Document Sanitization Guide

GCPSG-024 (2026)

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

Publication Issued: 2026-04-13
Updated: YYYY-MM-DD

Foreword

The GCPSG-024 – Document Sanitization Guide 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 and serves as a guide for properly sanitizing documents and plans for the GC and may be used by GC employees and others during the contracting process for GC projects and initiatives.

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-024 – Document Sanitization Guide is 2026-04-13

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 (LSA) for physical security for the GC, is responsible for providing advice and guidance on all matters relating to physical security.

1.1. Purpose

The purpose of this document is to serve as a guide for sanitizing building plans and documents prior to releasing them to third party contractors. Before sharing documents and facility drawings with external contractors, consultants, or the public, all sensitive information (technical and security related content) should be sanitized in accordance with information management policies contained in the Policy on Government Security (PGS) and their individual department or agency.

Security requirements are outlined below for removing or obscuring content such as, architectural, structural, electrical or mechanical design elements and security related information. Key objectives of this security practice are to:

- **Protect sensitive information** – Prevent the unauthorized disclosure of details that could compromise safety, security, or business interests.
- **Control access to sensitive information** – Ensure only relevant information is shared based on the recipient's role and need-to-know.
- **Apply consistency to ensure compliance** – Align with department/agency's security policies, legal obligations, and contractual security clauses within a Security Requirements Check List (SRCL) or Non-Disclosure Agreement (NDA).

1.2. Applicability

This guide applies to GC employees and is applicable to individuals who are responsible for the creation, distribution, and modification of construction documents and facility drawings and, when required, the necessary sanitization of those documents.

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

All employees of the 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

Information technology (IT) considerations may not always be necessary when formulating plans for physical security solutions. There is however, a constantly evolving threat regarding IT systems and with the convergence of physical and IT security, the requirement to assess the risk of IT applications and software connected to a network to operate and support equipment in GC controlled buildings is critical. Examples of these control systems could be for items such as, but not limited to, security lighting, perimeter gates, doors, HVAC, etc.

1.4.1. Security Assessment and Authorization

Before implementing any applications or software that will control or automate certain building functions, your departmental security requires the completion of a Security Assessment and Authorization (SA&A). This will ensure the integrity and availability of the components, the applications, 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 IT security.

1.4.2. Quantum Computing Considerations

Departments and agencies in the GC are accountable for managing cyber security risks in their program areas, and that includes systems that operate in conjunction with physical security systems. It is important that staff across the GC are aware of the quantum computing threat and the impact it may have on the systems they use or are responsible for. Quantum computers will use quantum physics to process information and solve problems that are impractical to solve using current computing capabilities.

Cryptography, which is the study of techniques used to make plain information unreadable, and then convert it back to a readable form, is an effective way to protect the confidentiality and integrity of GC information. The future of quantum computing threatens to break much of the cryptography we currently use, and steps need to be taken to protect and “future proof” the GC. It is recommended that departments and agencies transition existing cyber security solutions to use Post Quantum Cryptography (PQC) which are algorithms that are designed to be quantum-safe but that can be run on a conventional computer. For more information on quantum computing and PQCs, department and agencies should contact the Canadian Center for Cyber Security (CCCS).

In order to properly manage the quantum threat, CCCS recommends that departments and agencies evaluate the sensitivity of their information and determine its lifespan to identify information that may be at risk. Review their IT lifecycle management plan and budget for potentially significant software and hardware updates and educate their workforce on the quantum threat. Refer to CCCS cyber security guidance ITSE.00.017 for more information.

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
BIM	Building Information Modeling
CAD	Computer-Aided Design
CCTV	Closed-circuit television
DSM	Directive on Security Management
GC	Government of Canada
GCPSG	Government of Canada Physical Security Guide
HVAC	Heating, Ventilation, and Air Conditioning
NDA	Non-Disclosure Agreement
PGS	Policy on Government Security
RCMP LSA	RCMP Lead Security Agency for Physical Security
SDW	Secure Demising Wall
SRCL	Security Requirements Checklist
TBS	Treasury Board Secretariat of Canada

4. Glossary

Term	Definition
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)
Sanitization	The deliberate modification of documents and facility drawings to eliminate sensitive information that could compromise physical security, operational integrity, or proprietary knowledge.
Sensitive Information /	Refers to information or assets that requires protection against

Assets	unwarranted disclosure as compromise would reasonably be expected to cause injury in either the national or non-national interest (i.e. Classified or Protected information and assets).

