Secret	Serious Injury	Security Zone	
Top Secret	Exceptionally Grave Injury	High Security Zone	

NOTES:

1. In accordance with DSM Appendix J
2. Consult with the RCMP LSA for storage requirements of assets other than information having high integrity and availability requirements.
3. Identification of assets requires that injury assessment levels be assigned for the integrity, availability and value of the asset. It may be necessary to increase the zone requirement if the assigned injury level is greater than the level established for confidentiality.

5.3. Baseline Zone Requirements

The following charts summarize the five fundamental zones and their baseline requirements. In addition to these zones, it has become necessary to expand zoning options to better reflect the current needs of the GC. These are called "Special Purpose Spaces" and are further referred to in appendices of this guide. Appendix A discusses the Scientific Research Collaborative Environment (SRCE) and Appendix B discusses zoning considerations for Detention Spaces.

5.3.1. Public Zone (PZ)

PUBLIC ZONE	
Definition	An area where the public has unimpeded access and generally surrounds or forms part of a government facility.
Examples	The grounds surrounding a building such as sidewalks or public corridors and elevator lobbies in multiple occupancy buildings.
Perimeter	There are no perimeter requirements for a PZ however it may include signage referencing the RZ entrance or location.
Monitoring	N/A

5.3.2. Reception Zone (RZ)

RECEPTION ZONE	
Definition	Where the transition from a PZ to an RAA is demarcated and controlled.
Examples	Typically located at the entry to the facility where initial contact between visitors and the department or agency occurs. This can include such spaces as places where services are provided and information is exchanged. Access by visitors may be limited to specific times of the day or for specific reasons.
Perimeter	May be delineated by signage, perimeter may vary depending on the time of day.
Monitoring	The extent of monitoring will vary depending on the time of day or as indicated by the TRA.
Notes: Consider after closing hours or lock up a RZ could become an OZ as it could be part of the GC facility that requires protection (ie. The need to control access when not occupied)	

5.3.3. Operations Zone (OZ)

OPERATIONS ZONE	
Definition	The OZ is an area where access is limited to appropriately security screened personnel who work there and to escorted visitors.
Examples	Typical open office areas.
Perimeter	Must be indicated by a recognizable perimeter or a secure perimeter as indicated by the TRA.
Monitoring	*** Monitored periodically.**
*** Monitored periodically** - to confirm on a regular basis that there has not been a breach of security. The frequency and diligence of monitoring is based on the recommendations of a Threat and Risk Assessment. Examples include a guard patrol, electronic intrusion detection logs, or employees working at the location.	

5.3.4. Security Zone (SZ)

SECURITY ZONE	
Definition	An area to which access is limited to authorized, appropriately security screened personnel and to authorized escorted visitors.
Examples	An area where information/assets categorized at the Secret level are processed or stored.
Perimeter	Must be indicated by a recognizable perimeter or a secure perimeter as indicated by the TRA.
Monitoring	**Monitored continuously, i.e., 24 hours a day and 7 days a week.
**** Monitored continuously** - to confirm on a continuous basis there has not been a breach of security. Examples include electronic intrusion detection systems or someone guarding a particular point for a continuous period	

5.3.5. High Security Zone (HSZ)

HIGH SECURITY ZONE	
Definition	An area to which access is limited to authorized, appropriately security screened personnel and to authorized escorted visitors.
Examples	An area where information/assets categorized as Top Secret or above are processed or stored.
Perimeter	Must be indicated by a perimeter built to the specifications recommended in the TRA.
Monitoring	Monitored continuously **, i.e., 24 hours a day and 7 days a week and where details of access are recorded and audited.

The last three zones, OZ, SZ and HSZ are referred to as restricted-access areas (RAA) and instituting a hierarchy of zones allows departments and agencies to:

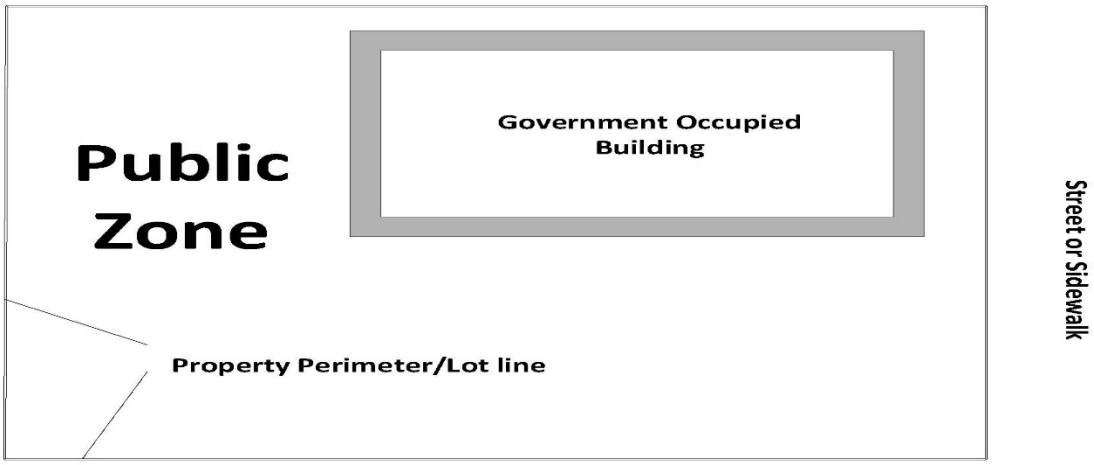
- Store assets of different threat levels in the same facility,
- Institute varied levels of controls of access to protect various levels in assets,
- Reduce cost by processing and destroying various levels of information and assets within the same facility, and
- With appropriate planning, change zones from one period of time to another (ie. an OZ during working hours might become a SZ during silent hours or an RZ might become an OZ during a similar period).

