Interconnection Security Agreement for Cloud to Ground Connectivity Pilot Service

**Between Shared Services Canada and <Department Name>**

Version: 1.0

Date: April 15 2020

**Revision History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Date** | **Description** | **Author/Contributors** |
| 0.1 | 2019-05-23 | Incorporated TBS Document and document created by Jun Hu (SSC Contractor) | Lorne Willmott |
| 0.2 | 2019-05-31 | Reviewed feedback and incorporated into document | Lorne Willmott |
| 0.3 | 2019-06-12 | Added Additional References | Jessalynn Miller |
| 0.4 | 2019-06-28 | Incorporated Treasury Board Feedback | Jessalynn Miller |
| 0.5 | 2019-08-18 | Additional feedback from TBS | TBS Cyber |
| 0.6 | 2019-09-09 | Incorporated feedback from TBS I | TBS Cyber |
| 0.7 | 2020-02-26 | Added Roles & Responsibilities | CPMSD |
| 0.8 | 2020-02-26 | Added content from project S.C.O.P.E. document | CPMSD |
| 0.9 | 2020-03-01 | Added Network Service Levels | CPMSD |
| 1.0 | 2020-03-09 | Incorporated feedback from CBSA | CPMSD |

**Table of Contents**

[1 Purpose 4](#_Toc34730734)

[2 Background 4](#_Toc34730735)

[3 Interconnection Statement of Requirements 6](#_Toc34730736)

[4 Service Overview 7](#_Toc34730737)

[4.1 General Information 7](#_Toc34730738)

[4.2 Security Categorization of Information 7](#_Toc34730739)

[4.3 Service Components 7](#_Toc34730740)

4.4 Conceptual Architecture………………………………………………………………………9

[5 Mandatory Security Requirements 10](#_Toc34730741)

[6 Responsibilities 14](#_Toc34730742)

[6.1 Operational Roles 14](#_Toc34730743)

[6.1.1 SSC Roles 14](#_Toc34730744)

[6.1.2 Department Roles 14](#_Toc34730745)

[6.2 Data Protection 15](#_Toc34730746)

[6.3 Security Assessment and Authorization 15](#_Toc34730747)

[6.4 Personnel Security 15](#_Toc34730748)

[6.5 System Monitoring 15](#_Toc34730749)

[6.5.1 In Scope 16](#_Toc34730750)

[6.5.2 Out of Scope 17](#_Toc34730751)

[6.6 Access Control 18](#_Toc34730752)

[6.7 Changes to Secure Cloud-to-Ground Connectivity System Configuration 18](#_Toc34730753)

[6.8 Disasters and Other Contingencies 18](#_Toc34730754)

[6.9 Security Incidents 18](#_Toc34730755)

[6.10 Auditing 19](#_Toc34730756)

[6.11 Changes to Contacts 19](#_Toc34730757)

[6.12 Timeline 19](#_Toc34730758)

[7 Signatory Authorities 20](#_Toc34730759)

[8 References 21](#_Toc34730760)

[8.1 Related policy instruments 21](#_Toc34730761)

[8.2 Additional references 21](#_Toc34730762)

[9 Abbreviations and Acronyms 22](#_Toc34730763)

# Purpose

The Interconnection Security Agreement outlines the service scope of Secure Cloud-to-Ground Connectivity. Service levels and security requirements may change as a result of the clients onboarded to Architecture 2 pilot. The Interconnection Security Agreement is part of the formal Service Authorization process before the service is added to SSC’s Services Catalogue for General Availability which will require a new agreement post pilot. As part of the Agreement, clients onboarding to Architecture 2 pilot will be supported by the Enterprise Service Desk support.

This document serves to set clear expectations on the Architecture 2 pilot scope, as well as define roles and responsibilities.

