# Cloud Guardrails

This document focuses on a **preliminary set of baseline security controls** to ensure that the cloud service environment has a minimum set of configurations for the cloud environment. Departments are expected to must implement, validate, and report on in the first 30 business days.

Departments are responsible for implementing the minimum configurations identified in the table below. Validation of the guardrails will be performed by SSC Cloud Services Directorate. The [Standard Operating Procedure (SOP) on Validating Cloud Guardrails](https://www.gcpedia.gc.ca/gcwiki/images/1/19/SOP_for_Validating_Cloud_Guardrails.pdf) has been developed to support this activity.

For this document the following definitions will be used:

* Mandatory requirements: A set of baseline security controls that departments must implement, validate, and report on in the first 30 business days.
* Additional considerations: Additional security controls that are highly recommended and should be taken into consideration. While these are not expected to be implemented within 30 business days, they include best practices that should be considered as departments progress with the establishment of their cloud-based environments.

## Guardrail #1 – Protect user accounts and identities

|  |  |
| --- | --- |
| **Objective:**  Protect user accounts and identities. | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Implement strong multi-factor authentication (MFA) for all user accounts. Use phishing resistant MFA where and when available.   *(Note: User accounts and identities include:*   1. *Root/Global administrator (as it is one that that has enhanced/highest level of privileges over the control plane and addresses all aspects of access control).* 2. *Other Administrative user accounts. Refer to Section 4 of the “*[*Directive on Service and Digital- Canada.ca*](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601)*,* [*Appendix G: Standard on Enterprise Information Technology Service Common Configurations- Canada.ca*](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32713) *-* [*Account Management Configuration Requirements - Canada.ca*](https://www.canada.ca/en/government/system/digital-government/policies-standards/enterprise-it-service-common-configurations/account.html)*”* *for the definition of privileged accounts.* 3. *Regular user accounts)* | * Confirm that MFA is implemented as per GC guidance through screenshots, compliance reports, or compliance check enabled through a reporting tool for all user accounts. * Confirm that digital policies are in place to ensure that MFA configurations are enforced. * Confirm and report the count of Root/Global administrator registered (should have at least two and no more than five). |
| * Configure alerting to ensure the prompt detection of a potential compromise, in accordance with the GC Event Logging Guidance. | * Confirm if monitoring and auditing is implemented for all user accounts. * Confirm alert notification to the authorized personnel is implemented for flagging misuse, suspicious activities , for all user accounts. |
| * Use separate dedicated accounts for highly privileged roles (e.g. domain admins, global admins, root, and any domain admin equivalent access) when administering cloud services to minimize the blast radius. | * Provide evidence that dedicated user accounts are used for administration (e.g., privileged access). |
| **Additional Considerations** | |
| **None** | |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.3 2. CSE Top 10 #3 3. Refer to the [Recommendations for Two-Factor User Authentication Within the Government of Canada Enterprise Domain](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp) 4. Refer to the [GC Multi-Factor Authentication (MFA) Strategy Paper](https://www.gcpedia.gc.ca/gcwiki/images/9/9e/GC_MFA_Strategy.pdf) 5. Refer to the [Directive on Service and Digital](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601), [Appendix G: Standard on Enterprise Information Technology Service Common Configurations](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32713) - [Account Management Configuration Requirements](https://www.canada.ca/en/government/system/digital-government/policies-standards/enterprise-it-service-common-configurations/account.html) 6. Refer to the [GC Event Logging Guidance](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf) 7. Refer to [ITSP.50.104 Guidance on defence in depth for cloud-based services,](https://cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services) subsection 4.6 8. [User authentication guidance for information technology systems (ITSP.30.031 v3)](https://www.cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) | |
| **Related security controls:** AC-2, AC-2(11), AC-3, AC-5, AC-6, AC- 6(5), AC- 6(10), AC-19, AC – 20 (3), IA-2, IA-2(1)  IA - 2(2), IA-2(3), IA – 2(11), IA-5(8), SI-4, SI-4(5), SA-4(12), CM-5. | |