The appropriate number of zones within a facility is dependent on the number of tenants (single or multi-tenant) and the building owner / custodian (federal, provincial or municipal government or private sector). In a multi-tenant government building, the building security committee should determine the hierarchy of zones for the common areas. The tenant is responsible for determining appropriate zones within its space.

It is important to note that the forgoing definitions do not preclude the establishment of a temporary restricted zone either inside or outside a controlled area. These temporary areas could be established to house or process material categorized above the level normally stored in the zone provided the necessary physical security safeguards are in place, the increased risk is documented through a formal TRA, and the risk is accepted by the CSO (or their delegate). For example, a temporary SZ could be established around a seized vessel or truck under continuous guard. Another example could be a desk in an open office area that normally functions as an OZ but could serve as a SZ provided the person handling the material is in full control of it at all times and prevents unauthorized disclosure.

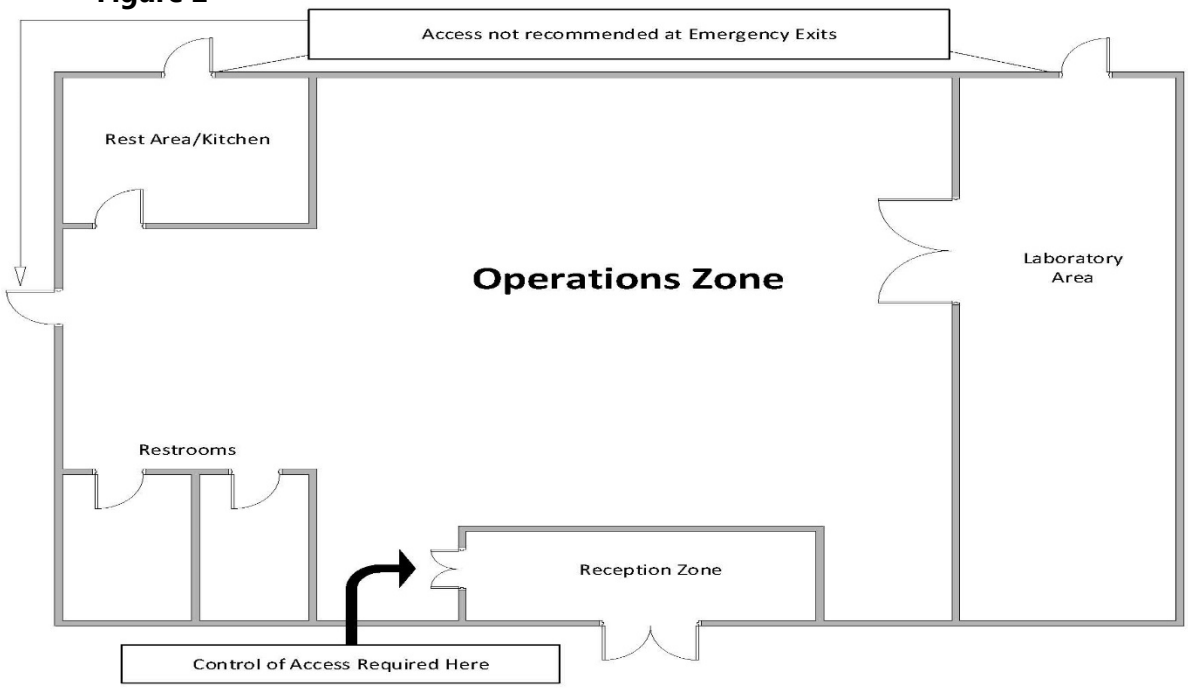
In considering physical security zone design and layout, the first two zones (PZ, RZ) should set the stage for access to the RAAs. The baseline security requirement is that access be controlled in OZ and higher and since no two facilities are identical, the locations where OZs begin will also be different from one facility to another. The following examples (Figures 1 through 5) illustrate these considerations through some generic facility types.

Figure 1



Alt Text Figure 1 depicts a site plan of a typical facility type.

Figure 2



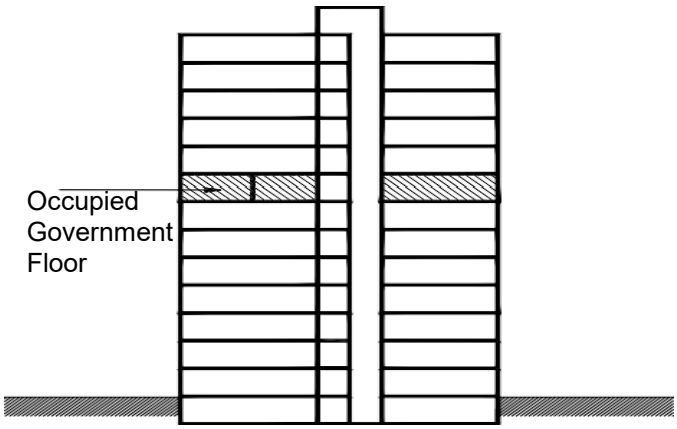
Alt Text Figure 2 depicts a floor plan of a typical facility type.

Figures 1 and 2 depict examples of a single-purpose government facility on government owned land. The PZ consists of the grounds around the building and although departments and agencies may wish to monitor this area, there is no requirement to control access. A RZ is located at the front entry.

Within this zone, there is a means for the public to make initial contact and exchange information. This may happen at a reception desk, where there will be personnel present to monitor entrance to the space. Entry beyond the RZ is restricted to those who have a need-to-

access. There should be a recognizable perimeter such as a doorway or an arrangement of furniture which clearly demarcates the entrance to the RAA and access is controlled from this point on. Access is also to be controlled at every point at which the OZ allows access to a SZ.

