Guide de l’expurgation des documents

GSMGC-024 (2026)

Rédigé par :
Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
Sécurité ministérielle
Direction générale
73 promenades Leikin Ottawa Ontario, K1A 0R2

Date de publication : 2026-04-13
Date de mise à jour : YYYY-MM-DD

Avant-propos

GSMGC-024 – Guide de l'expurgation des documents, une publication NON CLASSIFIÉE, publiée avec l'autorisation du principal organisme responsable de la sécurité matérielle de la Gendarmerie royale du Canada (POSM-GRC).

Il s'agit d'une publication du gouvernement du Canada (GC) qui sert de guide pour la mise à jour des documents et des plans du GC ; elle peut être utilisée par les employés du GC et d'autres personnes dans le cadre du processus de passation de marcher pour les projets et initiatives du GC.

Les suggestions de modifications et autres renseignements peuvent être envoyés au principal organisme responsable de la sécurité matérielle de la GRC par courriel à l'adresse RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

Reproduction

Date d'entrée en vigueur

La date d'entrée en vigueur de GSMGC-024 (2026) – Guide de nettoyage des dessins est 2026-04-13

Registre des modifications

No de modification	Date	Par	Résumé de la modification

Remarque : C'est le POSM-GRC qui est autorisé à apporter des modifications.

Contenu

1. Introduction

La GRC, en tant principal organisme responsable de la sécurité matérielle (POSM) du gouvernement du Canada (GC) est charger de fournir des conseils et des orientations sur toutes les questions liées à la sécurité matérielle.

1.1. Objectif

Ce document a pour objectif de servir de guide pour l'expurgation des plans et documents relatifs aux bâtiments avant leur transmission à des prestataires tiers. Avant de communiquer des documents et des plans des installations à des prestataires externes, à des consultants ou au public, toutes les informations sensibles (contenu technique et lié à la sécurité) doivent être expurgé conformément aux politiques de gestion de l'information inclus dans la Politique sur la sécurité du gouvernement (PSG) et leur ministère ou organisme respectif.

Les exigences de sécurité relative à la suppression ou au masquage des contenues tels que les éléments de conception architecturale, structurelle, électrique ou mécanique, ainsi que les informations liées à la sécurité, sont décrites ci-dessous. Les principaux objectifs de cette pratique de sécurité sont les suivants :

- **Protéger les informations sensibles** – Empêcher la divulgation non autorisée d'informations susceptibles de compromettre la sûreté, la sécurité ou les intérêts commerciaux.
- **Contrôle d'accès aux informations sensibles** – Veillez à ne partager que les informations pertinentes, en fonction du rôle du destinataire et de leur besoin d'en connaître.
- **Veiller à la cohérence pour garantir la conformité** – Respecter les politiques de sécurité, les obligations légales et les clauses contractuelles en matière de sécurité du département ou de l'organisme au sein d'une Liste de vérification des exigences relatives à la sécurité (LVERS) ou accord de confidentialité.

1.2. Applicabilité

Ce guide s'adresse aux employés du GC et s'applique aux personnes chargées de la création, de la diffusion et de la modification des documents de construction et des plans des installations ainsi que, le cas échéant, de la mise à jour de ces documents.

1.3. Équité, diversité et inclusion dans les systèmes de sécurité matérielle

Tous les employés du GC ont la responsabilité de protéger les personnes, les renseignements et les biens du GC. Il est important que les politiques et les pratiques en matière de sécurité ne servent pas d'obstacles à l'inclusion, mais soutiennent et respectent plutôt tout le personnel du GC tout en veillant à ce que les mesures de sécurité appropriées soient maintenues pour protéger le personnel, les biens et l'information du GC.

Les initiatives visant à promouvoir l'égalité et l'inclusion entre les diverses communautés et patrimoines au sein du GC devraient être respectées dans le développement et la maintenance des systèmes de sécurité matérielle. Les ministères et organismes devraient respecter toutes les lois, politiques et directives du GC sur l'équité, la diversité et l'inclusion (EDI) dans la promotion d'un milieu de travail juste et équitable pour toutes les personnes, tout en s'assurant qu'elles s'acquittent de leurs responsabilités en matière de sécurité.
Les ministères et organismes devraient mener un exercice de gestion des risques pour veiller à ce que, même si la dignité de toussent est respectée, la protection des renseignements, des biens et du personnel du GC soit maintenue. Toutes les questions sur les politiques et les directives de l'EDI doivent d'abord être adressées à l'autorité ministérielle responsable.