## Guardrail #2 – Manage access

|  |  |
| --- | --- |
| **Objective:**  Establish access control policies and procedures for management of all accounts. | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Implement a mechanism for enforcing access authorizations for all user accounts, based on criteria listed in Directive on Service and Digital Appendix G – Account Management Configuration Requirements – Section 3. | * Demonstrate access configurations and policies are implemented for different classes of users (non-privileged, and privileged users). * Confirm that the access authorization mechanisms have been implemented for the following:  1. To uniquely identify and authenticate users to the cloud service; 2. Validating that the least privilege role is assigned; 3. Validating that Role Based Access is implemented; 4. Terminating of role assignment upon job change or termination; 5. Performing periodic reviews of role assignment (minimum yearly); 6. Disabling default and dormant accounts; 7. Avoiding use of user generic accounts.  * Verify that a review of Root/Global administrator accounts role assignment is performed at a minimum every 12 months. |
| * Leverage role-based access that are configured with least privileges. This can include built-in roles or custom roles that have been established with only the minimum number of privileges required to perform the job function. | * Demonstrate that cloud platform built-in roles are used with least privileges. Custom roles can be used but rationale should be documented and approved. |
| * Change default passwords in accordance with the GC password guidance. | * Confirm that the default passwords have been changed for all the built-in accounts for the cloud-service. |
| * Configure the default password policy in accordance with [GC Password Guidance](https://www.canada.ca/en/government/system/digital-government/online-security-privacy/password-guidance.html). | * Demonstrate that password policy for the cloud platform has been configured as per the GC Password Guidance:   1. Require longer passwords – At least 12 characters in length without a maximum length limit;   2. Counter online guessing or brute forcing of passwords using throttling, account lockout policies, monitoring, and multi-factor authentication;   3. Protect against offline attacks using effecting hashing, salting, and keyed hashing. |
| * Implement password protection mechanisms to protect against password brute force attacks. | * Confirm that mechanisms, such as throttling, account lock out policies, monitoring and risk based authentication, to protect against password bruteforce attacks have been implemented |
| * Establish a guest user access policy and procedures that minimizes the number of guest users and manages their lifecycle where accounts are deprovisioned when access is no longer needed.   (Note: A guest is someone who isn't an employee, student, or member of your organization. They don't have an existing account with the organization’s cloud tenant). | * Confirm only the required guest user accounts are enabled (The required guest user accounts are as per the business requirements of the service) * Provide list of non-organizational users with elevated privileges. * Verify that periodic guest access reviews are performed periodically. |
| **Additional Considerations** | |
| * Document a process for managing accounts, access privileges, and access credentials for organizational users, non-organizational users (if required), based on criteria listed in Directive on Service and Digital Appendix G – Account Management Configuration Requirements – Section 3. This process should be approved by Chief Security Officer (CSO) (or delegate) and designated official for cyber security. | * Confirm that the Access Control procedure for management of administrative accounts have been documented for the cloud service. The procedure should include provision for any guest accounts, custom accounts, and must reference to the Emergency Break Glass procedure. |
| * Enforce just-in-time access for privileged user accounts to provide time-based and approval-based role activation to mitigate the risks of excessive, unnecessary, or misused access permissions. | * Confirm that just-in-time access for all privileged user accounts to provide time-based and approval-based role activation. |
| * Enforce attribute-based access control (ABAC) to restrict access based on combination of authentication factors (MFA), , GC issued and managed devices, device compliance, sign-in and user risks, and location. | * Provide evidence that attribute-based access control (ABAC) mechanisms are in place to restrict access based on attributes/signals such as authentication factors (MFA), GC issued and managed devices, device compliance, sign-in and user risks, and location. |
| * Leverage tools such as privilege access management systems to enforce access control to privilege functions by configuring roles that requires approval for activation and choose one or multiple users or groups as delegated approvers. | * Provide evidence that all privileged user accounts role activation requires approval, and that privilege elevation is time-bound (temporary activation). |
|  |  |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.3 2. CSE Top 10 #3 3. Refer to [User authentication guidance for information technology systems (ITSP.30.031 v3)](https://www.cyber.gc.ca/en/guidance/user-authentication-guidance-information-technology-systems-itsp30031-v3) 4. Refer to the [Guidance on Cloud Authentication for the Government of Canada](https://intranet.canada.ca/wg-tg/cagc-angc-eng.asp) 5. Refer to the [Recommendations for Two-Factor User Authentication Within the Government of Canada Enterprise Domain](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp) 6. Refer to the [Directive on Service and Digital](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601), [Appendix G: Standard on Enterprise Information Technology Service Common Configurations](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32713) - [Account Management Configuration Requirements](https://www.canada.ca/en/government/system/digital-government/policies-standards/enterprise-it-service-common-configurations/account.html) 7. Refer to [ITSP.50.104 Guidance on defence in depth for cloud-based services,](https://cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services) subsection 4.6 8. [GC Password Guidance](https://www.canada.ca/en/government/system/digital-government/online-security-privacy/password-guidance.html) | |
| **Related security controls:** AC‑2, AC‑2(1), AC‑2(7) AC‑3, AC‑3(7), AC‑3, AC‑4 AC‑5, AC‑6, AC‑6(5), IA‑2, IA‑2(1), IA‑2(8), IA‑2(11), IA‑4, IA‑5, IA‑5(1), IA‑5(6) | |