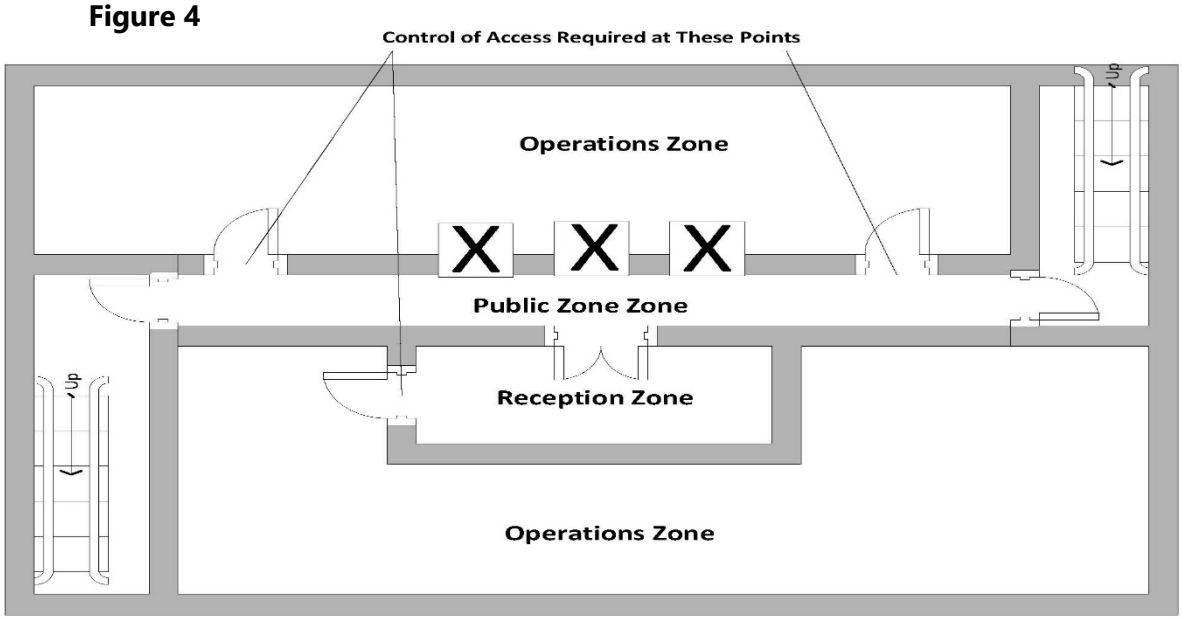
Figure 3



Building Section

Alt Text Figure 3 depicts a multistory building section of a GC tenant occupied space.

Figure 4



Alt Text Figure 4 depicts a multistory building floor plan of a GC tenant occupied space.

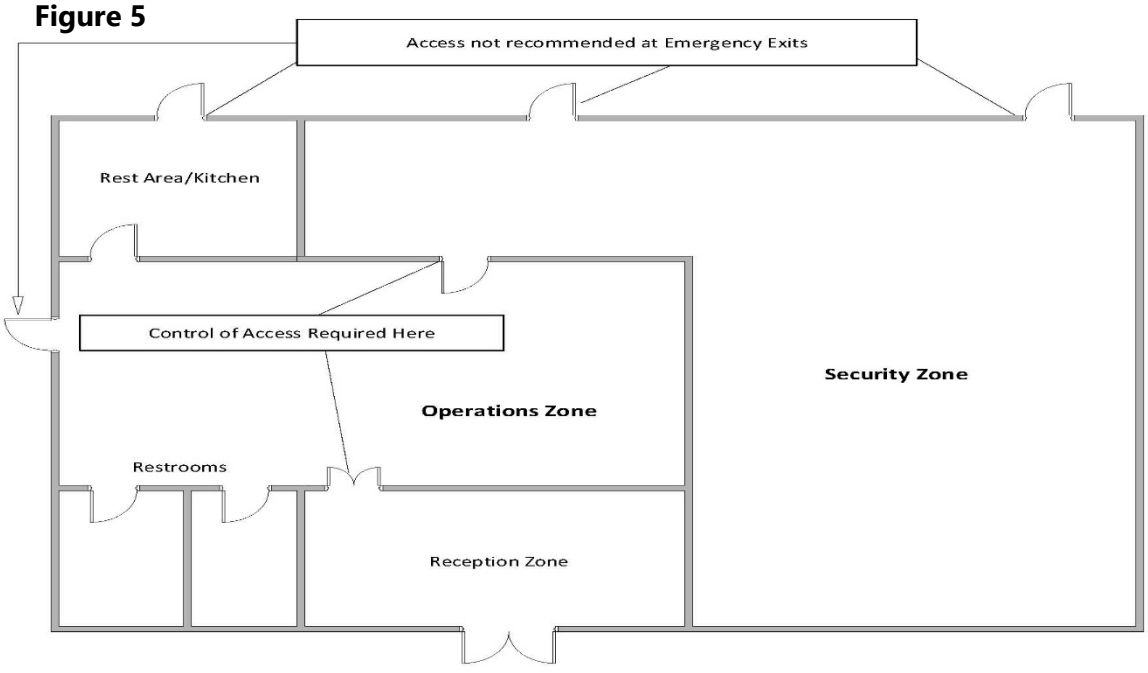
Figures 3 and 4 depict an example of a multi-story building in which the government is a tenant on multiple floors. The PZ includes the main floor lobby as well as the elevator and corridors on each floor. There is an RZ located adjacent to the PZ on one side of the floor. The remaining office areas are OZ.

Access to the OZ from the RZ is to be controlled, in this example, it is possible to enter the OZ from either the RZ or the PZ (the corridor). Access to the OZs should gained through a RZ wherever possible.

Physical security zones should be implemented in a progressively restrictive manner, proceeding from the least restrictive (PZ) to the most restrictive (OZ, SZ or HSZ) zone required, so that sequential entry points must be passed through. An entry point is a design feature that channels traffic in such a way that effective control of access is possible at that point. Entry points between zones should be clearly identifiable. The boundary of the zone should not permit access other than at an entry point unless there are functional requirements such as a service counter which handles or processes client requests. It should be clear that entry into an OZ is for limited to authorized personnel and escorted visitors only. Typically, this is done with signage which directs individuals to, and in the RZ. The floor plan below (figure 5) illustrates some of these suggested criteria.

