Physical Security Considerations in Shared Space

GCPSG-023 (2025)

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

Publication Issued: 2025-10-20
Updated: YYYY-MM-DD

Royal Canadian Mounted Police Gendarmerie royale du Canada

Canada

Foreword

Physical Security Considerations in Shared Space 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 (GC) publication to serve as a guide for shared GC workplaces. It addresses the physical security factors to consider in these spaces and can be used by shared space providers, facility managers and all users of these GC workspaces.

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

Reproduction

Effective Date

The effective date of GCPSG-023 (2025) – Physical Security Considerations in Shared Space is 2025-10-20.

Acknowledgement

The RCMP LSA would like to express gratitude to the United Kingdom's National Protective Security Authority (NPSA) whose research greatly informed this document. The works - SHARED WORKSPACES-Security Guidance for Users, and SHARED WORKSPACES-Security Guidance for Providers, provided a valuable foundation for understanding the complexities and dynamics of shared workspaces. Their expertise and published findings were instrumental in shaping both the analysis and conclusions presented herein.

Record of Amendments

Amendment No.	Date	Entered By	Summary of Amendment

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 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 purpose of this guide is to inform departments and agencies entering into the use of shared space about physical security concerns and solutions. Included in this guide are the application and efficiency of these solutions from both the provider and user perspectives. Following these basic steps will help to safeguard shared space, and minimize risks to the personnel, information, and assets of the GC.

1.2. Applicability

This guide applies to GC providers of shared space, security functional specialists assigned physical security responsibilities in shared spaces, GC facility or property managers and, for all users of shared space. This includes property management personnel and decision makers with a risk management or risk acceptance authority within the department or agency making use of shared space options.

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

All employees of the GC have a shared 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 GC 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**
CCTV	Closed Circuit Television
CPTED	Crime Prevention Through Environmental Design
CSE	Communications Security Establishment
CSO	Chief Security Officer
DSM	Directive on Security Management
EDI	Equity, Diversity, and Inclusion
EID	Electronic Intrusion Device
GC	Government of Canada
HSZ	High Security Zone
OZ	Operations Zone
PGS	Policy on Government Security
RCMP LSA	RCMP Lead Security Agency for Physical Security
RCMP	Royal Canadian Mounted Police
RZ	Reception Zone
SSC	Shared Services Canada
SZ	Security Zone

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.
Compromise	Unauthorized disclosure, destruction, removal, modification, interruption or use of information or assets.
Defense-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.
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. The term encompasses both the physical object and its use (i.e., weapons' ranges, agriculture fields)
Insider risk	An individual with authorized access who harms an organization's or nation's national security, assets, or operations, either intentionally or unintentionally. This threat can include espionage, terrorism, unauthorized data disclosure, or the loss or degradation of resources. Actions may include criminal activity, physical threats or actions, espionage, subversion, and sabotage.
Mitigation	Activities taken to reduce risks.
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.
Provider	A provider is a broad term for an entity that owns, operates, or manages a facility to other parties. This could be Public Service and Procurement Canada (PSPC) or another lessor.
Safeguards	Assets or external controls that reduce overall risk to employees, other assets, or service delivery by decreasing the likelihood of a threat event, reducing the probability of compromise, or mitigating the severity of the outcome through direct or indirect interaction with asset values, threats, or vulnerabilities.
User	A user is any person, group, department or agency who uses a space for an authorized purpose. Users may be employees, visitors, or contractors or others authorized to use the space.
Vulnerability	An inadequacy related to security that could increase susceptibility to compromise or injury.

5. Security Guidance for Shared Space Providers

Shared spaces provide innovative and flexible environments for individuals and organizations to collaborate, innovate, and grow. Shared spaces cater to a wide range of users, offering cost savings by sharing resources and fostering collaboration. Such dynamic environments also present unique physical security challenges, with sensitive information, intellectual property, and equipment often at risk of theft, unauthorized access, or accidental exposure.

Workspace providers play a critical role in establishing the foundation for security within these spaces. By implementing appropriate security measures, you not only protect your users, their property and privacy, but also safeguard your facility, assets, and reputation. Effective security practices enhance user trust, support compliance with security requirements, and create an environment where innovation can thrive.