## Guardrail #3 – Secure endpoints

|  |  |
| --- | --- |
| **Objective:** Implement increased levels of protection for management interfaces. | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Implement access restrictions to ensure the use GC issued and managed devices that are patched and managed, in accordance with [GC Endpoint Management Configuration Requirements](https://www.canada.ca/en/government/system/digital-government/policies-standards/enterprise-it-service-common-configurations/endpoint.html). | * Confirm that administrative access to cloud environments is from approved and trusted locations and GC issued and managed devices that enforce the GC endpoint management configuration requirements. * Demonstrate access configurations and policies are implemented for devices. |
| **Additional Considerations** | |
| * All administrative tasks should be undertaken on dedicated administrative workstations.   (Note: A dedicated administrative workstation is a secured physical (thick or thin) client workstation used to perform specific and sensitive administrative tasks or tasks requiring privileged access. This device must have no Internet access and services such as email and web browsing must be disabled and prohibited) | * Confirm if dedicated administrative workstations are utilized to conduct all administrative activities |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.3 2. CSE Top 10 #2 3. Refer to the [Recommendations for Two-Factor User Authentication Within the Government of Canada Enterprise Domain](https://intranet.canada.ca/wg-tg/rtua-rafu-eng.asp) 4. Refer to the [Directive on Service and Digital](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601), [Appendix G: Standard on Enterprise Information Technology Service Common Configurations](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32713) - [Endpoint Management Configuration Requirements](https://www.canada.ca/en/government/system/digital-government/policies-standards/enterprise-it-service-common-configurations/endpoint.html) 5. Refer to [ITSP.50.104 Guidance on defence in depth for cloud-based services,](https://cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services) subsection 4.9. | |
| **Related security controls**: AC3, AC-3(7), AC-4, AC5, AC6, AC6(5), AC6(10), AC19, AC20(3), IA2, IA2(1),IA2(11), IA4, IA5, IA5(1), SI-4, AU-6, AU-12 | |

## Guardrail #4 – Enterprise monitoring accounts

|  |  |
| --- | --- |
| **Objective:** Create role-based account to enable enterprise monitoring and visibility | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| Create role-based account to enable enterprise monitoring and visibility for cloud environments that are procured via the GC Cloud Broker or are included in scope of centralized guardrails validation. | * Verify that roles required to enable GC visibility to have been provisioned/assigned. |
| * Review access privileges periodically and remove access when it is no longer required. | * Confirm alert notification to the authorized personnel is implemented flagging misuse, suspicious sign-in attempts, or when changes are made to the privileged and non-privileged accounts. |
| **Additional Considerations** | |
| **None** | |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.3 2. CSE Top 10 #2 | |
| **Related security controls**: AC-3(7), AC-6(5), IA-2(1) | |

## Guardrail #5 – Data location

|  |  |
| --- | --- |
| **Objective:** Establish policies to restrict GC sensitive workloads to approved geographic locations | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * As per Section 4.4.3.14 of the Directive on Service and Digital, “Ensuring computing facilities located within the geographic boundaries of Canada or within the premises of a Government of Canada department located abroad, such as a diplomatic or consular mission, be identified and evaluated as a principal delivery option for all sensitive electronic information and data under government control that has been categorized as Protected B, Protected C or is Classified.” | * Demonstrate that service location is within Canada (For all PB cloud-services) where configurable , in accordance with the applicable cloud usage profiles. |
| **Additional Considerations** | |
| **None** | |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.3 2. Refer to [Directive on Service and Digita](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601)l, subsection 4.4.3.14 | |
| **Related security controls**: SA-9(5) | |