1.4. Aspects liés aux technologies de l'information

Les aspects liés aux technologies de l'information (TI) ne sont pas toujours nécessaires lors de l'élaboration de plans de solutions de sécurité matérielle. Il existe toutefois une menace en constante évolution concernant les systèmes informatiques et, compte tenu de la convergence entre la sécurité matérielle et la sécurité informatique, il est essentiel d'évaluer les risques liés aux applications informatiques et aux logiciels connectés à un réseau qui assurent le fonctionnement et le soutien des équipements dans les bâtiments gérés par GC. Ces systèmes de contrôle peuvent notamment concerner, sans s'y limiter, l'éclairage de sécurité, les portails périphériques, les portes, les systèmes de chauffage, de ventilation et de climatisation (CVC), etc.

1.4.1. Évaluation de la sécurité et autorisation

Avant de mettre en œuvre toute application ou tout logiciel destiné à contrôler ou à automatiser certaines fonctions du bâtiment, le service de sécurité de votre département exige la réalisation d'une évaluation et d'une autorisation de sécurité (SA&A). Cela permettra de garantir le maintien de l'intégrité et de la disponibilité des composants, des applications ou des contrôles logiciels et d'assurer que tout risque identifier sera atténué. Il est fortement recommandé de lancer le processus SA&A suffisamment tôt afin de ne pas perturber le calendrier de réalisation du projet. Pour plus d'informations sur le processus SA&A, veuillez consulter le service de sécurité informatique de votre département.

1.4.2. Considérations relatives à l'informatique quantique

Les ministères et organismes du gouvernement du Canada sont chargés de gérer les risques liés à la cybersécurité dans leurs domaines de compétence, ce qui inclut les systèmes fonctionnant en conjonction avec les systèmes de sécurité matérielle. Il est important que l'ensemble du personnel du gouvernement du Canada soit conscient de la menace que représente l'informatique quantique et de l'impact qu'elle pourrait avoir sur les systèmes qu'il utilise ou dont il est responsable. Les ordinateurs quantiques utiliseront la physique quantique pour traiter des informations et résoudre des problèmes qu'il est impossible de résoudre avec les capacités informatiques actuelles.

La cryptographie, qui est l'étude des techniques utilisées pour rendre illisibles des informations en clair, puis les reconvertir dans une forme lisible, est un moyen efficace de protéger la confidentialité et l'intégrité des informations de l'administration fédérale. L'avenir de l'informatique quantique menace de rendre inefficace une grande partie de la cryptographie que nous utilisons actuellement, et des mesures doivent être prises pour protéger l'administration fédérale et la « pérenniser ». Il est recommandé aux ministères et aux organismes de faire évoluer leurs solutions de cybersécurité existantes vers l'utilisation de la cryptographie poste-quantique (PQC), qui consiste des algorithmes conçus pour être résistants à l'informatique quantique tout en pouvant être exécutés sur un ordinateur classique. Pour plus d'informations sur l'informatique quantique et la PQC, les ministères et les organismes sont invités à contacter le Centre canadien de cybersécurité (CCCS).

Afin de gérer efficacement la menace quantique, le CCCS recommande aux ministères et aux agences d'évaluer le niveau de sensibilité de leurs informations et d'en déterminer la durée de vie, afin d'identifier celles qui pourraient être exposées à un risque. Ils doivent également revoir leur plan de gestion du cycle de vie informatique et leur budget afin de prévoir les mises à jour logicielles et matérielles susceptibles d'avoir un impact significatif et sensibiliser leur personnel à la menace quantique. Pour plus d'informations, veuillez vous reporter à la directive de cybersécurité ITSE.00.017 du CCCS.

2. Coordonnées

Pour de plus amples renseignements, veuillez communiquer avec :

Gendarmerie royale du Canada
Principal organisme responsable de la sécurité matérielle
73, promenade Leikin, arrêt postal 165
Ottawa (Ontario)
K1A 0R2
Courriel: RCMP.LSA-GRC.POSM@rcmp-grc.gc.ca.