In shared spaces, it is imperative that security is considered right from the start. Strategies for designing, retrofitting, and maintaining facilities that meet diverse user needs must be part of the overall process. By understanding the specific risks associated with shared workspace and applying appropriate controls, providers can ensure the safety and collaboration sought by users of shared space.

5.1. Understanding Users’ Threats and Risks

Shared spaces can be attractive targets for those seeking to gain unauthorized access to sensitive information, assets or systems. The same open, collaborative environments that make them appealing to users can also allow individuals with malicious intent to gain, or appear to have, legitimate access to your users’ information and assets. As a shared space provider, understanding the threats, risks and vulnerabilities and how adversaries may exploit them is essential to safeguarding the GC.

- **State Actors:** State Actors may target users handling sensitive projects or research. They exploit vulnerabilities to access user data which damages both the reputation and the integrity of GC information and assets;
- **Competitors**: Competitors may use shared spaces to gather information on users or operations. They could pose as legitimate users, undermining user confidence and the department or agency reputation;
- **Cyber Criminals:** Although not the focus of this guidance, cyber criminals exploit digital systems like Wi-Fi or access controls. Breaches disrupt services, expose data, and damage infrastructure, causing downtime and reputational harm;
- **Opportunistic Criminals:** Opportunistic criminals exploit opportunities in shared spaces, targeting things such as; unattended devices, information, assets, or people. They may seek to gain access by legitimate means and once inside, take advantage of open environments to identify vulnerable targets;
- **Insider Risk:** A person with authorized access or understanding of an organization that causes harm to that organization either intentionally or unintentionally negatively affects the integrity, confidentiality, and availability of the organization, its

data, personnel, or facilities by; espionage, terrorism, unauthorized disclosure of information, crime, sabotage, or violence; and

- **Protesters:** Protesters may target shared spaces by way of disruption or vandalism. This could be based on issues relating to users' business activities or supply chains. Their actions harm reputation and impact productivity.

Note: Any of these threat actors could present as legitimate shared workspace users, visitors, or contractors.

5.2. Appropriate Physical Security Measures

It is understood that shared spaces aim to be environments that maximize collaboration and space saving. This however, is only possible if security risks are managed appropriately. This is made more complex when considering the varying needs of departments and agencies using the space for a variety of reasons and working with different levels of sensitivity.

There are different space requirements even in shared spaces. Zoning is still required based upon the categorization of information being processed or stored, however most shared space will be considered an operations zone environment.

It may also be necessary to offer "neighbourhoods" to departments and agencies that need to be close to one another in a shared space. The use of the "neighbourhood" model may also be beneficial for departments and agencies to maintain the need-to-know, need-to-access principles of information and asset protection. This may be for collaborative, or for security of information purposes. In some cases, security zones may also need to be established for working on information at higher categorization levels. Private spaces may also be needed for having conversations of higher sensitivity, to prevent overhearing or simply for the comfort of those working in the space.

The physical security and other measures recommended for operations zones in shared spaces focus primarily on awareness and basic provisions, whereas those for security zones or private spaces cover more advanced security controls and management practices. It is important to remember that a space provider must offer the minimum security requirements based upon the zones required in the shared space.

5.3. Security Screening

As for any facility or property in the GC, there is a requirement to ensure access is granted only to those holding the appropriate security status or clearance. It will be a joint responsibility between the provider and the user(s) to ensure all those who are granted access to the shared space are appropriately security screened and are in possession of the required security status or clearance.

5.4. Types of Space

The physical security requirements for operations zones and security zones are detailed in GCPSG-015 – Guide to the Application of Physical Security Zones. Physical security zones in shared space should be built and managed using the same guidance as those in single department spaces and, in fact, require greater control and management to ensure the security of GC information, assets and people. In addition to the above guidance, physical security zones in shared spaces could include:

- **Operations Zones:** Operations zones (OZ) are designed for collaboration, shared equipment, and communal areas. Providers must prioritize accessibility and baseline security for diverse users while maintaining the physical and other security requirements of the OZ;
- **Security Zones:** Security zones (SZ) cater to users handling sensitive information, where security is a priority. These spaces require providers to implement enhanced security measures aligned with RCMP guidance and best practices;
- **High Security Zones:** High Security Zones (HSZ) are among the highest security spaces and must be treated as such despite the need for diverse, shared space. These will be rare but all physical security and other security measures must be considered prior to commissioning such a space in a shared facility;
    - **Private Spaces:** Private spaces such as, private offices, boardrooms or quiet rooms set up within any of the above zones offer users greater control over their environment, allowing for more tailored security and privacy. These spaces are typically used by individuals or small teams requiring a dedicated workspace away from other users for focused work or sensitive discussions where a need to know within the shared space needs to be respected.