## Guardrail #6 – Protection of data-at-rest

|  |  |
| --- | --- |
| **Objective:** Protect data at rest by default (e.g., storage) for cloud-based workloads | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Implement an encryption mechanism to protect the confidentiality and integrity of data when data are at rest in your solution's storage. | * For IaaS and PaaS, confirm that storage service encryption is enabled for data at rest (if required based on the security risk assessment). * For SaaS, confirm that the CSP has implemented encryption to protect customer data. |
| * Use CSE-approved cryptographic algorithms and protocols, in accordance with ITSP.40.111 and ITSP.40.062. | * Cryptographic algorithms and protocols configurable by the consumer are leveraged in accordance with ITSP 40.111 and 40.062. * For SaaS, confirm that the CSP has implemented algorithms that align with ITSP 40.111 and 40.062. |
| **Additional Considerations** | |
| * Seek guidance from privacy and access to information officials within institutions before storing personal information in cloud-based environments. | * Confirm that privacy is included as part of the Departmental SDLC process. |
| * Leverage an appropriate key management system for the cryptographic protection used in cloud-based services, in accordance with GC Considerations for the Use of Cryptography in Commercial Cloud Services and CCCS guidance on key management at Guidance on cloud [service](https://www.cyber.gc.ca/en/guidance/guidance-cloud-service-cryptography-itsp50106) cryptography (ITSP.50.106). | * Confirm that a key management strategy has been adopted for the cloud tenant. |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.4 2. Refer to the cryptography guidance in [ITSP.40.111](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111) and [ITSP.40.062](https://www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062). 3. Refer to the guidance in Guidance on cloud [service](https://www.cyber.gc.ca/en/guidance/guidance-cloud-service-cryptography-itsp50106) cryptography (ITSP.50.106) 4. Refer to [ITSP.50.104 Guidance on defence in depth for cloud-based services,](https://cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services) subsection 4.5. | |
| **Related security controls:** IA-7, SC-12, SC-13, SC-28, SC-28(1) | |

## Guardrail #7 – Protection of data-in-transit

|  |  |
| --- | --- |
| **Objective:** Protect data transiting networks through the use of appropriate encryption and network safeguards | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Encrypt data in transit by default (e.g., TLS v1.2, etc.) to protect the confidentiality and integrity of data, including for all publicly accessible sites and external communications as per the GC Website and Services Configuration Requirements, and wherever possible for internal zone communication. | * Confirm that TLS v1.2 or above encryption is implemented for all cloud services (via HTTPS, TLS or other mechanism).   *(Note: While this is often the default, cloud platforms and cloud services often have configuration options to select the permitted TLS version.)* |
| * Use CSE-approved cryptographic algorithms and protocols, in accordance with ITSP.40.111 and ITSP.40.062. | * Cryptographic algorithms and protocols configurable by the consumer are leveraged in accordance with ITSP 40.111 and 40.062. |
| * Leverage non-person entity certificates from certificate authorities that align with the Recommendations for TLS Server Certificates. | * Confirm that NPE certificates are issued from certificate authorities that align with GC recommendations for TLS server certificates. |
| **Additional Considerations** | |
| **None** | |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.4 2. Refer to the [Directive on Service and Digital](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601), [Appendix G: Standard on Enterprise Information Technology Service Common Configurations](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32713) – [Web Sites and Services Management Configuration Requirements](https://www.canada.ca/en/government/system/digital-government/policies-standards/enterprise-it-service-common-configurations/web-sites.html) 3. Refer to the cryptography guidance in [ITSP.40.111](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111) and [ITSP.40.062](https://www.cyber.gc.ca/en/guidance/guidance-securely-configuring-network-protocols-itsp40062) 4. Refer to the network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38) 5. Refer to the guidance in Guidance on cloud [service](https://www.cyber.gc.ca/en/guidance/guidance-cloud-service-cryptography-itsp50106) cryptography (ITSP.50.106) 6. [Government of Canada Recommendations for TLS Server Certificates for GC Public Facing Web Services](https://wiki.gccollab.ca/images/9/92/Recommendations_for_TLS_Server_Certificates_-_14_May_2021.pdf) 7. Refer to [ITSP.50.104 Guidance on defence in depth for cloud-based services](https://cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services), subsection 4.5 | |
| **Related security controls:** IA-7,SC-12, SC-13, SC-28, SC-28(1) | |