3. Acronymes

acronymes/ abréviations	Définition
AND	Accord de non-divulgation
CAO	Conception assisté par ordinateur
CTV	Circuit fermé de télévision
CVC	Chauffage, ventilation et climatisation
DGS	Directive sur la gestion de la sécurité
GC	Gouvernement du Canada
GRC POSM	GRC Principal organisme responsable de la sécurité matérielle

GSMGC	Guide sur la sécurité matérielle du gouvernement du Canada
LVERS	Liste de vérification des exigences relatives à la sécurité
MDB	Modélisation des données du bâtiment
MMS	Mur mitoyen sécuritaire
PSG	Politique sur la sécurité du gouvernement
SCT	Secrétariat du Conseil du Trésor du Canada

4. Glossaire

Terme	Définition
Installation	Lieu physique utilisé dans un but particulier. On entend par installation une partie ou la totalité d'un immeuble, soit un immeuble, son emplacement et ses alentours, ou encore une construction qui n'est pas un immeuble. Le terme désigne non seulement l'objet même, mais aussi son usage (p. ex. champs de tir, terres agricoles).
Expurgation	La modification délibérée de documents et de plans d'installations visant à supprimer les informations sensibles susceptibles de compromettre la sécurité matérielle, l'intégrité opérationnelle ou les connaissances exclusives.
Informations sensibles / Actifs	Désigne les informations ou les biens qui doivent être protégés contre toute divulgation non autorisée, car leur compromission serait raisonnablement susceptible de porter atteinte à l'intérêt national ou à des intérêts non nationaux (c'est-à-dire les informations et les biens classifiés ou protégés).

5. L'expurgation de la documentation relative aux projets de construction

Conformément à la Secrétariat du Conseil du Trésor du Canada (SCT) Directive sur la gestion de la sécurité (DGS), ministères sont tenus de protéger les informations contre la divulgation non autorisée de documents sensibles échangés entre le gouvernement du Canada et d'autres administrations (notamment étrangères, provinciales, territoriales et municipales), ainsi qu'avec des organismes internationaux, éducatives et privées. Chaque ministère à la responsabilité de classer les documents de construction et les plans des installations, selon le niveau de protection requis et de veiller à ce que ces documents soient dûment expurgé avant leur diffusion.

5.1. Préparation

Les informations contenues dans les documents de construction du projet, y compris, sans s'y limiter, la documentation technique, la correspondance relative au projet, les plans publiés, la documentation de chantier, les avis de modification, les avenants, les cahiers des chargent, les fichiers de modélisation des données du bâtiment (MDB), etc., doivent faire l'objet d'une suppression ou d'un masquage des éléments communs lors du traitement de

confidentialité. Il s'agit notamment:

- Identifiant de ministère ou d'organisme. Supprimez toute référence au ministère ou à l'organisme, y compris, mais sans s'y limiter:
    - Logos, insignes ou éléments visuels d'identité visuelle;
    - Noms des établissements, adresses des sites et signalétique; et
    - Domaines de messagerie et mentions de noms d'unités ou d'équipes.

  Remarque: les identifiants GC peuvent être utilisés.
- Noms et fonctions des pièces:
    - Les locaux sensibles (tels que les centres de données, les espaces de stockage sécurisés, les salles d'entretien et les bureaux de direction) doivent être identifiés par un numéro (salle 101, salle 202) sans mention de leur fonction;

  Remarque: Tenir à jour une liste codée des salles, distincte et soumise à un contrôle d'accès, à des fins de référence interne.
- Sécurité et données sensibles – Ne pas représenter ni identifier:
    - Zones de sécurité matérielle et niveaux de classification;
    - Locaux de stockage d'armes à feu, chambres fortes, salles des pièces à conviction, salles d'exposition; et
    - Équipements de sécurité telle que coffres-forts, boutons d'alarme, caméras ou lecteurs biométriques.
- Infrastructure du système de sécurité – Supprimer ou isoler les informations contenues dans les logiciels MDB, ainsi que les calques de conception assistée par ordinateur (CAO) qui affichent:
    - Systèmes de vidéo-surveillance (emplacement des caméras de vidéo-surveillance);
    - Systèmes de détection d'intrusion (détecteurs de mouvement, contacts de porte); et
    - Systèmes de contrôle d'accès (lecteurs de cartes, tourniquets).
- Systèmes mécaniques, électriques et de plomberie (MEP) – Supprimer les schémas détaillés susceptibles de révéler des vulnérabilités telles que:
    - Composants critiques des systèmes CVC liés à des zones sécurisées;
    - Schémas d'alimentation par générateur ou d'alimentation de secours; et
    - Points d'accès de la plomberie susceptible d'être exploités.
- Infrastructure informatique – expurgation:
    - Emplacement des salles de serveurs et tracés du câblage de données;
    - Équipements de télécommunications et schémas de standard téléphonique; et
    - Points d'accès sans fil et panneaux de brassage.