5. Sanitization of Construction Project Documentation

In accordance with the Treasury Board Secretariat's (TBS) Directive on Security Management (DSM), departments are required to protect information against the unauthorized disclosure of sensitive material shared between GC and other governments (including foreign, provincial, territorial, and municipal), as well as international, educational and private organizations. Each department has the responsibility to categorize construction documents and facility drawings to the level of protection required and to ensure this material is appropriately sanitized before being distributed.

5.1. Preparation

Information within the project construction documents, including (but not limited to) design documentation, project correspondence, issued drawing sets, construction documentation, notices of change, addendums, project specifications, building information modeling (BIM) files and other documents must have common elements removed or obscured during sanitization. These include:

- Departmental or agency identifiers. Remove all references to the department or agency including (but not limited to):
    - Logos, insignias, or visual branding;
    - Facility names, site addresses, and signage; and
    - Email domains and references to unit or team names.

  Note: GC identifiers can be used.
- Room names and functions:
    - Sensitive rooms (such as data centers, secure storage, interview rooms, and executive offices) are to be labeled numerically (Room 101, Room 202) without functional identifiers;

  Note: Maintain a separate, access-controlled coded room list for internal reference.
- Security and sensitive assets – Do not depict or identify:
    - Physical security zones and classification levels;
    - Firearms storage, vaults, evidence rooms, exhibit rooms; and
    - Security equipment such as safes, panic buttons, cameras, or biometric readers.
- Security system infrastructure – Remove or isolate information within BIM software, as well as computer-aided design (CAD) layers that show:
    - Surveillance systems (CCTV camera locations);
    - Intrusion detection systems (motion sensors, door contacts); and
    - Access control systems (card readers, turnstiles).
- Mechanical, electrical, and plumbing (MEP) Systems – Remove detailed schematics that may expose vulnerabilities such as:
    - Critical HVAC components tied to secure zones;

    - Generator or emergency power layouts; and
    - Plumbing access points that could be exploited.
- IT infrastructure – Sanitize:
    - Server room locations and data cabling routes;
    - Telecommunications equipment and switchboard diagrams; and
    - Wireless access points and patch panels.

5.2. Important Considerations

There will be times when the function of a room will be self-evident, such as washrooms, private offices, or security areas, however sensitive system details associated with these spaces should be omitted.

Consider the cumulative sensitivity of multiple data points. Certain elements may become exploitable when combined, such as a safe location combined with a High Security zone label or signage. The identification of certain construction requirements, such as a secure demising wall (SDW), could indicate the room's purpose or indicate assets of interest.

It should be noted that various third parties, contractors, and sub-contractors will require different levels of information to complete their scope of work, including some that may be listed in section 5.1. The appropriate security screening for the contractor should be conducted for the level of information and the space they require access to on a case-by-case basis – however, any items not relevant to the completion of their work must still be considered for sanitization.

6. Secure Handling of Construction Project Documentation

All project information, including but not limited to design documentation, project correspondence, issued drawing sets, construction documentation, notices of change, addendums, project specifications, BIM files and so on, are to be managed in accordance with the terms outlined in the associated contract Security Requirements Checklist (SRCL) or arrangement. Access to construction documents and facility drawings should be limited to authorized individuals who require access to perform assigned work-related activities; the "need-to-know" principle. Consult GCPSG-007 Transport, Transmittal and Storage of Protected and Classified Material for more information.

Construction documents and facility drawings are to be treated as controlled documents, subject to the following safeguards:

- Access control:
    - Limit access to authorized individuals who have the need-to-know; and
    - Validate security categorization and security status or clearance level where applicable.
- Transmission:
    - Use secure digital communication (file-sharing) approved by the department; and

