Appendix E-1 – Security Classification Guide

The following table outlines the personnel and facility security clearance requirements based on the expected roles and access to Canada Data.

The Contractor must contact PSPC CISD to ensure that the appropriate sub-SRCL is established for Sub-Contractors.
Screening measures must be applied in accordance with the definition and practices in the Treasury Board Standard on Security Screening (https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=28115), or use an acceptable equivalent agreed to by Canada.

NOTE:

- End user ECCS data PA Now (backend management data is PB)/ end user CCaaS data Unclassified now (back end management data is PA).
- End user ECCS and CCaaS data Protected B in the future.

Table A-1 Security Classification Guide

#	Role/Function	Expected Access	**Screening Required (ECCS) – PA Now**	**Screening Required (CCaaS)- Unclassified Now**	**Screening Required (CCaaS)- PB Future**	**Screening Required (CCaaS)- PB Future**
1	Any Contractor personnel with general duites, including facilities management resources (maintenance services, guard duties etc) that have physical access to hardware equipment at the Contractor data centers for Services and where Canada Data is stored.	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local backup media	Reliability	Reliability	Reliability	Reliability
2	Any Contractor personnel who have restricted logical access to operate, administer and configure IT systems and applications for Services in the Contractor data centers.	• Business data • Data as stored on the Contractor's compute, storage, and network components	Reliability	Reliability	Reliability	Reliability
3	Any Contractor personnel that have elevated privileges allowing unrestricted logical access to operate, administer, and configure IT systems and applications for Services in the Contractor data centers.	• Business data • Data as stored on the Contractor's compute, storage, and network components • Security data including audit logs for Contractor Infrastructure components • Sensitive data • Canada's Data	Reliability	Reliability	Secret	Secret

#	Role/Function	Expected Access	**Screening Required (ECCS) – PA Now**	**Screening Required (CCaaS)- Unclassified Now**	**Screening Required (CCaaS)- PB Future**	**Screening Required (CCaaS)- PB Future**
		• Voice and Screen Recordings				

Appendice E-1 – Guide de classification de sécurité

Le tableau suivant présente les exigences en matière d'attestation de sécurité du personnel et des installations en fonction des rôles prévus et de l'accès aux données du GC.

L'entrepreneur doit communiquer avec la DSIC de SPAC pour s'assurer que la LVERS secondaire appropriée est établie pour les sous-traitants.
Les mesures de contrôle du fournisseur doivent être appliquées conformément à la définition et aux pratiques énoncées dans la Norme sur le filtrage de sécurité du Conseil du Trésor (https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=28115), ou utiliser un équivalent accepté par le Canada.

REMARQUE :

- Les données des utilisateurs finaux des SCCE sont actuellement « Protégé A » (les données de gestion principale sont « Protégé B »); les données sur les utilisateurs finaux des CCaaS sont actuellement non classifiées (les données de gestion principale sont « Protégé A »).
- Les données des utilisateurs finaux des SCCE et des CCaaS seront « Protégé B » à l'avenir.

Tableau A-1 Guide de classification de sécurité

Nº	Rôle/fonction	Accès prévu	**Filtrage requis (SCCE), actuellement « Protégé A »**	**Filtrage requis (CCAAS), actuellement sans classification**	**Filtrage requis (CCAAS), « Protégé B » à l'avenir**	**Filtrage requis (CCAAS), « Protégé B » à l'avenir**
1	Tout employé d'un entrepreneur ayant des tâches générales, y compris les employés de gestion des installations (services d'entretien, surveillance, etc.) qui ont un accès physique à l'équipement dans les centres de données de l'entrepreneur pour les services, où des données du Canada sont stockées.	• Matériel physique • Installations de centres de données • Données stockées sur des supports de sauvegarde locaux de l'entrepreneur	Fiabilité	Fiabilité	Fiabilité	Fiabilité
2	Tout employé d'un entrepreneur qui a un accès logique restreint lui permettant d'utiliser, de gérer et de configurer des systèmes et des applications informatiques pour les services dans les centres de données de l'entrepreneur.	• Données opérationnelles • Données stockées dans les composantes de calcul, de stockage et de réseau de l'entrepreneur	Fiabilité	Fiabilité	Fiabilité	Fiabilité
3	Tout employé d'un entrepreneur qui a des privilèges supérieurs lui donnant un accès logique sans restriction lui permettant d'utiliser, de gérer et de	• Données opérationnelles • Données stockées dans les composantes de calcul, de stockage et de réseau de	Fiabilité	Fiabilité	Secret	Secret

	configurer des systèmes et des applications informatiques pour les services dans les centres de données de l'entrepreneur.	l'entrepreneur • Données de sécurité, y compris les journaux de vérification des composantes de l'infrastructure de l'entrepreneur • Données sensibles • Données du Canada • Enregistrements de voix et d'écrans				