5.2. Points importants à prendre en considération

Dans certains cas, la fonction d'une pièce sera évidente, comme c'est le cas pour les toilettes, les bureaux privés ou certaines zones de sécurité. Les détails techniques sensibles liés à ces espaces doivent être omis.

Il convient de tenir compte de la sensibilité cumulative de plusieurs points de données.

Certains éléments peuvent devenir exploitables lorsqu'ils sont combinés, par exemple un emplacement sécurisé associé à une étiquette ou à une signalisation indiquant une « zone de haute sécurité ». L'identification de certaines exigences de construction, telles qu'un mur mitoyen sécuritaire (MMS), pourrait révéler la fonction de la pièce ou mettre en évidence des biens d'intérêt.

Il convient de noter que divers tiers, prestataires et sous-traitants auront besoin de différents niveaux d'informations pour mener à bien leur mission, y compris certains qui peuvent être mentionnés à la section 5.1. Un contrôle de sécurité adaptée au prestataire doit être effectué au cas par cas, en fonction du niveau d'informations et des locaux auxquels il doit avoir accès ; toutefois, tout élément non pertinent pour l'exécution de son travail doit tout de même faire l'objet de l'expurgation.

6. Gestion sécurisée de la documentation relative aux projets de construction

Toutes les informations relatives au projet, y compris, sans s'y limiter, la documentation de conception, la correspondance relative au projet, les plans publiés, la documentation de construction, les avis de modification, les avenants, les cahiers des chargent, les fichiers MDB, etc., doivent être gérées conformément aux conditions énoncées dans la liste de vérification des exigences relatives à la sécurité (LVERS) ou l'accord correspondant. L'accès aux documents de construction et aux plans des installations doivent être limitées aux personnes autorisées qui en ont besoin pour effectuer les tâches qui leur sont assignées ; c'est le principe du « besoin d'en connaître ». Consulter GSMGC-007 Transport, transmission et entreposage de matériel protégé ou classifié pour plus d'informations.

Les documents de construction et les plans des installations doivent être considérées comme des documents soumis à un contrôle d'accès, conformément aux mesures de sécurité suivante:

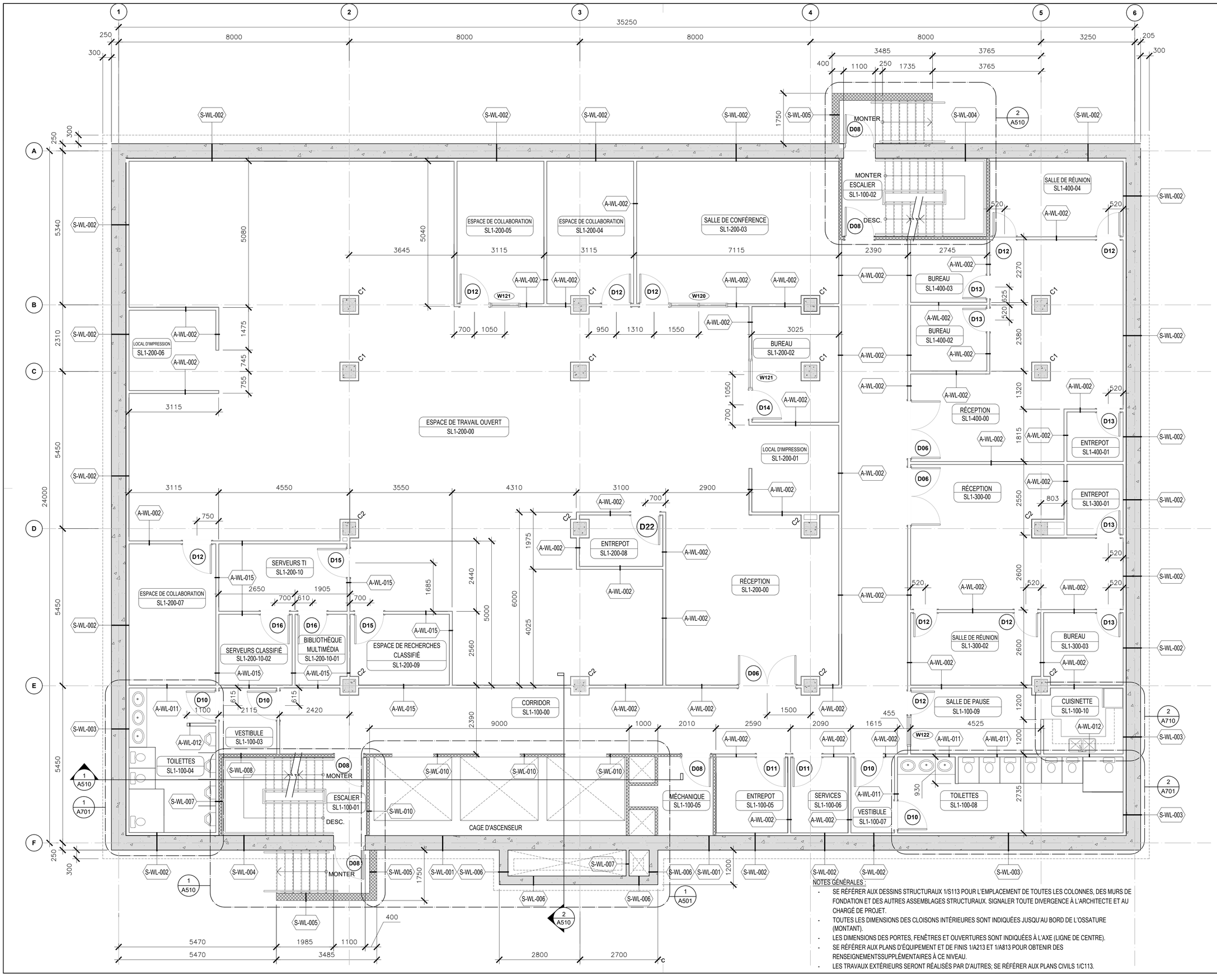
- Contrôle d'accès:
    - Limiter l'accès aux personnes autorisées qui ont besoin d'en connaître; et
    - Vérifier la classification de sécurité et le statut de sécurité ou le niveau d'habilitation, le cas échéant.
- Transmission:
    - Utilisez un système de communication numérique sécurisé (partage de fichiers) approuvé par le service; et
    - Veillez à ce que toutes les données de couches sensibles ou les méta-données soient expurgées. Ces données pourraient encore contenir, même en quantité limitée, des informations sensibles.
- Stockage:
    - Conserver et traiter les copies physiques et numériques des documents de construction et des plans des installations conformément au niveau de classification de sécurité et en accord avec GSMGC-007 Transport, transmission et entreposage de matériel protégé ou classifié; et

    - Tenir à jour les registres d'accès et de diffusion, en particulier pour les projets sensibles ou classifiés.
- Guide de référence:
    - Consultez le LVERS et le Manuel de la sécurité des contrats pour les spécifications relatives à la protection des informations sensibles relatives au projet.

7. Méthodes de nettoyage approuvées

L'expurgation des documents peut faire appel à une ou plusieurs méthodes suivantes :

- Rédaction:
    - Supprimez définitivement ou masquez les informations sensibles (par exemple, les annotations, les légendes, les références).
- Gestion des calques:
    - Supprimer les couches sensibles (par exemple, sécurité, informatique, CVC) des fichiers CAO ou MDB avant leur publication.
    - Conserver une copie maître interne avec un accès complet aux calques.
- Obscurcissement:
    - Remplacer les noms ou descriptions permettant d'identifier un lieu par des termes génériques ou des codes (par exemple, « Salle sécurisée » → " Chambre 130").
- Aplatissement des fichiers:
    - Exportez le dessin nettoyé dans un format non modifiable (par exemple, PDF ou image) afin d'empêcher toute manipulation ultérieure ou inspection des calques.
- Filigrane:
    - Apposez clairement sur les versions diffusées des mentions telles que « À usage externe – Copie expurgée » ou « Confidentiel – Ne pas diffuser ».