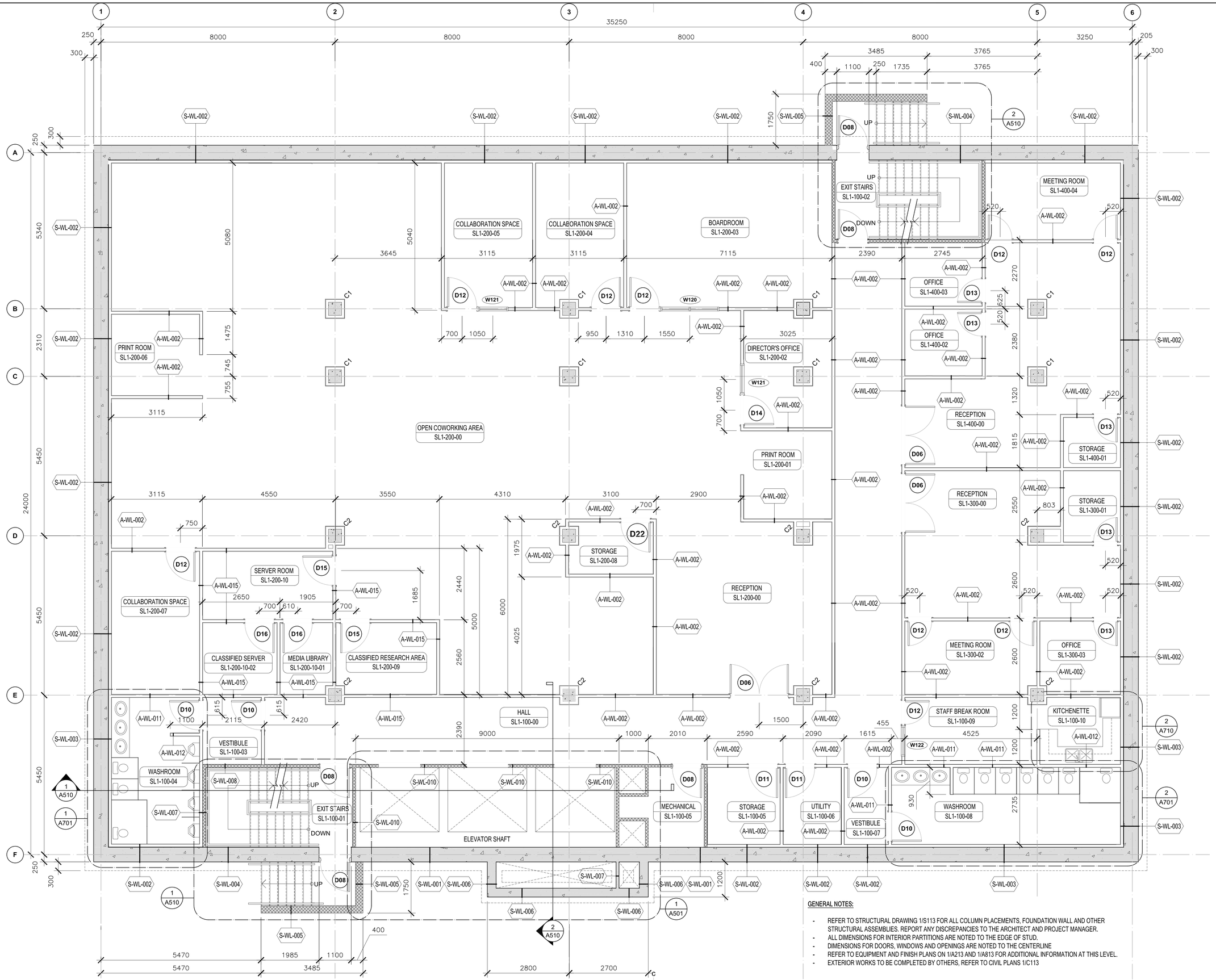
    - Ensure all sensitive layer data or meta data is sanitized. This material could still have an amount of data that, although limited, may still contain sensitive information.
- Storage:
    - Store and handle physical and digital copies of the construction documents and facility drawings to the level of security categorization, and in accordance with GCPSG-007 Transport, Transmittal and Storage of Protected and Classified Material; and
    - Maintain access and distribution logs, especially for sensitive or classified projects.
- Referential Guidance:
    - Consult the SRCL and Contract Security Manual for specifications related to safeguarding sensitive project information.

7. Approved Sanitization Methods

Sanitization may involve one or more of the following methods:

- Redaction:
    - Permanently remove or black out sensitive information (for example, annotations, legends, references).
- Layer management:
    - Delete sensitive layers (for example, security, IT, HVAC) from CAD or BIM files before release.
    - Retain an internal master copy with full layer access.
- Obfuscation:
    - Replace identifying names or descriptions with generic terms or codes (for example, "Secure Room" → "Room 130").
- File flattening:
    - Export the sanitized drawing to a non-editable format (for example, PDF or image) to prevent further manipulation or layer inspection.
- Watermarking:
    - Clearly label distributed versions with disclaimers such as "For External Use – Sanitized Copy" or "Confidential – Do Not Redistribute".