5.5. Security Culture in Shared Space

For shared space providers, fostering a strong security culture is not only part of your duty of care to users, but also a key differentiator in attracting and retaining clients. By promoting a proactive, security-conscious culture, providers can build trust, strengthen reputation, and better support their users as their security needs develop.

The appointment of a shared space security committee is an important step in building a strong security culture. Other factors for the promotion of a strong security culture include:

- **Security Awareness and reporting:** Highlighting security awareness encourages users to report suspicious behaviour. This can be achieved through approachable staff, messaging, and signage. It fosters the adoption of security policies and reporting procedures and continuously seeks user feedback to improve shared space security;
- **Collaboration and accountability:** Collaboration when implementing security policies and procedures ensures the needs of both GC and the user are met. Conduct regular review sessions with users to review and address ongoing or emerging security concerns. Provide training for users on the use and security of all spaces within the shared space and how to conduct effective visitor management; and

- **Compliance and trust:** Promote communication amongst all shared space users to ensure compliance with security requirements. Assign dedicated staff to shared spaces to ensure quick, effective communication on security-related needs. Build trust by demonstrating consistent application of security policies and practices, such as access control and visitor management procedures.

5.6. Design and Fit-up of Shared Space

When designing shared spaces, providers should consider security measures from the outset and use the FSA&A process for this purpose. An integrated, holistic approach to security at this stage of the process supports flexibility in operations and scalability of security controls.

Consider the users requirements and RCMP guidance when determining the most appropriate security control measures needed when designing shared space. Define the space zoning requirements and implement all physical security requirements of these zones and, determine what access control points between zones are necessary. It may also be helpful to consider if separation of neighbourhoods is necessary and what security controls may be required in these cases.

Consider what security systems are required by each user and try to find commonality in the application of these systems. It would also be helpful at this stage to determine if and what user will have access to these systems and what that level of access will be (viewer or administrator). Ensure to design and install appropriate security systems with performance and adaptability/scalability needs of all users in mind. Install Closed Circuit Television (CCTV), access control, and intrusion detection systems that allow for upgrade or adaptability to accommodate evolving user needs. Ensure all security systems meet GC security requirements and RCMP guidance.

If designing stand-alone buildings as a shared space, consider natural surveillance protection. Crime Prevention Through Environmental Design (CPTED) principles support security considerations by providing clear sight lines to increase visibility, clearly defined boundaries between public and controlled areas, use of lighting to provide conditions which support safety and security, and cleaning and maintenance routines to demonstrate space ownership.

5.7. Privacy Concerns in Shared Space

Ensuring user privacy is a core expectation for shared space providers. By tailoring privacy measures to security zoning and other requirements, providers can balance security with the collaboration that users desire.

Operations Zones: In OZs, provide bookable meeting rooms or quiet rooms to support user privacy. Install screens in communal areas such as kitchens or break areas to provide a basic degree of privacy for users. Regularly remind users to use private areas for sensitive or loud discussions and to secure belongings when in shared spaces. Ensure clear communication channels for users to report any privacy concerns and put measures in place to address these issues promptly.

Private Spaces: Allow users to customise their spaces with privacy measures like blinds or departmental security containers. Fit blinds or privacy film on glazed partitions and windows, offer secure, lockable storage for user belongings and provide shredders or destruction services. Escort third parties and contractors conducting work on your behalf, when they require access to a user's private space. Engage with users to identify their privacy needs during onboarding and support customisation requests where feasible. Include user privacy requirements such as, solid or frosted glass walls or acoustic protections in service agreements and periodically review and update them.