In addition to meeting the baseline requirements, departments and agencies may wish to establish additional measures to further limit access within a facility. The requirement for a SZ or HSZ within a facility will depend upon the categorization of material handled, as well as the specific threats to the department. Different means of controlling access may be appropriate depending on the zone accessed by the entry point. Anything from a staff member or security guard verifying access badges for entry to an OZ up to a sophisticated biometric access control system when entering an HSZ may be used. The selection of the access control measure can be determined based upon a TRA. In addition, there should be a corresponding level of personnel security screening and physical barriers to support the access control measures.

Figure 5

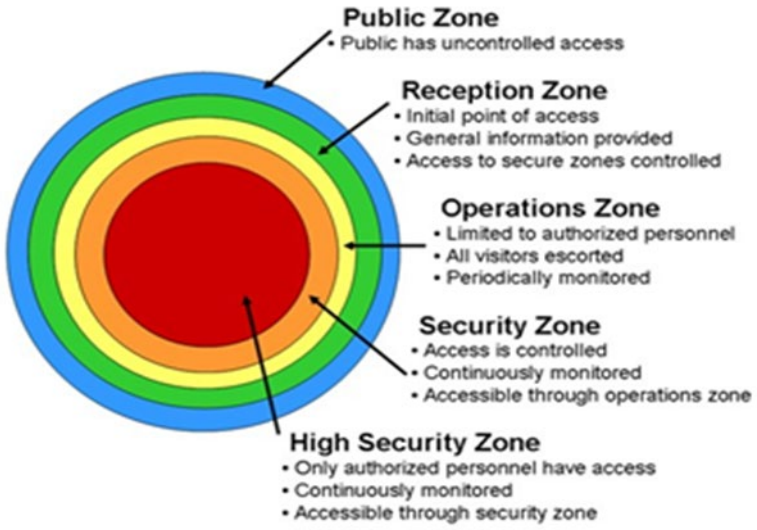


Alt Text figure 5 depicts a floor plan of a building with different physical security zones where access is controlled to each area.

6. Zoning Concerns and Issues

6.1. Defence-in-Depth (Using all Physical Security Zones)

Security zones should not be skipped, by-passed or omitted as it takes all necessary zones to create "defence-in-depth". This is the principle where security zones are implemented in a progressively restrictive manner, proceeding from the least restrictive zone to the most restrictive. There are instances however, where specific departmental business lines or facility functional requirements may make it inefficient to implement all physical security zones and there are also limited situations where it may be difficult or impractical to do so. In these limited cases, a single zone may be by-passed or left out of the zoning model provided that the security measures of that zone are compensated for in the subsequent zone. Any zoning deviations should be carefully and thoroughly documented in a TRA, and the risks associated with this deviation accepted by the security authority, either the CSO or their delegate.



6.2. Information and Asset Storage in Physical Security Zones

GCPSG-007 - Transport, Transmittal and Storage of Classified and Protected Material outlines the minimum storage requirements of sensitive material by physical security zone and security categorization. In limited circumstances, and as a part of a departmental risk management solution, storing small amounts of higher categorized material within lower physical security zones may be considered. Before information can be stored in this capacity, a TRA should be done to analyze any residual risk and the implementation of additional security control measures should be considered to ensure the protection of the material. The CSO or delegate should then sign off as accepting the residual risk. Departments and agencies can contact the RCMP LSA with specific questions pertaining to these deviations and solicit advice and guidance on next steps.

6.3. Changing Physical Security Zone Designations

It is possible that the physical security zone designation could change over the course of a business day (i.e. The RZ zone is locked up and not accessed by personnel or clients during

hours the office is closed or during limited access hours ie. lunch time). Re-designating zones during these periods will depend on the business conducted within them during regular hours, the type of security measures used outside of regular hours and when the area is closed, and who has access. Careful consideration should be given to any additional physical security measures that may be required in this circumstance. Implementing such a solution may require the completion of a TRA and be approved by the CSO or delegate after careful consideration and acceptance of any residual risk involved.

7. Special Purpose Spaces

Special Purpose Spaces (SPS) are additional non-standard areas that may be required by a department or agency to accommodate specific functional or business line activities. These spaces should only be implemented as needed based on specific business or operationally essential requirements of the department or agency. The RCMP LSA recommends an SPS only be used in limited circumstances such as:

- When supporting business requirements for non-GC groups;
- To temporarily house persons waiting questioning as part of an investigation, or transfer to another GC facility or domestic or foreign government facility; and
- Only for non-sensitive or unclassified work unless specifically designated and approved by the CSO or delegate.

It should be noted that not all GC departments and agencies will need to have SPS in their facilities and that SPS should not be used as a way of circumventing the GC security clearance requirements.

7.1. Scientific Research Collaboration Environment (SRCE)

A Scientific Research Collaboration Environment (SRCE) is an optional SPS that enables members of the scientific community from outside the GC (ie. foreign nationals, universities researchers or scientists, and private industry) to work collaboratively with the GC to conduct scientific research and testing in a controlled secure environment separate from other GC information or assets.

An SRCE may only be implemented by GC departments and agencies specifically designated as a Science-Based Department or Agencies (SBDA). SRCEs should not be confused with, or used in place of, GC co-working spaces and should never be used as a means to by-pass the security clearance process. SBDAs requiring the use of an SRCE should always conduct a complete and thorough credential verification of any non-GC security cleared researcher designated to work in these spaces. For more detailed information refer to Appendix A.

7.2. Detention Space

A Detention space is an SPS that is used to detain persons as a part of an investigatory or law enforcement process. GC departments and agencies which have law enforcement activities as a part of their responsibilities (ie. RCMP, Canada Border Services Agency (CBSA), Department of Fisheries and Oceans (DFO), etc.) may have a need for this type of SPS. For more detailed information refer to Appendix B.