8. Pre and Post Sanitized Floorplan Example



GENERAL NOTES:

- REFER TO STRUCTURAL DRAWING 1/S113 FOR ALL COLUMN PLACEMENTS, FOUNDATION WALL AND OTHER STRUCTURAL ASSEMBLIES. REPORT ANY DISCREPANCIES TO THE ARCHITECT AND PROJECT MANAGER.
- ALL DIMENSIONS FOR INTERIOR PARTITIONS ARE NOTED TO THE EDGE OF STUD.
- DIMENSIONS FOR DOORS, WINDOWS AND OPENINGS ARE NOTED TO THE CENTERLINE
- REFER TO EQUIPMENT AND FINISH PLANS ON 1/A213 AND 1/A813 FOR ADDITIONAL INFORMATION AT THIS LEVEL.
- EXTERIOR WORKS TO BE COMPLETED BY OTHERS, REFER TO CIVIL PLANS 1/C113

Canada

Public Works and Government Services Canada
Travaux publics et services gouvernementaux Canada

Real Property Branch
Direction générale des biens immobiliers

Contractor to verify all dimensions & conditions on site and immediately notify the departmental representative of all discrepancies.

revisions	description	date
3	ISSUED FOR CONSTRUCTION	2026-03-01
2	ISSUED FOR TENDER	2025-12-01
1	ISSUED FOR REVIEW	2025-10-30

A detail no., no. du détail
B location drawing no., sur dessin no.
C drawing no., dessin no.