## Guardrail #8 – Segment and separate

|  |  |
| --- | --- |
| **Objective:** Segment and separate information based on sensitivity of information | |
| **Applicable Service Models:** IaaS, PaaS  *(Note: The following guardrail is not applicable for SaaS model. Management and security of the network is a Cloud Service Provider responsibility and is included as part of the SaaS offering. Please refer to* [*ITSP.50.104 Guidance on defence in depth for cloud-based services*](https://www.cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services) *Section 4.3 to understand key considerations for cloud network segmentation)* | |
| **Mandatory Requirements** | **Validation** |
| * Isolate and secure cloud workloads based on the sensitivity of the data. | * Confirm that department has a target network architecture high level design and / or diagram with appropriate segmentation between network security zones in alignment with CSE’s ITSP.50.104, ITSG-22 and ITSG-38. * Confirm that the department has documented a deployment guide of the cloud platform and associated services. (The document is to capture landing zone if applicable) * Confirm that CSP segmentation features are leveraged to provide segmentation of Management, Prod, UAT, DEV, and test. (For example, use of subscription, instances, or other cloud provider construct). |
| **Additional Considerations** | |
| * Develop a target network security design that considers segmentation via network security zones, in alignment with ITSP.50.104, ITSG-22 and ITSG-38. | * Leverage landing zones that include pre-defined, secured, multi-account support to allow different workloads and teams to be onboarded in an automated manner. |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.4 2. CSE Top 10 #5 3. Refer to the network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38) 4. Refer to [ITSP.50.104 Guidance on defence in depth for cloud-based services](https://cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services), subsections 4.3, 4.5 | |
| **Related security controls:** AC‑4, SC‑7 | |

## Guardrail #9 – Network security services

|  |  |
| --- | --- |
| **Objective:** Establish external and internal network perimeters and monitor network traffic. | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Ensure that egress/ingress points to and from GC cloud-based environments are managed and monitored. | * Confirm policy for limiting number of public IPs. |
| * Implement network boundary protection mechanisms for all external facing interfaces that enforce a deny-all or allow-by-exception policy. | * Confirm policy for network boundary protection. |
| * Perimeter security services such as boundary protection, intrusion prevention services, proxy services, TLS traffic inspection, etc. must be enabled based on risk profile, in alignment with GC Secure Connectivity Requirements and CSE guidance. | * Confirm policy for limiting to authorized source IP addresses (e.g., GC IP addresses). |
| * Ensure that access to cloud storage services is protected and restricted to authorized security zones/network, users, and services. | * Confirm that storage accounts are not exposed to the public. |
| **Additional Considerations** | |
| * Use centrally provisioned network security services where available. | * Confirm if the department is intending to establish dedicated and secure connections to on-premise resources. |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.4 2. CSE Top 10 #1 3. Refer to the network security zoning guidance in [ITSG-22](https://cyber.gc.ca/en/guidance/baseline-security-requirements-network-security-zones-government-canada-itsg-22) and [ITSG-38](https://cyber.gc.ca/en/guidance/network-security-zoning-design-considerations-placement-services-within-zones-itsg-38) 4. Refer to [ITSP.50.104 Guidance on defence in depth for cloud-based services](https://cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services), subsection 4.3 | |
| **Related security controls:** AC-3, AC‑4, SC‑7, SC‑7(5), SI-4, SI-4(18) | |

## Guardrail #10 – Cyber defense services

|  |  |
| --- | --- |
| **Objective:** Establish MOU for defensive services and threat monitoring protection services. | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Sign an MOU with Canadian Centre for Cyber Security (CCCS). *(*[*CDOServiceDeployments@cyber.gc.ca*](mailto:CDOServiceDeployments@cyber.gc.ca)*.)* | * Confirmation from CCCS that the MOU has been signed by the Department. |
| * Implement defensive services including HBS, CBS, and NBS in accordance with CCCS onboarding guidance where available. | * Confirm that the sensors or other cyber defense services by CCCS are implemented where available. |
| **Additional Considerations** | |
| **None** | |
| **References**   1. [SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.3 | |
| **Related security controls:** SI‑4 | |