Security Zones: Support user-specific privacy needs by providing all security requirements in a SZ. Provide high security locks as per RCMP guidance and access control that gives users an auditable record of who accessed their spaces. Provide acoustic spaces if required, considering RCMP guidance as required, and escort third parties and contractors when conducting work on your behalf, particularly when they require access to SZs. Support users by providing clear guidance on escorting protocols and providing necessary resources, such as temporary visitor passes or monitored access points. Conduct regular reviews of security measures and ensure compliance with agreed processes and procedures.

5.8. Physical Security Systems in Shared Space

A secure environment helps users work confidently in any space. Providers should implement measures that support deterring and preventing unauthorised access, monitoring of activity, and responding to incidents.

	Operations Zone	Private Spaces	Security Zones
Systems Criteria	Ensure all workspace entrance/exit points and any other high risk areas are covered by CCTV.	Offer users the ability to introduce additional security measures like departmental locks or security containers to private areas.	Provide enhanced technologies such as biometric access and intrusion detection.
Enhancements	Provide access control barriers that prevent tailgating. Ensure there is progressive access control between zones and neighbourhood within the space.	Install access control systems, such as locks and card readers, to private offices and rooms.	Fit enhanced access control systems for specific spaces, critical areas, or rooms, supplemented by additional CCTV surveillance. Provide segregation where necessary.
Behaviours	Train staff to monitor shared spaces and how to identify and report suspicious activity.	Regularly inspect all physical security system devices and promptly address any user-reported issues.	Introduce additional security protocols such as supervised entry for third-party personnel.

Governance	Operate and maintain a process for regularly reviewing and updating physical security systems based on user feedback.	Ensure compliance with security requirements to identify suspicious access patterns and ensure user specific requirements are being met.

5.9. Access Management and Visitor Control

Some shared spaces have deliberately relaxed entry policies. However, it is important to strike the right balance between openness and prevention of unauthorised access. It is important that you provide a space that manages access well to mitigate risks effectively and provide users with the reassurance they desire. For complete access control requirements refer to RCMP guidance on access control however some considerations are listed in the chart below.

	Operations Zone	**Private Spaces**	**Security Zones**
Systems Criteria	Select visitor management systems suitable for your busiest times and train reception staff on their use.	Provide users with customisable access systems and clear visitor registration protocols.	Support advanced visitor pre-approval systems and integrate identity verification solutions.
Enhancements	Provide staffed receptions in addition to physical security systems.	Deploy access controls credentials for specific spaces.	Use appropriate access controls for critical areas, preventing unauthorized entry.
Operational Practices	Train staff to monitor visitor activity and to recognise and report suspicious behaviour.	Ensure workspace visitor policies are followed, such as escorting and signing in guests.	Ensure visitors are pre-screened and escorted at all times after entering security zones.
Governance	Ensure visitor logs are retained securely and for a defined period and resolve access-related issues transparently.	Regularly review access logs for user spaces and address non-compliance swiftly.	Ensure compliance with access requirements to SZs, enforce user adherence and address identified non-compliance swiftly.

5.10. Operational Security and Incident Management

Operational security and incident management relates to the role that people, policies and procedures play in the everyday operation of a shared space. The way in which security issues are being prevented, handled and, resolved if one occurs is important. Provide users with reassurance that security incidents that occur are taken seriously and dealt with quickly.

Threat and risk awareness is important and identifies potential risks in OZs such as theft or misuse of shared resources, supports users in establishing risk assessment practices for private spaces, and allows for the assessment of SZs for targeted threats, such as espionage or sabotage.

Providers should develop a range of basic emergency management procedures for staff to follow in the event of an incident at the workspace or nearby. Collaborating with users to define space specific emergency plans promotes alignment with space-wide needs. Implementing tailored emergency plans, including secure evacuation routes and lockdown capabilities ensures the ongoing protection of security areas which safeguards GC information and assets.

Provide a central point of contact for reporting security incidents or suspicious activity and ensure all users are aware of when, how and who to report. Ensure prompt containment measures for incidents involving sensitive material, coordinating directly with affected users, and law enforcement if necessary. Departments should refer to the Mandatory Procedures for Security Event Management Control at Appendix G of the Directive on Security Management (DSM).