# Background

In support of the Government of Canada’s (GC) Cloud First Strategy, new approaches for the delivery of digital services are increasingly reliant on secure technologies. As the reliance on digital services increases, so does the exposure to cyber threats. These threats have rapidly evolved in sophistication and disguise, resulting in the compromise of entire information technology (IT) and communications infrastructure and leading to unusable systems and loss of data and information. In turn, this has hindered, or in some cases, completely shut down operations. The GC must continue to strengthen its IT and cybersecurity posture to minimize this exposure.

The SCED project was identified by the IT Security Tripartite (ITST) — SSC, Communications Security Establishment (CSE) and Treasury Board Secretariat (TBS) – Office of the Chief Information Officer (TBS-OCIO) — to address the risk of exposure. The project will help the GC maintain its visibility of the information stored, processed and transmitted when using cloud-based services. Once implemented, the new service will support a target-state cloud architecture that provides the GC with an adaptive and resilient environment supported by CSE defensive services. The SCED project will focus on maintaining the current security posture for:

* GC assets and data that are deployed in public cloud environments: and,
* on-premise GC services and data centres, to which direct connections may be implemented to public cloud environments;
* the deployment and testing (in a pilot environment) of connectivity and hybrid security concepts required to meet the unique GC use cases while providing direct, high-speed access to Cloud Service Providers(CSP). The pilot would provide for:
  1. the establishment of cloud connectivity infrastructure at a co-location facility;
  2. the physical security infrastructure at the co-location facilities to secure workloads and infrastructure managed by the GC in the public cloud;
  3. the virtual security infrastructure within each of the CSP’s infrastructures to secure workloads and infrastructure managed by the GC in the public cloud; and
  4. the evaluation of Cloud Access Security Broker solutions that provide security policy compliance and enforcement for third-party applications hosted in cloud environments where the GC does not control the application, or the infrastructure on which it operates.

Business / Solution Objectives and Milestones

| No. | Outcome | Description |
| --- | --- | --- |
| 1 | Full security monitoring and visibility of cloud traffic between internet and cloud workloads, as well as on premise and departmental cloud instances. | The tools would be in place to perform security monitoring, through the Canadian Center for Cyber Security (CCCS), of network traffic between Internet and cloud-based workloads, between on premise and departmental cloud instances, to raise alerts when required, and provide comprehensive incident response capability and reports on activity. |
| 2 | Dedicated private connections between the GC and external networks to improve security, service availability, network performance and reliability, and access to GC services and applications when compared to using the public Internet. | Point-to-point network connections would be established between the GC-wide area network and the cloud exchange providers for accessing the cloud subscriptions of the GC departments for up to Protected B medium-medium workloads and data. This will provide network performance and reliability, and ensure monitoring and control of network traffic is in place between on premise networks to off-premise cloud environments versus routing this network traffic over the public Internet. |
| 3 | Consolidation of external access points within and across the GC to reduce the attack surface. | The consolidation of the external access points will reduce the opportunities for external entities to mount cyberattacks against cloud workloads and the GC network and make it easier to implement and manage robust controls for protecting these external access points. |
| 4 | Improvement of the GC’s ability to prevent, detect, respond and recover more rapidly to cyber threats across the entire GC enterprise with enterprise monitoring services. With this increased visibility on GC enterprise network points, situational awareness across the GC network will be improved. | The GC will have improved visibility into the network usage and traffic through improved monitoring, alerting and reporting, which will allow for better agility in responding to cyber threats and cyberattacks. |
| 5 | Improve the ability of the SSC security management teams to respond to the security and technology demands as GC departments extend services to cloud-enabled IT environments. | The tools will be in place for the CCCS security management teams to be notified and to respond to incidents that occur in the cloud or on the ground, in a timely manner. |

# Interconnection Statement of Requirements

The requirements for interconnection between SSC and **<Department Name>** are for the express purpose of establishing dedicated connections (either Ground-to-Cloud and/or Cloud-to-Internet connectivity) between the **<Department Name>**’s systems hosted at on-premise networks (Ground) and their cloud solutions (Cloud) hosted within a public cloud.

