Annex C- Appendix A – Security Classification Guide

Objective

The purpose of this document is to outline the security screening requirements to support the expected roles and access to GC data in the context of commercial cloud services.

Context

As per the expected results detailed in section 5.2.2 of Treasury Board *Standard on Security Screening*, security screening practices must provide reasonable assurance that individuals can be trusted to safeguard government information, assets and facilities, and to reliably fulfill their duties. Access to GC data requires a valid security status or clearance. As such security requirements include limiting access to authorized users only who have been security-screened at the appropriate level and have a need-to-know. These measures extend to Cloud Service Provider[1] (CSP) personnel, who by virtue of their position could:

- gain unauthorized access to GC data; or
- have the ability to adversely affect cloud-based GC services; or
- Cause reputational harm to the GC

In order to perform duties on behalf of the GC, CSPs are expected at all times to demonstrate the measures they perform to grant and maintain the required level of security screening for CSP personnel pursuant to their access privileges to protected information. In all cases, access to information, assets, facilities or information technology (IT) systems is determined and provided based on a need-to-know or need-to-access. This includes roles that have highly privileged access to information systems and services. Privileged accounts are considered to be those that have one or more of the following abilities or accesses:

- The ability to change key system configuration settings;
- The ability to change or circumvent security controls;
- Access to audit and security monitoring information;
- Logical and physical access to data, files and accounts used by other users, including backups and media; and
- Access to troubleshoot a system.

Scope

The Contractor must implement security measures that grant and maintain the required level of security screening for Contractor Personnel engaged in the provision of the Cloud Services and for Sub-processor

[1] As per the Direction on the Secure Use of Commercial Cloud Services, a Cloud Service Provider (CSP) (https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html) is defined as *"a non-federal government organization that offers cloud services to the public and/or government customers as part of a business venture, typically for a fee with the intent to make a profit."*

personnel pursuant to their access privileges to information system assets on which the Government of Canada's Data is stored and processed. In the situation where the Contractor is a SaaS provider using a GC-approved IaaS Provider that already complies with the screening requirements, the SaaS provider must provide Canada with evidence to that effect.

Table A-1 outlines the screening requirements for various roles/functions for commercial cloud services.

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[2]	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	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 computer, storage, and network components	Both	Reliability	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	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.

[2] 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[2]	Details
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	This is for any Contractor personnel that has access to the GC master account or root credentials for the cloud service account setup.
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	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	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	Information that is sent from Prime Contractor to Subcontractor - needs to be encrypted.
8.	General duties	Public and reception zones	Both	N/A	
9.	General duties*	Sensitive sites (such as operational zones where data is stored)	Both	Reliability	*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's Contract Security Program to ensure that the appropriate sub-SRCL is established for Sub-Contractors.