Lessons learned from incidents are an important part of the process. Maintain an incident log and review patterns to make continual improvements to security controls. Conduct regular reviews of user feedback and review any incidents in detail to improve overall security. Hold post-incident reviews to identify lessons learned and collaborate with users to strengthen security.

5.11. Cyber Security

As previously mentioned, this guidance is not specific to cyber security and any specific concerns in this area should be addressed by the Communication Security Establishment (CSE) or Shared Services Canada (SSC). The security of IT systems within shared spaces requires providers to play a proactive role. Cyber-attacks come in many forms, but the vast majority can be mitigated by implementing a few essential controls. It is important to ensure all cyber security arrangements are in place and conduct audits to verify their effectiveness.

Providers play a huge role in supporting users to protect the digital infrastructure and minimising the impact of cyber incidents. Providers are encouraged to share the tips for staying secure online with users, which includes advice that all users should follow to stay secure online and keep their devices safe.

6. Security Guidance for Users

Shared workspaces offer flexible and cost-effective solutions for individuals and organisations. These environments are designed to support creativity, collaboration, and scalability. They cater to a wide range of users offering shared resources and fostering partnerships.

Shared workspaces also bring unique security challenges whether you're sharing workspaces in a coworking area, processing sensitive information, using sensitive equipment, or just trying to have a conversation in the shared area. These spaces can be vulnerable to unauthorised access or accidental disclosure of information presenting different security risks.

This section is for users of shared workspaces and provides advice to help you safeguard your information and assets. By understanding the space areas and environments, you can identify the measures most relevant to your circumstances and by understanding the threats and risks, and then applying appropriate steps, you can fully embrace the benefits of shared spaces while protecting your information, assets and others using the space.

6.1. Who are You at Risk From

Shared space can present easy targets to threat actors seeking unauthorised access to sensitive information and assets. The open, collaborative environment that makes them popular, make then easy to access from someone with ill intent. As a shared space user, it is important that you understand the key threat actors that might seek to exploit these vulnerabilities to gain access to GC information and assets.

- **State Actors:** State Actors may target users handling sensitive projects or research. They exploit vulnerabilities to access user data which damages both reputation and the integrity of GC information and assets;
- **Competitors**: Competitors may use shared spaces to gather information on users or operations. They could pose as legitimate users, undermining user confidence and the department or agency reputation;
- **Cyber Criminals:** Although not the focus of this guidance, cyber criminals exploit digital systems like Wi-Fi or access controls. Breaches disrupt services, expose data, and damage infrastructure, causing downtime and reputational harm;
- **Opportunistic Criminals:** Opportunistic criminals exploit opportunities in shared spaces, targeting things such as; unattended devices, information, assets, or people. They may seek to gain access by legitimate means and once inside, take advantage of open environments to identify vulnerable targets;
- **Insider Risk:** A person with authorized access to an organization and intentionally or unintentionally causes harm negatively affecting the integrity, confidentiality, and availability of the organization, its information, assets or personnel by; espionage, terrorism, unauthorized disclosure of information, crime, sabotage, or violence; and
- **Protesters:** Protesters may target shared spaces by way of disruption or vandalism. This could be based on issues relating to users' business activities or supply chains. Their actions harm reputation and impact productivity.

Note: Any of these threat actors could present as legitimate shared workspace users, visitors, or contractors.

6.2. Which Type of User are You?

Identify which type of user aligns closest with your particular circumstances for tailored guidance on managing security risks in shared space. While these illustrate typical activities and security measures, they do not cover every situation. Refer to Types of Space for more in-depth guidance depending on the type of space that you are using.

	Casual User	Continuous User	Specialty User
Profile	Workers who only make use of shared space occasionally, using hot desking for convenience.	Workers who use shared spaces everyday and need flexibility of all spaces within the facility.	Workers who use SZs for processing and storing highly sensitive information on a continual basis.
Space Needs	Workspace with internet and access to private spaces for sensitive work. Occasional access to SZs.	Flexible workspace options for individual work and team collaboration. Access to private spaces for confidentiality and access to communal resources like meeting rooms.	Private workspace with enhanced security measures.
Considerations	Select a workspace which provides access to the spaces you need while ensuring device and document protection in communal areas. Select your workspace based upon your security needs.	Maintaining flexibility of workplace selection while maintaining control over access to your information and assets. Ensure that shared resources outside of private spaces are used appropriately. Be mindful when using shared resources or open areas.	Selecting a space that can meet security requirements. Consider other users of the space and their impact on your security. Select your SZ workspace based upon your security needs.