The **<Department Name>** requires the use of SSC’s Secure Cloud-to-Ground Connectivity service to establish and secure these dedicated connections with major public Cloud Service Providers (CSPs, AWS & MS Azure), as approved and directed by the executive authority of **<Department Name>** in **<*Document Name*>**, dated **<*Date*>**. Once General Availability is ready, a new agreement will need to be signed post pilot.

The Architecture 2 pilot will establish network connectivity and network access perimeters to support access to GC cloud workloads and data to help the GC maintain its visibility of the information stored, processed, and transmitted when using cloud-based services while maintaining a consistent security posture across the GC.

# Service Overview

## General Information

By entering into this agreement, SSC and **<Department Name>** will share cyber information. The client agrees to secure and protect this data, in accordance with relevant policy instruments and guidance, including

* [Policy on Service and Digital](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603)
* [Policy on Government Security](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578)
* [Directive on Security Management](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=html)
* [Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html) 2017-01
* [Implementing HTTPS for Secure Web Connections: Information Technology Policy Implementation Notice (ITPIN) 2018-01](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/policy-implementation-notices/implementing-https-secure-web-connections-itpin.html)
* [Direction for Electronic Data Residency](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-electronic-data-residency.html)
* [Government of Canada Security Control Profile for Cloud-based GC Services](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-computing/government-canada-security-control-profile-cloud-based-it-services.html)
* [GC Cloud Naming and Tagging Strategy](https://gccollab.ca/file/download/3634499)

## Security Categorization of Information

The security categorization of the Secure Cloud to Ground Connectivity service is Protected-B, Medium Integrity, and Medium Availability (PBMM). Clients requiring an Integrity and/or Availability target above Medium for their information system solutions will need to implement additional security controls on the ground and in the cloud prior to the deployment of their solutions to a Cloud Service Provider.

Both SSC and **<Department Name>** agree to provide due care and implementation of described security controls to limit unauthorised disclosure, loss of data integrity, and unavailability of data or service for information that is transmitted over the Secure Cloud to Ground Connectivity service.

## Service Components

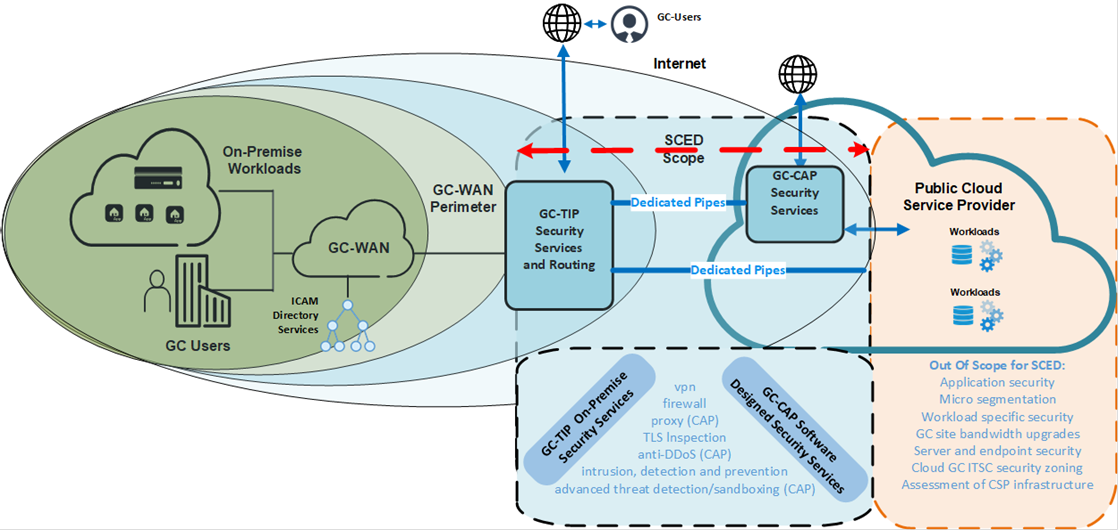
The Secure Cloud-to-Ground Connectivity service provides dedicated private connections with major CSPs. At this time, the only CSPs being offered are AWS and Microsoft Azure. This will establish physical cloud access perimeters (Government of Canada-Trust Interconnection Points (GC-TIP)) on the GC wide area network and physical cloud access perimeters (Government of Canada-Cloud Access Points (GC-CAP)) in CSP networks.

