## 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. | |