6.3. Appropriate Physical Security Measures

It is understood that shared space users want to make the most of shared space benefits while managing security risks. A key consideration is that shared space users will require the use of different spaces and functions at different times. There are different space requirements even in shared spaces and zoning is still required based on the categorization of information or asset being processed or stored. Most shared space facilities will be considered an OZ environment however the ability to process or store higher categorizations of information or assets may be required.

It may also be necessary to work in "neighbourhoods" specific to your department or agency with the idea that staff need to be close to one another in a shared space. This may be for collaborative purposes or for security of information purposes to prevent overhearing.

The physical security and other measures recommended for OZs in shared spaces focus primarily on awareness and basic provisions, whereas those for SZs or private spaces require more advanced security controls and management practices. It is important to remember that users must adhere to all security requirements based upon the zone in which they are working.

Users may be required to transport or transmit information or assets to and from the shared space from time to time. It is important to remember that security of information and assets while in transit is important especially in shared spaces. For information and security requirements while transporting or transmitting information and assets refer to RCMP guide GCPSG-007 – Transport, Transmittal and Storage of Protected and Classified Material.

6.4. Security Screening

As for any facility or property in the GC, there is a requirement to ensure access is granted only to those holding the appropriate security status or clearance. It will be a joint responsibility between the provider and the user(s) to ensure all those who are granted access to the shared space are appropriately security screened and are in possession of the required security status or clearance. It is also important to remember that this is also the responsibility of the user to ensure their security status or clearance remains valid and that they only access information and assets up to their security categorization level.

6.5. Types of Space

The physical security requirements for OZs and SZs are detailed in GCPSG-015 – Guide to the Application of Physical Security Zones. Physical security zones in shared space should be built and managed using the same guidance as those in single department spaces and, in fact, require greater control and management is required to ensure the security of GC information, assets and people. Physical security zones in shared spaces could include:

- **Operations Zones:** OZs are designed for collaboration, shared equipment, and communal areas. Users share the space and facilities, share equipment and desks meaning there is limited control over physical access to individual workspaces. Users should be aware of their general security awareness, maintenance of confidentiality and safeguard their information and assets in open areas and maintain the physical and other security requirements of the OZ;

- **Security Zones:** SZs cater to users who routinely handle sensitive information or assets in their workspaces. Users should ensure all enhanced security measures for the protection of material processed or stored in these zones align with RCMP guidance and best practices;
- **High Security Zones:** HSZs are among the highest security spaces and must be treated as such despite the need for diverse, shared space. These will be rare but all physical security and other security measures must be considered prior to processing information in such a space in a shared facility;
    - **Private Spaces:** Private spaces such as, private offices, boardrooms or quiet rooms set up within any of the above zones offer users greater control over their environment, allowing for more tailored security and privacy. These spaces are typically used by individuals or small teams requiring a dedicated workspace away from other users for focused work or sensitive discussions where a need to know within the shared space needs to be respected.

6.6. Security Culture in Shared Space

For shared space users, developing a security culture is a journey that evolves with your workspace and needs. Whether working in an OZ, private space, or SZ, it all starts with basic awareness and builds toward stronger practices. Security is a shared responsibility between all parties using a shared space. Users who participate on a shared space security committee helps link providers and users together to help build a strong security culture. Other factors for the promotion of a strong security culture include:

- **Security Awareness and reporting:** Understand the risks of shared spaces, such as tailgating or overheard conversations. Promote a culture where reporting suspicious behaviour or misplaced passes is second nature and adopt and comply with good security habits, like securing devices and documents when you are not using them;
- **Collaboration and accountability:** Set the example by exemplifying and promoting security-conscious behaviours within your space. Ensure everyone takes ownership of monitoring access into your space and work closely with your space provider to address potential vulnerabilities in all areas within the space; and
- **Compliance and trust:** Reinforce appropriate handling of sensitive information and assets through discussions and training. Establish clear expectations with workspace providers to meet security needs and periodically review incidents and adjust security behaviours to stay aligned with best practices.