## Guardrail #11 – Logging and monitoring

|  |  |
| --- | --- |
| **Objective:** Enable logging for the cloud environment and for cloud-based workloads. | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Implement adequate level of logging and reporting, including a security audit log function in all information systems. | * Confirm policy for event logging is implemented. * This includes logs for the following:   1. Sign-in logs (interactive and non-interactive sign-ins, API sign-ins)   2. Access privilege and group changes (including group membership and group privilege assignment)   3. Changes in configuration of cloud platform   4. Cloud resource provisioning activities. |
| * Configure events within the solution to support security monitoring, in accordance with GC Event Logging Guidance. | * Confirm if monitoring and auditing is implemented for all users. |
| * Ensure that the appropriate contact information is configured so that the CSP can notify the GC organization of incidents they detect. | * Confirm that the security contact record within the account should be completed with details of at least two (if multiple permitted by cloud platform) appropriate information security personnel. |
| * Configure an appropriate time zone for the audit records generated by your solution components. | * Confirm that the appropriate time zone has been set. |
| * Ensure that resources are assigned to monitor cloud-based events. | * Demonstrate that the monitoring use cases for the cloud platform have been implemented and have been integrated with the overall security monitoring activities being performed by the department. Evidence could include monitoring run book/checklist, system generated report. |
| **Additional Considerations** | |
| None | |
| **References**   1. [[SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html)](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.3.1 2. CSE Top 10 #1, 5, 8 3. Refer to [GC Event Logging Guidance](https://www.gcpedia.gc.ca/gcwiki/images/e/e3/GC_Event_Logging_Strategy.pdf) 4. Refer to [ITSP.50.104 Guidance on defence in depth for cloud-based services,](https://cyber.gc.ca/en/guidance/itsp50104-guidance-defence-depth-cloud-based-services) subsection 4.8 | |
| **Related security controls:** AU‑12, SI-4, SI-4(7) | |

## Guardrail #12 – Configuration of cloud marketplaces

|  |  |
| --- | --- |
| **Objective:** Restrict Third-Party CSP Marketplace software to GC-approved products. | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Only GC approved cloud marketplace products are to be consumed. Turning on the commercial marketplace is prohibited. | * Confirm that third-party marketplace restrictions have been implemented. |
| **Additional Considerations** | |
| * Submit requests to add third-party products to marketplace to SSC Cloud Broker. |  |
| * Ensure that software offered through the CSPs or CSP marketplace undergo a software assurance process to ensure that only approved products are consumed. |  |
| **References**   1. [SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), subsection 6.2.5 | |
| **Related security controls:** CM‑5, CM‑8, SA‑12 | |

## Guardrail #13 – Plan for continuity

|  |  |
| --- | --- |
| **Objective:** Ensure that there is a plan for continuity of access and service that accommodates both expected and unexpected events. | |
| **Applicable Service Models:** IaaS, PaaS, SaaS | |
| **Mandatory Requirements** | **Validation** |
| * Document, implement, and test a break glass emergency account management process. | * Verify that a break glass emergency account management procedure has been developed. * Verify that alerting is in place to report any use of break glass accounts. * Verify that testing of break glass account took place, and that periodic testing is included in break glass emergency account management procedure. |
| * Obtain signature from Departmental Chief Information Officer (CIO) in collaboration with designated official for cyber security (DOCS) to confirm acknowledgement and approval of the break glass emergency account management procedures. | * Confirm through attestation that the Departmental Chief Information Officer (CIO) in collaboration with DOCS have approved the break glass emergency account management procedure for the cloud service. |
| **Additional Considerations** | |
| * Develop a cloud backup strategy that takes into account where GC data is stored, replicated, or backed up by the cloud service, in consideration of the IT continuity plan for the service/application. | * Confirm through attestation that the cloud backup strategy procedure is developed and approved by the business owner. * Verify if there are scripts that support the ability to restore from code (e.g., infrastructure as code). |
| * Ensure that cloud workloads are associated with the applicable Application ID in the TBS Application Portfolio Management (APM) tool, in support of the Standard on At-Risk Technology. | * Provide a list of all software, including versions, deployed on VMs associated with the application IDs from APM. |
| * Ensure departmental cyber security event management plans include cloud services, in alignment with the GC Cyber Security Event Management Plan. | * Provide a list of all software, including versions, deployed on VMs associated with the application IDs from APM. |
| **References**   1. [SPIN 2017-01](https://www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/security-identity-management/direction-secure-use-commercial-cloud-services-spin.html), [sub-section 6.2.9](https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-secure-use-commercial-cloud-services-spin.html#toc6-2-9) 2. Refer to the [template](https://gcconnex.gc.ca/file/view/55010566/break-glass-emergency-account-procedure-departments-can-use-to-develop-their-emergency-access-management-controls-for-cloud?language=en) for a break glass emergency account management procedure. 3. Refer to the [Department Cyber Security Event Management Plan (CSEMP) Template](https://www.gcpedia.gc.ca/gcwiki/images/6/66/Department_CSEMP_Template.docx). 4. [Directive on Service and Digital- Canada.ca](https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32601) | |
| **Related security controls:** AC-1, CP-1,CP-2,CP-9,CA-3 | |