7.3. Computer Server Rooms

Contrary to SRCEs and detention spaces, virtually all GC department and agencies have a need for one or more computer server rooms to house GC Information Technology (IT) that supports all GC processes. The design and management of these IT systems is guided by the Communications Security Establishment of Canada. For more information on the location and physical protection of computer server rooms, refer to Appendix C.

8. References and Related Documents

- Policy on Government Security
- Directive on Security Management
- RCMP Security Equipment Guide G1-001.
- GCPSG-007 - Transport, Transmittal and Storage of Classified and Protected Material
- GCPSG-008 - Physical Security Considerations for Remote and Telework Environments
- GCPSG-010 - Operational Physical Security Guide
- GCPSG-011 – Guide to CCTV-CCVE Systems
- GCPSG-013 – Fundamentals of Glazing in Physical Security
- G13-01 Secure Storage Rooms (SSR)
- G13-02 Secure Demising Wall (SDW
- Communications Security Establishment of Canada
- Call to Action on Anti-Racism, Equity, and Inclusion in the Federal Public Service
- Directive on the Duty to Accommodate
- Guide for Two-Spirit, Transgender, Non-Binary, and Gender-Diverse Employees

Appendix A – Scientific Research Collaboration Environment

1. Purpose

The intent of this Appendix is to provide physical security guidance, in addition to the information contained in this guide, related to the design and development of a Scientific Research Collaboration Environment (SRCE). For the purpose of this guideline, scientific research is defined as a systematic investigation or study of scientific theories and/or hypothesis. It is quantitative in nature and is strongly based on the collection of data. Scientific research is often used in the fields of Biology, Physics and Chemistry.

2. Definition: Scientific Research Collaboration Environment

A Scientific Research Collaboration Environment (SRCE) is an environment that is designed to enable members of the scientific community who come from outside the Government of Canada (GC) such as foreign nationals, university researchers, and private industry to work collaboratively with GC departments and agencies to conduct scientific research and testing in a controlled and secure environment.

3. Applicability

The application, use, and operation of an SRCE and the guidance contained in this appendix is only applicable to departments and agencies within the GC specifically identified as Science-Based Departments and Agencies (SBDA) and should not be confused with GC Co-working sites/facilities. SBDAs engage with scientific partners from non-GC organizations such as academia and industry, including foreign nationals, on collaborative scientific based research in a laboratory setting. Examples (not exhaustive) of SBDAs include Agriculture and Agri-Food Canada, Health Canada, and Public Health Agency of Canada. It is important to note that the risk acceptance of SRCE use remains the purview of the department or agency CSO or their delegate operating the SRCE.

The use of a SRCE is applicable where:

- It is not possible or practical to obtain applicable security clearances for collaborating partners due to:
    - Researchers having foreign nationalities; and
    - Researchers or collaborators from Academia or industry and where the nature of these collaborations is of extremely short duration.

If the nature of the collaborative research is considered sensitive, protected or classified based on GC guidance, refer to zone selection for further information on what zone designs might be required to ensure the protection of the information being researched or collaborated.

It should be noted that collaborators should only be permitted access to the information specific to their work and not to the totality of the information.

The use of an SRCE is NOT applicable:

- Where research is being collaborated/conducted between GC departments and agencies (even those identified as SBDAs) where all users hold a GC security clearance or status; and
- As a means to circumvent or by-pass the security clearance process.

SBDAs responsible for the operations of an SRCE should still conduct a thorough vetting of all collaborative researchers to verify their academic or industry credentials and complete all required site access screening procedures.

The guidance outlined in this appendix is limited to general principles (physical security, "Need-to-Know", "Need-to-Access", personnel security etc.). Comprehensive security requirements for the SRCE should be designed based on the overall security requirements of the project being undertaken within the environment. The acceptance of risk for the use of an SRCE remains with the CSO or their delegate of the department or agency hosting the space.

4. Introduction

As no two facilities are identical, the locations of laboratories or research areas within a facility will differ from one facility to another. The physical security safeguards for the SRCE must conform to GC physical security zoning requirements for the category of the material being researched, and be integrated with the overall security of the facility. As per this guide the GC physical security zoning model includes 5 zones including:

- Public Zone (PZ);
- Reception Zone (RZ);
- Operation Zone (OZ);
- Security Zone (SZ); and
- High Security Zone (HSZ).

Although the preferred option is to have an SRCE completely separate from all other GC zones, with proper planning and additional security controls, an SCRE may be integrated into any of the existing zones. A TRA should be completed which identifies all risks and additional physical security control measures required prior to operating an SRCE especially in a SZ or HSZ.

SCIENTIFIC RESEARCH COLLABORATIVE ENVIRONMENT (SRCE)	
Definition	An area that is designed to enable members of the scientific community outside the GC to work collaboratively with GC Departments on research projects in a controlled / secure environment.
Examples	An area where persons from outside the GC such as international governments, universities, private sector, can conduct scientific research and testing.
Zoning	The zoning for the collaborative space must follow the fundamental requirements of progressively restrictive access and be integrated with the overall security of the facility.
Perimeter	Must be indicated by a perimeter built to the specifications recommended in the TRA.
Monitoring	Monitored continuously **, i.e., 24 hours a day and 7 days a week and where details of access are recorded and audited.

