Annex C – SRCL Classification Guide

Appendix A – Security Classification Guide

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

Table A-1 Security Classification Guide for Commercial Cloud Services

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required[1]	Responsibility	Details
1.	Any Contractor personnel with physical access to the Contractor data centers	• Physical hardware • Data Center facilities • Data as stored on the Contractor's local Backup Media	Canada	Reliability	Contractor	This is for any Contractor personnel including facilities management resources that have physical access to the Cloud Services hardware equipment at the Contractor data centers.
2.	Any Contractor personnel who have logical access to the Contractor services	• All Business Data • Data as stored on the Contractor's compute, storage, and network components	Both	Reliability	Contractor	This is for any Contractor personnel that has logical access to the GC data hosted in the Contractor data centers and any sensitive system and security incident data.
3.	Any Contractor personnel with privileged roles and unrestricted logical access to GC assets within the Contractor services	• All Business Data • GC Data as stored on the Contractor's compute, storage, and network components • Security Data including audit logs for Contractor Infrastructure components • Assets include GC data and credentials	Both	Secret	Contractor	This is for any Contractor personnel that has elevated privileges with unrestricted logical access to the GC assets hosted in the Contractor data centers and any sensitive system and security incident data.
4.	Any Contractor personnel who has temporary access to the GC Master Account information	• All Business Data • GC Data as stored on the Contractor's compute, storage, and network components • GC Master Account Information	Both	Reliability	Contractor	This is for any Contractor personnel that has access to the GC master account or root credentials for the cloud service account setup.

[1] 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.

#	Role/Function	Expected Type of Data Accessed	Data Access Location (Canada / Foreign / Both)	Screening Required[1]	Responsibility	Details
5.	Any Agent who has access to the GC billing information	• All Business Data • GC Data as stored on the Contractor's compute, storage, and network components • GC Billing Information	Both	Reliability	Contractor	This is for any Agent personnel that has access to the GC billing account information or information that facilitates GC access to cloud services.
6.	Prime Contractor*	Media	Both	Reliability	Contractor	Information that is sent from Prime Contractor to Subcontractor - needs to be encrypted.
7.	Operations Manager/Personnel *	Name, addresses, email, phone numbers and data centers	Both	Reliability	Contractor	Information that is sent from Prime Contractor to Subcontractor - needs to be encrypted.
8.	General duties	Public and reception zones	Both	N/A	Contractor	
9.	General duties*	Sensitive sites (such as operational zones where data is stored)	Both	Reliability	Contractor	*Information within site may be of sensitive nature. Individuals who are not screened must be escorted at all times. General duties include personnel providing maintenance services, security guards in the Operational Zone, etc.

*The Contractor must contact PSPC CISD to ensure that the appropriate sub-SRCL is established for Sub-Contractors.