project / projet

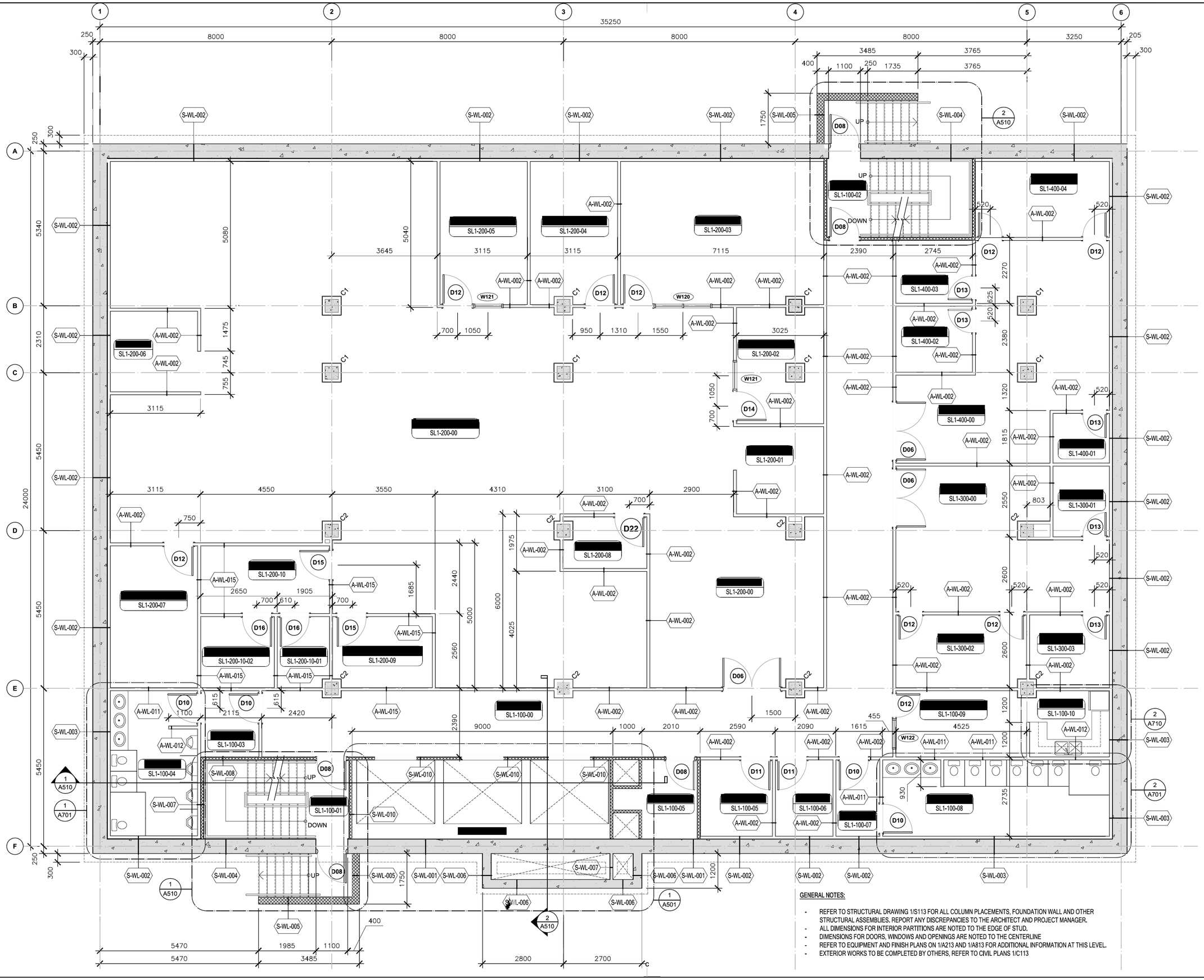
ROSEWOOD BUSINESS COMPLEX | CANADIAN AUDITING AGENCY

175 LEIKIN DRIVE, OTTAWA, ONTARIO

drawing / dessin

SUB-LEVEL 1 FLOOR PLAN

Designed By / Conçu par	DEVIN PUMPHREY	
Date	2023-11-30	(yyyy/mm/dd)
Drawn By / Dessiné par	ALEXANDRE WYCZYNSKI	
Date	2025-10-01	(yyyy/mm/dd)
Reviewed By / Examiné par	SHAWN NATRESS	
Date	2025-10-30	(yyyy/mm/dd)
Approved By / Approuvé par	ANDRE ST-PIERRE	
Date	2025-11-28	(yyyy/mm/dd)
Tender / Soumission		
Project Manager / Administrateur de projets	ALEXANDRE WYCZYNSKI	
Project no. / No. du projet	X864951372-A	
Drawing no. / No. du dessin	A113	



Canada

Public Works and Government Services Canada
Travaux publics et services gouvernementaux Canada

Real Property Branch
Direction générale des biens immobiliers

Contractor to verify all dimensions & conditions on site and immediately notify the departmental representative of all discrepancies.

revisions	description	date
3	ISSUED FOR CONSTRUCTION	2026-03-01
2	ISSUED FOR TENDER	2025-12-01
1	ISSUED FOR REVIEW	2025-10-30

A detail no. no. du detail
B location drawing no. sur dessin no.
C drawing no. dessin no.

project / projet

[redacted]

drawing / dessin

SUB-LEVEL 1 FLOOR PLAN

Designed By / Conçu par	[redacted]	
Date	2023-11-30	(yyyy/mm/dd)
Drawn By / Dessiné par	[redacted]	
Date	2025-10-01	(yyyy/mm/dd)
Reviewed By / Examiné par	[redacted]	
Date	2025-10-30	(yyyy/mm/dd)
Approved By / Approuvé par	[redacted]	
Date	2025-11-28	(yyyy/mm/dd)
Tender / Soumission		
Project Manager / Administrateur de projets	[redacted]	

Project no. / No. du projet: X864951372-A

Drawing no. / No. du dessin: A113

9. References and Source Documents

- Policy on Government Security- Canada.ca
- Directive on Security Management- Canada.ca
- 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
- GCPSG-007 Transport, Transmittal and Storage of Protected and Classified Material
- GCPSG-015 Guide to the Application of Physical Security Zones
- Security Requirements Check List (SRCL)

10. Promulgation

Reviewed and recommended for approval.

I have reviewed and hereby recommend, GCPSG-024 (2026) – Document Sanitization Guide, for approval.

Nattress,Shawn Thomas,000302786 Digitally signed by Nattress,Shawn Thomas,000302786 Date: 2026.04.14 08:05:19 -04'00'

Shawn Nattress, Date
Manager
RCMP Lead Security Agency

Approved

I have reviewed and hereby approve, GCPSG-024 (2026) – Document Sanitization Guide.

Lafrance,Gaetan Joseph,000133993 Digitally signed by Lafrance,Gaetan Joseph,000133993 Date: 2026.04.20 10:31:57 -04'00'

Gaetan Lafrance, Date
(A) Director, Physical Security
Royal Canadian Mounted Police