Table 1: Interconnection System Overview

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Function or Services Offered | Location | Data Description |
| GC-TIP | GC Trusted Interconnection Points [physical network perimeters on GC WAN] | Toronto & Montreal (after Sep 2020) | Departments data from/to Departments On-Premise Networks in the SSC datacenters (Ground Environments) and the Departments Cloud Networks (Cloud Environment(s)). |
| GC-CAP | GC cloud access points (GC-CAP) [cloud access perimeters to protect GC CSP networks] | CSP’s (Azure, AWS and others as they are added) or on the same physical hardware as the GC-TIP | Departments data from/to Departments Cloud Networks (Cloud Environment(s)) and the Internet. |

* 1. **Conceptual Architecture**

The following conceptual diagram depicts the deployment of the SCED perimeter components in relation to the GC network, and the services provided by the solution (as an overview).



The SCED service includes the following perimeter protective and defensive capabilities:

**Protection services**

* **Next Generation Firewall (NGFW)** - will be deployed as the “System High” first line of defence between the client cloud tenants and the internet.
* **Web Filtering** - prevents access to unacceptable/illegal Web sites and Web sites known to contain malicious threats or viruses.
* **SSL Decryption** - provides the decryption of inbound and outbound network flows to the SSC security infrastructure to protect against the use malicious code hidden in encrypted traffic flows.
* **Distributed Denial of Service (DDoS) Protection** – Anti-DDoS is a service which can be deployed in an inline DDoS protection model to mitigate anonymous attacks across network connections to the internet.  It is a subscription based service that can be integrated without additional hardware and software. This enables organizations to optimize the response to malicious events, without the investment in equipment and infrastructure as well as the reduced cost of managing and maintaining typical hardware solutions.

**Defensive services**

* **ATD Sandboxing** - will be leveraged to evaluate and determine progressive and highly sophisticated advanced threats by ‘detonating’ applicable file contents within an isolated ‘sandbox’ environment. Various Advanced Threat Detection (ATD) appliances  will be used to detect and protect against current and new threats that are not normally captured by existing security appliances.
* **Analytics** - provides integrated central logging, reporting, and security analytics from the SCED  solution to the existing SOC/SIEM within CCCS.
* **Intrusion Detection/Prevention Systems (IDPS)** - The IDPS is a new industry standard for naming IDS/IPS systems which will be used to analyze the decrypted and normal traffic for intrusion attempts and to protect the network.

The connectivity provided by the SCED service connection the GC network to the GC departments environments in the cloud will be through encrypted links from the Enterprise Data Centers and Legacy Data Centers to the Cloud Service Provider (CSP) GC departments virtual environments using commercial products that support CSE directives for PBMM security (Confidentiality, Integrity).  This connectivity will utilize redundant network links to Toronto, which allows diverse network paths in order to maintain availability in the event of a failure at any point in the connection.  SSC will also be implementing these types of connections in Montreal to provide a geographical diverse and redundant network capability for an even higher availability capability.

The SCED (and CSE) design provides a hybrid logging and monitoring solution that can enable capture of departmental logs within their tenancies by CCCS, as per [*Security Log Management Standard*](https://gcdocs.gc.ca/ssc-spc/llisapi.dll/Overview/36332578).  CCCS will capture activity, audit, diagnostic and system logs from the SCED perimeters.  Security logs will also be sent directly to CCCS. The SCED perimeter logging and monitoring solution complies with the existing MOU established between SSC and CSE as a centralized solution.