5. Design Considerations:

- It is up to the SBDA to determine the categorization level of the SRCE based on their interpretation of the sensitivity, actual GC categorization or hazards/dangers of the research. In the case of multiple categorization levels, the zoning requirements of the highest categorization level will be required;
- Ideally, the SRCE should be designed as a separate distinct area with restricted or no access to other laboratory areas within the facility. It should follow the fundamental requirements of defence-in-depth, progressively restrictive physical security zoning and access requirement, the principles of Need-to-Know / Need-to-Access and be integrated with the overall security of the facility;
- The SRCE should be self-contained with workstations, scientific equipment, eating areas, washroom facilities, and IT controls that do not allow access to GC computer networks. Allowances for unauthorized personnel to cross zoning boundaries (i.e., washrooms, cafeteria, etc.) should be eliminated unless building design constraints prohibit this - in which case a TRA with appropriate risk acceptance authority is needed;
- The SRCE must meet the physical security control requirements necessary for the categorization of the research being conducted (ie. OZ, SZ, etc.). If the zone required cannot be newly constructed, retrofits to existing spaces should be made. It is recommended that a TRA be completed and all risks are identified;
- The SRCE should be integrated with the overall laboratory functional structure in which it will exist, including access to common spaces and shared laboratory equipment;
- Proper planning of the SRCE by the department should take place prior to the commencement of any scientific research project and consider the protection of GC information and assets not a part of the research, and the degree of injury related to high value information, assets, and proprietary rights;
- Standard Operating Procedures (SOPs) should be developed by the department hosting the SRCE which are designed to provide employees with clear step by step instructions and procedures while working in the SRCE space. SOPs should include:
    - Sanitization of the work space;
    - Employee escorts;

  - IT controls (no GC Intranet/network connection);
  - Monitoring requirements (periodic or continuous monitoring); and
  - Access control safeguards.

  Note: A checklist used prior to entering and exiting the SRCE, may also provide enhanced security measures;
- As research evolves, changes to the sensitivity of information and / or assets may necessitate that the security provisions of the SRCE be adapted or modified to mitigate the changing security risks; and
- Physical security zones, when appropriately integrated, should contribute to the overall security environment of a facility.

Note(s): Physical security zoning that simply adheres to the prescribed technical requirements or by integrating zones based solely on functional space requirements may not be sufficient or effective. Security measures that are excessive or do not address functional requirements will be circumvented and become ineffective. Refer to section 5.3 in this guide for more info.

It is also important to note that as research within a GC facility evolves, changes to the sensitivity of information and assets may occur. These changes in sensitivity might require that security provisions of the SRCE be adapted or modified to mitigate the changing security risks. These considerations should be factored into the initial TRA for the design of the space, and within the parameters of the scientific research project being conducted at the facility. These considerations should be carefully risk managed on a continuous basis by the CSO or their delegate.

6. Physical Security Zone Selection

To determine the appropriate physical security zone(s) for the SRCE, it is first necessary to determine the categorization of the work being conducted. Then it is necessary to establish the minimum baseline security requirements to safeguard that work. The RCMP guide GCPSG-010 - Operational Physical Security Guide designates physical security zones based on the categorization of the information and assets and the corresponding injury that would result from its unauthorized disclosure, destruction, removal, modification, interruption or misuse. These zones are defined in the chart below and in section 5.2 based on their injury levels along with specific examples to highlight zone demarcation for an SRCE.

ZONE SELECTION			
Categorization *(see Note 1)*	**Injury level** *(see Notes 1, 2)*	**Baseline Zone** *(see Note 3)*	**Enhanced Threat**
Protected A	Limited or moderate injury	Operations Zone	Operations Zone
Protected B	Serious Injury	Operations Zone	A TRA should be completed to determine the safeguards
Protected C	Extremely Grave Injury	Security Zone	
Confidential	Limited or Moderate Injury	Operations Zone	
Secret	Serious Injury	Security Zone	
Top Secret	Exceptionally Grave Injury	High Security Zone	

NOTES:

1. In accordance with DSM Appendix J
2. Consult with the RCMP LSA for storage requirements of assets other than information having high integrity and availability requirements.
3. Identification of assets requires that injury assessment levels be assigned for the integrity, availability and value of the asset. It may be necessary to increase the zone requirement if the assigned injury level is greater than the level established for confidentiality.

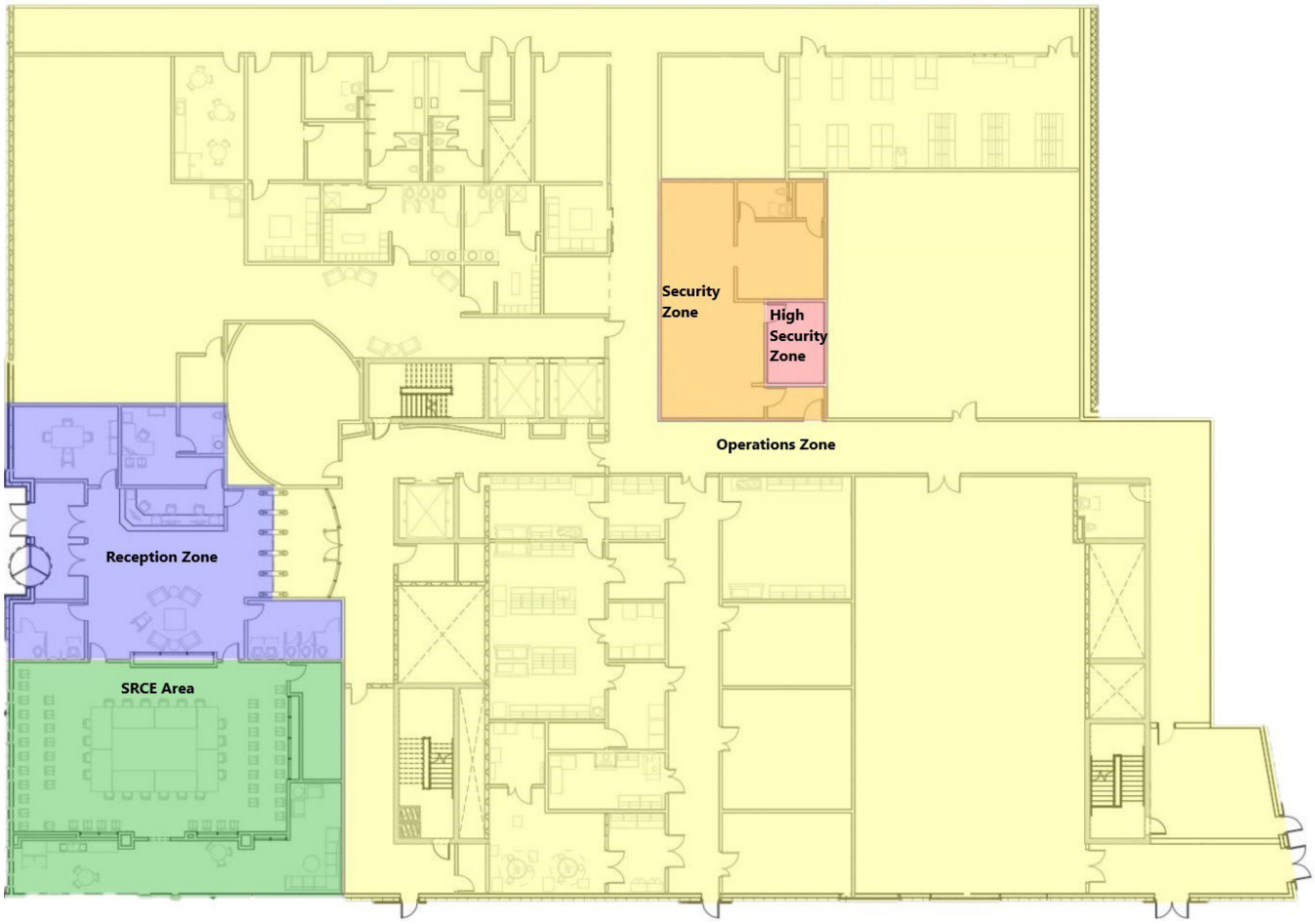
If a defined laboratory space or SRCE is not available, there may be a need to establish a temporary RAA either inside or outside a controlled area. For example, a temporary SZ could be established around a scientific research project. The requirement to limit unauthorized access to this area would need to be evaluated however, signage and demarcation of the work space should be considered a minimum. Guards, partitions, CCTV or other control measures should be used. There also may be a need to have continuous monitoring, through contract security guards or other monitoring tools.