NOTES GÉNÉRALES :

- SE RÉFÉRER AUX DESSINS STRUCTURAUX 1/S113 POUR L'EMPLACEMENT DE TOUTES LES COLONNES, DES MURS DE FONDATION ET DES AUTRES ASSEMBLAGES STRUCTURAUX. SIGNALER TOUTE DIVERGENCE À L'ARCHITECTE ET AU CHARGÉ DE PROJET.
- TOUTES LES DIMENSIONS DES CLOISONS INTÉRIEURES SONT INDIQUÉES JUSQU'AU BORD DE L'OSSATURE (MONTANT).
- LES DIMENSIONS DES PORTES, FENÊTRES ET OUVERTURES SONT INDIQUÉES À L'AXE (LIGNE DE CENTRE).
- SE RÉFÉRER AUX PLANS D'ÉQUIPEMENT ET DE FINIS 1/A213 ET 1/A813 POUR OBTENIR DES RENSEIGNEMENTSSUPPLÉMENTAIRES À CE NIVEAU.
- LES TRAVAUX EXTÉRIEURS SERONT RÉALISÉS PAR D'AUTRES; SE RÉFÉRER AUX PLANS CIVILS 1/C113.

Canada

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

Real Property Branch / Direction générale des biens immobiliers

L'ENTREPRENEUR DOIT VÉRIFIER TOUTES LES DIMENSIONS ET LES CONDITIONS SUR LE CHANTIER ET AVISER IMMÉDIATEMENT LE REPRÉSENTANT MINISTÉRIEL DE TOUTE DIVERGENCE.

revisions	description	date
3	ÉMIS POUR CONSTRUCTION	2026-03-01
2	ÉMIS POUR APPEL D'OFFRES	2025-12-01
1	ÉMIS POUR RÉVISION	2025-10-30