# Mandatory Security Requirements

The following outlines the mandatory security requirements for this interconnection security agreement.

| ID | Name | Ownership | | |
| --- | --- | --- | --- | --- |
| SSC | <Department Name> | *Shared* |
| 1 | SSC will design, implement, and operate the Secure Cloud to Ground Connectivity service in accordance with GC security policies and standards (e.g. Policy on Government Security, CSE’s ITSG-33, ITSG-22 and ITSG-38). | X |  |  |
| 2 | SSC will perform security assessment and authorization (SA&A) activities on the Secure Cloud to Ground Connectivity service components, including the common service components (such as GC-TIP, GC-CAP) and the baseline implementations of the Ground to Cloud connections. | X |  |  |
| 3 | SSC will provide a written authorization letter of approval to operate the Secure Cloud to Ground Connectivity service. SSC will make any security assessment results and any plan of actions and milestones (PoAM) available to Departments using the service. | X |  |  |
| 4 | The **<Department Name>** will design, implement, and operate their cloud-based environments in accordance with GC security policies and standards (e.g. Policy on Government Security, Directive on Security Management, Direction on the Secure Use of Commercial Cloud Services: Security Policy Implementation Notice (SPIN) 2017-01, CSE’s ITSG-33, ITSG-22 and ITSG-38). |  | X |  |
| 5 | The **<Department Name>** will provide to SSC a written authorization letter of approval from the **<Department Name>**’s Business Owner or Chief Security Office (CSO), to authorize the use of the SC Secure Cloud to Ground Connectivity service to transmit the Departments workloads and data up to and including Protected B between the Ground and Cloud environments, either for testing purpose or for production use.  **[Note: Please attach this letter to the email to ssc.cloud-infonuagique.spc@canada.ca with the subject line: “Interconnection Security Agreement” along with the signed ISA agreement.]** |  | X |  |
| 6 | SSC will perform security impact analysis of the **<Department Name>** specific variances to the baseline implementations of the Ground-to-Cloud connection as part of the SSC change management process. | X |  |  |
| 7 | For any deviations that introduce a high risk to the GC, the SSC and the **<Department Name>** will work together to identify and implement additional mitigations to reduce risks to the GC. Where there is no resolution, the request for change will be escalated to the appropriate governance body (e.g. GC Enterprise Architecture Review Board (GC EARB). |  |  | X |
| 8 | SSC and the **<Department Name>** will work together to:   * maintain the security of the cloud connections; * communicate any changes to either the Secure Cloud-to-Ground Connectivity service or the departmental cloud-based services that may have an impact to the Secure Cloud-to-Ground Connectivity service; and * Address the responsibilities outlined in this interconnection security agreement as specified in the Responsibilities section of this agreement. |  |  | X |
| 9 | <Department Name> submit requests to obtain a cloud account for IaaS/PaaS cloud services with a GC-approved Cloud Service Provider (CSP) via the [GC Cloud Broker](https://cloud-broker.canada.ca/). As per the Cloud PB Operationalization Framework, departments and agencies who are in-scope of the [Policy on Service and Digital](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603), must implement the enterprise-wide mandatory, minimum, initial 30-day [GC Cloud Guardrails](https://github.com/canada-ca/cloud-guardrails). |  | X |  |

# Responsibilities

The following section outlines the roles and responsibilities in support of this agreement.

## Operational Roles

As the Secure Cloud-to-Ground Connectivity service provider, SSC is responsible for security of the dedicated private connections with CSPs that have been established to support the secure transmission of Departments data.