7. Design Examples

7.1. Completely Separated Research Environment

A newly constructed SRCE (Figure 1), whether a stand-alone facility or built within an existing facility that does not provide access to any other operational zones in a GC facility is the ideal situation for an SRCE. The environment is self-contained and can only be accessed via a RZ. Proper access control mechanisms are in place and access to the area is routinely monitored.

Figure 1 Completely Separated



Alt Text Figure 1 facility layout depicting physical security zoning whereby the SRCE has no access to any other operational zones in a GC facility. The operations zone is self-contained and can only be accessed via the Reception Zone.

7.2. Partially Integrated Research Environment

A retrofit to existing GC facility where access to the SRCE is accessed via an OZ (Figure 2) may be required although is not the ideal solution. If this is the only means of creating an SRCE, proper access control mechanisms should be in place to prevent unauthorized access to other physical security zones. In this area, access is routinely monitored. Control of access is required at all entry points into all zones. Installation of signage can make it clear to any visitors that entry into an OZ is for authorized employees only. Signage can also direct the individual to the location of the RZ. Ingress into the space should be confined to primary entry points; all emergency exits should be egress only.

Figure 2 Partially Integrated

Alt Text Figure 2 facility layout depicting physical security zoning whereby access to the SRCE is accessed via an Operations Zone. All entry points to the zones have controlled access points.

7.3. Fully Integrated Research Environment

If the SRCE is located fully within a zone of a GC facility especially a SZ or HSZ (Figure 3), unauthorized access is much more difficult to manage. This type of set up should be used as a last resort and only if no other options exist. SBDAs should create detailed SOPs which should include provisions for constant monitoring and escorting to and from the SRCE and any other security control measures deemed appropriate through the TRA process. In this case, ingress and egress for the space should be restricted to single point with all other exits being used for emergency egress only.

Figure 3 Fully Integrated

Alt Text Figure 3 facility layout depicting physical security zoning whereby the SCRE is accessed via a Security Zone

Appendix B – Detention Space

1. Definition:

The intent of this Appendix is to provide physical security guidance, in addition to the information contained in this guide, related to the design and development of a Detention Space. The detention space is an SPS defined as a grouping of controlled / monitored physical security zones intended to restrict access and egress to temporarily house and safeguard persons or detainees. The establishment of this type of space will aid in the prevention of the detained person from escaping custody, harming themselves or others, maintaining the integrity of an investigation, or preventing witness tampering.

2. Applicability:

A detention space is not a new physical security zone added to the hierarchy of security zones. This zone is only to be used when there is operational requirement to detain individuals as a part of functional responsibilities and is not a requirement for all GC departments and agencies. Departments and agencies who might make use of these spaces include; RCMP, Canada Border Services Agency (CBSA), Department of Fisheries and Oceans (DFO), Correctional Services of Canada (CSC), etc.

This guidance is not meant to supersede any formal legislation in the creation of a detention zone it is simply guidance on where a detention zone might be placed within a facility. Standard Operating Procedures (SOPs) should be developed to govern the use of this type of space, and it is recommended that a TRA be conducted prior to the addition of a detention space to a GC facility.

DETENTION SPACE	
Definition	A space or grouping of spaces that are designed with physical barriers to control and restrict access and egress and contain additional controls to provide monitoring functions as well as reduce the potential for self-harm and violence. The intention of a detention space is to safeguard persons from escaping custody, harming themselves or others or to prevent witness tampering.
Examples	An area where persons are detained until transported to another GC facility.
Perimeter	Must be indicated by a perimeter built to the specifications recommended in the TRA.
Monitoring	Monitored continuously **, i.e., 24 hours a day and 7 days a week and where details of access are recorded and audited.

3. Detention Space Design Considerations

3.1. Transfer Area

This is an area which enables the transition from an RZ to an OZ. This could include a secure bay or patrol corridor/hallway. It is separated by a well-defined physical barrier that has been designed, built, and furnished to departmentally approved site-specific requirements. It restricts access to only authorized personnel, and controls movement that limits potential violence and contraband.