6.7. Privacy in the Shared Space

As some of the key benefits of shared spaces are collaboration and networking, it is to be expected that ensuring privacy may be a challenge. Nonetheless, it is possible to have a shared space that allows you to manage your privacy as effectively as possible, and to act in way that makes it more difficult for someone to overhear or view your sensitive information. By taking privacy seriously and utilizing the appropriate zone for conversations and other work requirements, a balance can be achieved between security and functionality that users desire.

Operations Zones: In OZs, bookable workspaces provide easy means of collaboration and networking however, not all measures to ensure privacy and security are present as the space is used by many people working for numerous departments and agencies. Privacy measures users can take in OZs include:

- Using meeting rooms or quiet rooms when necessary to support privacy;
- Installing privacy screens/shields on computers provide a basic degree of privacy against "shoulder surfers";
- Selecting a desk away from high traffic areas;
- Securing documents or computers if unattended, even for short durations;
- Being aware of your surroundings when working with sensitive information even if it is not classified;
- Not taking or making calls in the open areas; and
- Maintaining a clean desk policy, removing and securing all material when you will be away from the workspace.

Private Spaces: In private spaces, users should ensure all appropriate measures are available to ensure privacy and security. Remember that not all measures to ensure privacy and security are guaranteed as the space is used by many people working for a variety of departments and agencies. Privacy measures users can take in Private Spaces include:

- Ensuring privacy measures like blinds installed on partition windows are used;
- Using security containers for securing information and assets when required;
- Using appropriate shredders or destruction services for secure destruction;
- Installing privacy screens/shields on computers to guards against "shoulder surfers";
- Securing documents or computers if unattended, even for short durations;
- Being aware of your surroundings when working with sensitive information even if it is not classified;
- Maintaining a clean desk policy, removing and securing all material when you will be away from the workspace; and
- Ensuring all third parties and contractors are escorted or have appropriate security status or clearance when in private areas and challenging those who appear out of place or not displaying the correct badging.

Security Zones: In SZs, users should ensure all appropriate measures are available to ensure privacy and security. It is important to remember however that even though SZs support user-specific security and privacy needs for sensitive projects and should provide all security requirements of a SZ, not all measures should be taken as a guarantee as the space could be used by many people working for numerous departments and agencies. Privacy measures users can take in SZ include:

- Ensuring requirements for a SZ are present and sufficient and supported by your department or agency's Chief Security Officer (CSO) or security group;
- Not broadcasting your department or agency's occupation of the facility or space especially on tenant lists located in the building lobby;
- Ensuring privacy measures like blinds or glazing are installed on partition windows;

- Using specific high security containers issued by your department or agency for securing information and assets when required;
- Using appropriate shredders or destruction services for secure destruction;
- Installing privacy screens/shields on computers to guards against "shoulder surfers";
- Securing documents or computers if unattended, even for short durations;
- Being aware of your surroundings when working with sensitive information and assets especially when categorized as protected or classified;
- Maintaining a clean desk policy, removing and securing all material when you will be away from the workspace;
- Ensuring all third parties and contractors are escorted or have appropriate security clearance when in SZs and challenging those who appear out of place or not displaying the correct badging;
- Ensuring the use of high security locks as per RCMP guidance to secure the space;
- Ensuring access control requirements are followed (i.e. do not prop open doors for convenience);
- Ensuring there are appropriate acoustic restrictions if having conversations that require acoustic isolation or ask that a Special Discussion Area is provided; and
- Ensuring that deficiencies found in security measures are dealt with swiftly.

6.8. Access Management

Some shared spaces are deliberately relaxed about entry, meaning most are not designed for processing or working on highly sensitive or classified material. It is important that access is managed well in a shared space and work is only permitted up to the categorization level for which the space was built.