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

project / projet

COMPLEXE D'AFFAIRES ROSEWOOD | AGENCE CANADIENNE DE VÉRIFICATION

175 PROM. LEIKIN, OTTAWA, ONTARIO

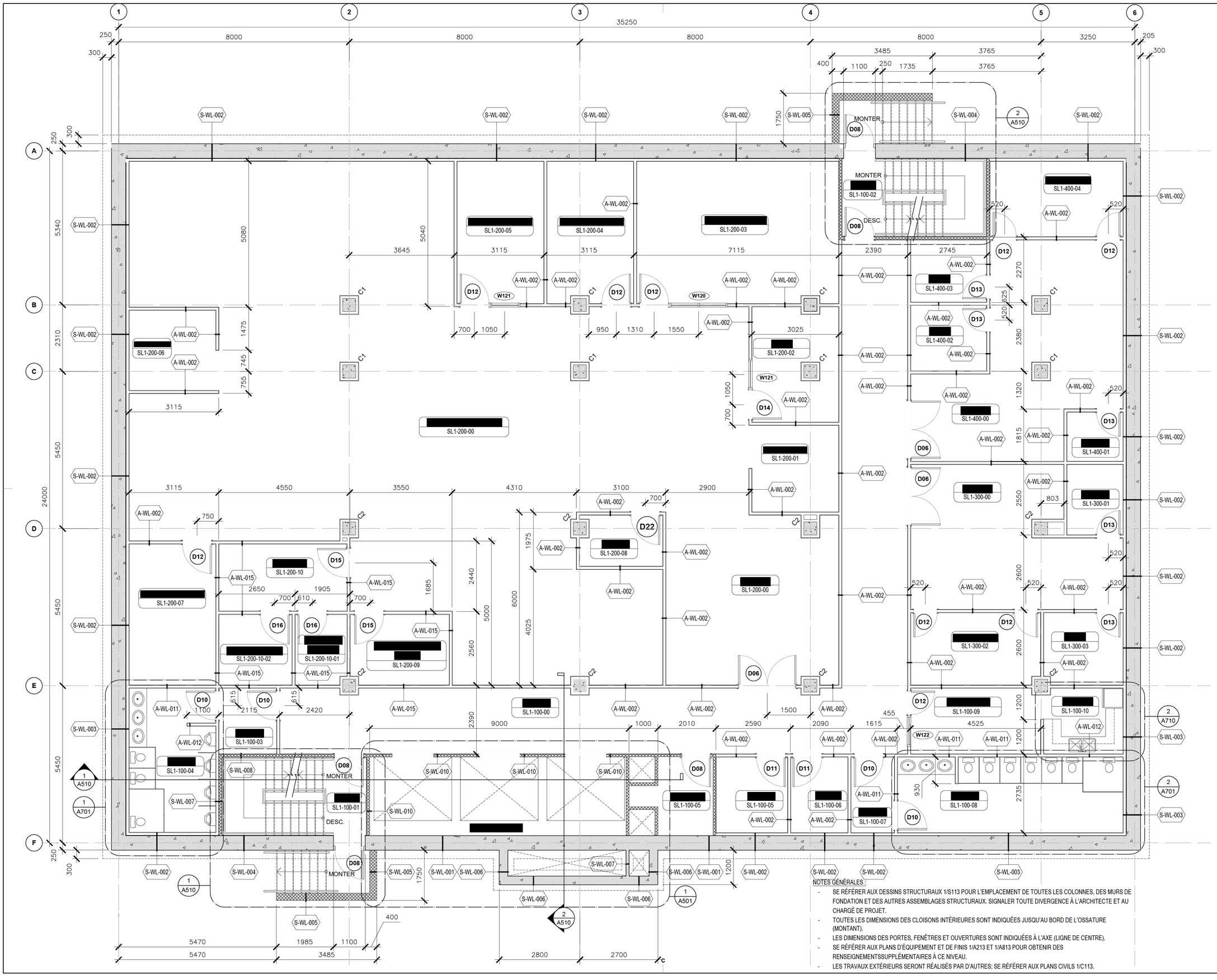
drawing / dessin

PLAN D'ÉTAGE SOUS-NIVEAU 1

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

L'ENTREPRENEUR DOIT VÉRIFIER TOUTES LES DIMENSIONS ET LES CONDITIONS SUR LE CHANTIER ET AVISER IMMÉDIATEMENT LE REPRÉSENTANT MINISTÉRIEL DE TOUTE DIVERGENCE.

revisions	description	date
3	ÉMIS POUR CONSTRUCTION	2026-03-01
2	ÉMIS POUR APPEL D'OFFRES	2025-12-01
1	ÉMIS POUR RÉVISION	2025-10-30

A detail no. no. du detail
B loca ion drawing no. sur dessin no.
C drawing no. dessin no.

project / projet

[redacted]

drawing / dessin

PLAN D'ÉTAGE SOUS-NIVEAU 1

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	[redacted]	
Project Manager / Administrateur de projets		
Project no. / No. du projet	X864951372-A	
Drawing no. / No. du dessin	A113	

8. Références et documents sources

- Politique sur la sécurité du gouvernement
- Directive sur la gestion de la sécurité
- Appel à l’action en faveur de la lutte contre le racisme, de l’équité et de l’inclusion dans la fonction publique fédérale
- Directive sur l’obligation de prendre des mesures d’adaptation
- Guide à l'intention des employés deux esprits, transgenres, non-binaires et de la pluralité des genres dans la fonction publique fédérale
- GSMGC-007 Transport, transmission et entreposage de matériel protégé ou classifié
- GSMGC-015 (2023)— Guide pour l’établissement des zones de sécurité matérielle
- Liste de vérification des exigences relatives à la sécurité (LVERS)

9. Promulgation

Examiné et recommandé aux fins d’approbation.

J’ai examiné le document GSMGC-024 (2026) – Guide de l’expurgation des documents, et j’en recommande l’approbation.

Whalen,Lucus Dwyer,000356990

Digitally signed by Whalen,Lucus Dwyer,000356990
Date: 2026.04.29 10:55:59 -04'00'

Lucus Whalen,
(I) Gestionnaire
GRC, Principal organisme responsable de la sécurité

Date

Approuvé

J’approuve par la présente le document GSMGC-024 (2026) – Guide de l’expurgation des documents.

Lafrance,Gaetan Joseph,000133993

Digitally signed by Lafrance,Gaetan Joseph,000133993
Date: 2026.04.29 11:24:38 -04'00'

Gaetan Lafrance,
(I) Directeur, Sécurité matérielle
Gendarmerie royale du Canada

Date