### SSC Roles

SSC is responsible and accountable for the following:

* Project Management of the onboarding client to the GC TIP & GC CAP
* Technical Requirements
* High Level Architecture Design and Detailed Design
* PPIA – Preliminary Privacy Impact Assessment (for decryption of traffic)
* Provide support for the SA&A ATO (Authority to Operate) for the Secure Cloud-to-Ground Connectivity environment
* Configuration of GC-TIP and GC-CAP to meet requirements of network flows to be supported
* Connectivity and Integration
* Support of End-to-End Secure Cloud-to-Ground Connectivity Service Functional Testing
* Security Monitoring of the Secure Cloud-to-Ground Connectivity service
* Pilot Assessment
* Provide end-to-end encryption

### Department Roles

The Departments are responsible for implementing appropriate safeguards, such as application level encryption, to protect data that transits over the cloud-to-ground connection.

Each stakeholder is responsible and accountable for the Secure Cloud-to-Ground Connectivity including the following:

* Requirements Definition and Validation
* Provision and Validation of Use Cases
* End-to-End Connectivity Testing
* Security Monitoring of the Tenant/Account
* SA&A (ATO) for environment
* Provisions for Operational Readiness
* Configuration information required for integration with the GC CAP
* Application encryption

Each GC department will be responsible for their own virtual datacentres and networks solutions to host departmental workloads and connect back to their legacy networks via the GC TIP. SSC is providing Cloud Identity Services which are being delivered primarily via the Digital Communication Access Management (DCAM).

## Data Protection

The Department is responsible for determining the security category of the information transiting through the Secure Cloud-to-Ground Connectivity system. The Department must not allow data above PBMM to transit through the Secure Cloud-to-Ground Connectivity system without implementing appropriate compensating measures.

The Department is responsible for encrypting sensitive data while in transit between ground and cloud environments in accordance with approved cryptographic standards.

## Security Assessment and Authorization

SSC is responsible for the initial and on-going security assessment and authorization activities related to the Secure Cloud-to-Ground Connectivity system.

The Department is responsible for the initial and on-going security assessment and authorization activities related to the cloud and ground information systems making use of the interconnection.

Immediately upon identification, both parties must inform the other in writing of any non-compliance to the security requirements specified under this agreement.

## Personnel Security

SSC must ensure that the personnel accessing the Secure Cloud-to-Ground Connectivity system for operational and maintenance purposes hold a valid security screening at the appropriate level (Secret).

## System Monitoring

SSC is responsible for monitoring and responding to events related to the Secure Cloud-to-Ground Connectivity system. 24/7/365 support and will follow Enterprise Service Management processes Availability: *Enterprise services: 24/7/365, XX.XX of the time.*

The Department is responsible for monitoring and responding to events related to the ground and cloud information systems making use of the interconnection.

### In Scope

The pilot will build on the Direct Connect connectivity implemented to AWS or Express Route implemented to Azure. It will deliver the required architecture, operational processes, governance, and policies to achieve accreditation for up to Protected B Med-Med workloads.

The pilot will leverage existing GC network and security services where available and implement new controls as required to deliver a GC hybrid cloud target architecture. SSC will provide network perimeter security services for up to Protected B data consumption of public cloud services, and to secure the ground-to-cloud network connectivity to the GC network.

The following table depicts the list of SCED Security Services that will be enabled for the period of the Pilot. These services may evolve based on lessons learned during the Pilot & Evaluation Phase.