	Operations Zone	**Private Spaces**	**Security Zones**
Criteria	Ensure all shared space entrance/exit points have functioning access control systems and report any deficiencies.	Ensure that if the private space is a departmental space that all access control efforts are functional.	Ensure that all access control efforts are functional including; security containers specific to the department or agency and installed intrusion detection systems.
Enhancements	Access control in Shared Spaces is usually managed by the workspace provider however any additional requirements may be necessary depending on the organizations needs.		There may be a need for enhanced access control systems (i.e. multifactor authentication or biometrics).
Behaviours	Users should monitor shared spaces and identify and report suspicious activity including tailgating or unauthorized individuals.	Close and lock doors to a private space every time you leave. Use assigned access credentials (no sharing) to maintain access integrity.	Use all provided security equipment and follow all security procedures for entry into a SZ (i.e. leaving mobile devices outside the space).

6.9. Physical Security Systems

The extent of electronic security provided to shared spaces may vary. While all will have some type of access control, it is important to remember that shared resources like meeting rooms, Private Spaces and SZs may be shared with all tenants rather than dedicated to specific departments and agencies. User departments and agencies should ensure that all required physical security systems are available and functional prior to permitting staff to work in a shared space.

Departments and agencies should also confirm that all emergency procedures are in place and have been tested, such as evacuations and intruder response plans. If Private Spaces or SZs are occupied by departmental personnel only (i.e. neighbourhoods), ensure that all required security equipment, containers and access control systems are functional. Users should also confirm that any provider supplied services such as CCTV do not infringe upon workspaces and only capture images of common areas.

All departments and agencies using these shared spaces should confirm that all departmentally owned or controlled spaces and equipment are inspected routinely for tampering or unauthorized access. Departments and agencies should also confirm that all procedures such as visitor management and escorting are in place and being followed.

6.10. Cyber Security

As previously mentioned, this guidance is not specific to cyber security and any specific concerns in this area should be addressed by CSE or SSC. The security of digital systems and information requires everyone to play their part. Cyber-attacks come in many forms, but the vast majority can be prevented by implementing a few basic actions.

Available Wi-Fi should be protected with a strong password, ideally with separate networks for visitors and shared space users. Follow guidance for addressing cyber incidents, such as data breaches or network intrusions and ensure users follow all cyber security procedure to minimise risks, such as locking devices and leaving mobile devices outside SZ prior to entry including; mobile phones, personal wearable devices and computer equipment not certified for use in a SZ.

7. Conclusion

The rise of shared spaces represents a fundamental shift in how we think about and utilize GC workspaces. From the provider's perspective, these spaces offer a dynamic business model that offers flexibility, while fostering collaboration, space, and cost savings. For users, shared spaces deliver affordability, adaptability, and opportunities for collaboration that traditional offices often lack.

The success of this model depends on aligning the needs and expectations of both sides. Providers must continue to innovate, offering not just physical space, but services and experiences that add value while protecting GC information and assets. Users, in turn, must approach shared workspaces with clarity about their goals, a willingness to engage with the broader community while ensuring this new method of work does not put government security at risk.

Ultimately, shared workspaces are more than a real estate solution—they reflect evolving work cultures that prioritize flexibility, connectivity, and well-being. When thoughtfully executed, they can serve as a powerful platform for productivity, growth, and collaboration for all involved.

8. Reference and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- The International Crime Prevention Through Environmental Design Association
- SHARED WORKSPACES - Security Guidance for Users, National Protective Security Authority (NPSA) – United Kingdom
- SHARED WORKSPACES - Security Guidance for Providers, National Protective Security Authority (NPSA) – United Kingdom
- Lead Security Agency for physical security | Royal Canadian Mounted Police
- GCPSG-007 – Transport, Transmittal and Storage of Protected and Classified Material.
- GCPSG-015 – Guide to the Application of Physical Security Zones

9. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-023 (2025) – Physical Security Considerations in Shared Space, for approval.

Nattress,Shawn
Thomas,000302786

Digitally signed by Nattress,Shawn
Thomas,000302786
Date: 2025.10.20 10:31:58 -04'00'

Shawn Nattress,
Manager
RCMP Lead Security Agency

Date

Approved

I have reviewed and hereby approve, GCPSG-023 (2025) – Physical Security Considerations in Shared Space.

St-Pierre,Andre
Vincent,000171484

Digitally signed by St-Pierre,Andre
Vincent,000171484
Date: 2025.10.23 12:43:57 -04'00'

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

Date