3.2. Support Area

This is an area which is a separated by a well-defined physical barrier that has been designed, built, and furnished to departmentally approved site-specific requirements. It restricts and controls access to only authorized personnel. An example of this area would be a staff area, mechanical rooms or storage rooms.

3.3. Processing Area

This is an area which is separated by a well-defined physical barrier that has been designed, built, and furnished to departmentally approved site-specific requirements. It restricts access to only authorized personnel, and controls movement that limits potential violence and contraband. This area could be comprised of interview rooms.

3.4. Holding Area

This is an area which is a separated by an approved physical barrier that has been designed, built, and furnished to departmentally approved site-specific requirements. It is monitored based upon current legislation and functional need to restrict and control movement to only authorized personnel, and to limit potential self-harm, violence and contraband to persons being held in the area. An example of a holding area would be detainee cells.

Not all of the areas listed above need to be used. This guideline provides the GC department or agency with the minimum recommendations. Actual requirements must be based on specific operational needs.

Appendix C – Physical Protection of Computer Server Rooms

1. Purpose

The intent of this appendix is to provide physical security guidance related to the physical protection of computer servers and server rooms. The guidance noted in this appendix does not supersede the previous information contained in the main guide on physical security zones; the information in this appendix and the main guide are to be used in tandem.

1.1. Server Room Location

Access to server rooms, regardless of the classification level of the data processed or technology housed in the server room, should be limited to appropriately security screened individuals who have an operational need to access the space and/or visitors who are appropriately escorted. Examples of individuals who have an operational need to access the space may include security personnel, Government of Canada (GC) IT technicians, and escorted persons granted temporary access.

The location of a server room is dependent on the highest classification level of data processed or stored on the server's networked system:

- Protected A and Protected B – Operations Zone (OZ);
- Protected C and Classified up to Secret – Security Zone (SZ); and
- Top Secret – High Security Zone (HSZ).

It is important to note that these are the minimum requirements and a TRA may determine that the server room be located in a higher zone than what is indicated.

1.2. Shared Server Rooms

While shared server rooms between GC departments/agencies may be economical, there are additional physical security considerations. When the number of people granted access to the sever room increases, so does the probability of compromise. To limit risk, access to the server room should be limited to only appropriately security screened individuals who have an operational need to access the space and/or visitors who are appropriately escorted. A TRA should be conducted to determine feasibility, as well as determine what safeguards are required to facilitate a shared server room. Participating departments and agencies should coordinate policies and procedures to ensure that access to the room is controlled. For more information consult GCPSG-006 Access Management Guide.

2. Safeguards

GC computer servers must be located in a separate room with access control measures such as a mechanical lock or electronic card reader. Access to this room should be limited to only appropriately security screened individuals who require access for operational needs. The room should be built with walls that extend from the floor slab to the underside of the floor/roof slab

above. Rooms with walls that extend to the underside of a suspended ceiling would not meet the requirements of a server room. Appropriate key management and storage is needed for all physical keys or electronic access cards.

2.1. Safeguarding Servers in a Shared Server Room

Servers may be considered "locked up" when physical protection is provided to the server unit itself. This may be done by utilizing a secure lid lock (to prevent physical intrusion into the server), secure drive locks (to prevent access to any drives), devices designed to lock-out possible sources of input/output (such as USB and serial ports, network interfaces, and ps/2 ports), and anchoring pads or cables to secure the server to the rack/table where it is located (to prevent removal of the server).

Servers may also be considered as locked up when they are placed within a lockable caged-in area within a server room. Lockable cages can incorporate separate access control and intrusion detection devices in addition to those installed for sever room access. Other access control measures can be used in conjunction to ensure sufficient monitoring of access as determined by a TRA. Servers can also be considered as locked up when they are located in a container listed in the RCMP Security Equipment Guide G1-001.

2.2. Secure Server Room

For the purposes of this appendix, a "secure server room" refers to a room in which the walls, door, and hardware are constructed similar to the specifications of a Secure Storage Room as outlined in G13-01 Secure Storage Rooms (SSR) while accounting for sever room specific design/construction requirements (such as additional electrical, vents and ducts, and air conditioning), as well as threats to the server as determined in a TRA.

Access to this room should be limited to essential personnel who are appropriately security screened with an operational need to access, and/or properly escorted visitors. The secure server room should be continuously monitored with an electronic intrusion detection system to ensure control of access. Additional access control measures can be implemented if determined by a TRA.

2.3. Secure Data Centre

A server room may be considered a Secure Data Centre when it is continuously monitored by personnel occupying a control room with a glazed window or wall in between these locations. The glazing should permit observation of the servers. Any areas considered out of direct view by personnel should be continuously monitored by CCTV cameras. The layout should allow for the observation of anyone entering the room; including the monitoring of any area for signing in and presenting of identification for authorized personnel.

The perimeter of a Secure Data Centre should meet the construction standards for a Secure Demising Wall (SDW) as outlined in G13-02 Secure Demising Wall (SDW). The monitoring room must be occupied during hours in which access to the servers is permitted. When 24/7 is indicated, the control room must be occupied continuously. A TRA will determine if there is a

need for a secure data centre and any additional measures such as continuous occupation of the control room.

9. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-015 (2024) – Guide to the Application of Physical Security Zones, for approval.

Whalen,Lucus Dwyer,000356990 Digitally signed by Whalen,Lucus Dwyer,000356990 Date: 2024.09.23 09:38:05 -04'00'

Lucus Whalen,
A/Manager
RCMP Lead Security Agency

Date

Approved

I hereby approve GCPSG-015 (2024) – Guide to the Application of Physical Security Zones.

St-Pierre,Andre Vincent,000171484 Digitally signed by St-Pierre,Andre Vincent,000171484 Date: 2024.10.07 11:15:07 -04'00'

Andre St-Pierre,
Director, Physical Security
Royal Canadian Mounted Police

Date