| Service Elements of Network Connectivity | **Description** | **Operating Capability** |
| --- | --- | --- |
| Routing | Service responsible for routing traffic in and out of the GC-TIP instance. | Yes |
| Boundary protection | Service responsible for enforcing the flow of network traffic. | Yes |
| Intrusion detection and prevention | Service responsible for detecting malicious activity in the network traffic, and either preventing attacks or initiating incident response. | Yes |
| LIAS High-Speed Internet | GC Local Internet Access Service (10Gbps); terminated within the CXP Collocation environment, and fully managed by SSC | Yes |
| Distributed Denial Of Service protection (Network Based DDoS) | Service responsible for detecting denial of service attacks at the inbound interface of the GC-CAP, and either preventing the attack or initiating incident response. This upstream protection service will be provisioned to the dedicated Internet connection. | Yes |
| Malware protection | Service responsible for the detection of and response to malware in the network traffic. This includes behaviour-based analysis such as sandboxing. | Yes |
| Access Control | Control access to authorized applications and services. | No |
| Proxy Service (Web filtering) | URL filtering of Web destined traffic. Accept, processes and forwards certain types of traffic entering or leaving a network. | Yes |
| Private Connectivity Encryption | Standard Network-based Encryption service where required to provide private connectivity to Cloud from on premise infrastructure or colocation facility. | Yes |

### Out of Scope

The project has identified several activities to be out of scope. However, many of these activities are worth mentioning in the context of hybrid-cloud. In some cases, dependencies exist on these activities for the implementation of the Secure Cloud-to-Ground Connectivity solution.

The following activities are out-of-scope for this project:

* cloud internet protocol address management and development of an IP address scheme strategy;
* SSC Foundational Services such as DNS, SMTP and DHCP;
* upgrades to Partner legacy network (WAN or Internet) connections are not funded by the pilot and will have to fall into the client’s budget;
* development of a client systems management strategy;
* development of CSP policy management and enforcement;
* the project team is not involved in the development of the client application;
* implementation of security controls within the Partner Department’s Tenant / Account and legacy environment;
* identity, credential and access management (ICAM) to provide access control and authorization for cloud-based services;
* setup of the federated identity management for management of user credentials for access to cloud-based services and systems
* tenancy subscription policies.

## Access Control

SSC is responsible for managing access to the Secure Cloud-to-Ground Connectivity interconnection services and all supporting information systems. This includes the management of user and service accounts and related identifiers and authenticators.

The Department must submit requests for access to the Secure Cloud-to-Ground Connectivity interconnection services to SSC via their Service Delivery Manager.

The Department must review access requirements and inform SSC in writing promptly of any change and when access by a user or a service is no longer required.

The Department is responsible for managing access to the ground and cloud information systems that make use of the interconnection and related identifiers and authenticators.

## Changes to Secure Cloud-to-Ground Connectivity System Configuration

SSC must inform the Department prior to implementing any configuration change that may impact the Department's use of the interconnection and potentially other Department’s use.

SSC must work with the Department to minimize the impact on Department operations.

## Disasters and Other Contingencies

SSC must immediately inform the Department by telephone or e-mail in the event of a disaster or other contingency that disrupts the normal operation of the Secure Cloud-to-Ground Connectivity services as per the enterprise service management process.

SSC must provide periodic updates of the status of the recovery activities until the disaster or the contingency is fully resolved.

## Security Incidents

SSC must report to the Department security incidents related to the Secure Cloud-to-Ground Connectivity services in accordance with the reporting requirements of the [GC Cyber Security Event Management Plan (GC CSEMP)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html).

The Department must report security incidents related to their ground and cloud environments making use of the Secure Cloud-to-Ground Connectivity services in accordance with the reporting requirements of the [GC CSEMP](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html).

Both parties must provide periodic updates of the status of incident response activities until the security incident is fully resolved as per the Cyber Center Memorandum of Understanding (MOU).

## Auditing

SSC must retain Secure Cloud-to-Ground Connectivity audit records for the prescribed period. SSC must protect the confidentiality and integrity of Secure Cloud-to-Ground Connectivity audit records while in transit and at rest.

SSC is responsible to conduct audit reviews related to the Secure Cloud-to-Ground Connectivity services for the prescribed events at the prescribed frequency.

The Department is responsible for the audit function related to the ground and cloud information systems making use of the interconnection.

## Changes to Contacts

Both parties must notify the other party of any changes the contacts specified in Section 8 of this agreement.

## Timeline

This Interconnection Security Agreement (ISA) will remain in effect so long as the service is required. SSC will have a process in place for yearly reviews to validate requirements and update the agreement and any conditions as needed. If changes are required, the agreement will be updated and new signatures will be obtained. The newly signed agreement should explicitly supersede this agreement, which should be referenced by title and date. If one or both of the parties wish to terminate this agreement prematurely, they may do so upon 30 days advance notice or in the event of a security incident that necessitates an immediate response.

# Signatory Authorities

This interconnection security agreement is valid after the last date of signature. At that time, it will be updated, reviewed, and reauthorized or terminated. Either party may also terminate this agreement upon a 30-day advanced notice in writing.

This interconnection security agreement has been reviewed and approved by the Client.

**Department Name:**

|  |  |  |
| --- | --- | --- |
|  |  |  |
| **<*Name*>, Director General** |  | Date |
|  |  |  |
| **<*Name*>, Assistant Deputy Minister** |  | Date |

The Interconnection Security Agreement must be completed, signed, and returned to ssc.cloud-infonuagique.spc@canada.ca with the subject line: “Interconnection Security Agreement”.

# References

## Related policy instruments

* [Policy on Government Security](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578)
* [Policy on Service and Digital](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32603)
* [Directive on Security Management](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32611&section=html)
* [Direction for Electronic Data Residency](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-electronic-data-residency.html)
* [Direction on the Secure Use of Commercial Cloud Services: Security Implementation Notice (SPIN)](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/direction-secure-use-commercial-cloud-services-spin.html) No. 2017-01

## Additional references

* [Government of Canada Security Control Profile for Cloud-based GC Services](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-security-control-profile-cloud-based-it-services.html)
* [Government of Canada Cloud Security Risk Management Approach and Procedures](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/cloud-security-risk-management-approach-procedures.html)
* [Security categorization guide and tool](http://www.gcpedia.gc.ca/gcwiki/images/6/66/Tool-Security_Categorization.zip)
* [Government of Canada Cyber Security Event Management Plan (GC CSEMP) 2018](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/government-canada-cyber-security-event-management-plan.html)
* [Considerations for Cryptography in Commercial Cloud Services](http://www.gcpedia.gc.ca/gcwiki/images/2/25/Considerations_for_Use_of_Cryptography_in_Cloud.pdf)
* [IT Security Risk Management: A Lifecycle Approach (ITSG‑33)](https://cyber.gc.ca/en/guidance/it-security-risk-management-lifecycle-approach-itsg-33)
* [Guidance on Securely Configuring Network Protocols (ITSP.40.062)](https://cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062)
* Cloud Service Provider Information Technology Security Assessment Process (ITSM.50.062)
* [Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22)
* [Network Security Zoning: Design Considerations for Placement of Services within Zones (ITSG-38)](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38)
* [CSE Top 10 Security Action](https://www.cse-cst.gc.ca/en/top10)

# Abbreviations and Acronyms

Table 2: Abbreviations and Acronyms

| Abbreviation/Acronym | Description |
| --- | --- |
| ATO | Authority to Operate |
| CCCS | Canadian Centre for Cyber Security |
| CSEMP | Cyber Security Event Management Plan |
| CSP | Cloud Service Provider |
| DSM | Directive on Security Management |
| CSO | Chief Security Officer |
| GC | Government of Canada |
| GC-CAP | Government of Canada – Cloud Access Perimeters |
| GC-TIP | Government of Canada – Trusted Interconnection Points |
| ITSG | Information Technology Security Guidance |
| MOA | Memorandum of Agreement |
| PGS | Policy on Government Security |
| PoAM | Plan of Action and Milestones |
| SA&A | Security Assessment and Authorization |
| SCED | Secure Cloud Enablement and Defence |
| SPIN | Security Policy Implementation Notice |
| SSC | Shared Services Canada |
| TBS | Treasury Board of Canada Secretariat |