# Management of Administrative Privileges

## Objective

Establish access control policies and procedures for management of administrative privileges.

## Key Considerations

* [ ] Document a process for managing accounts, access privileges, and access credentials for organizational users, non-organizational users (if required), and processes based on the principles of separation of duties and least privilege (for example, operational procedures and active directory).
* [ ] Implement a mechanism for enforcing access authorizations.
* [ ] Implement a mechanism for uniquely identifying and authenticating organizational users, non-organizational users (if applicable), and processes (for example, username and password).
* [ ] Implement a multi-factor authentication mechanism for privileged accounts (for example, username, password and one-time password) and for external facing interfaces.
* [ ] Change default passwords.
* [ ] Ensure that no custom subscription owner roles are created.
* [ ] Configure password policy in accordance with [GC Password Guidance](https://www.canada.ca/en/government/system/digital-government/password-guidance.html).
* [ ] Minimize number of guest users; add only if needed.
* [ ] Determine access restrictions and configuration requirements for GC-issued endpoint devices, including those of non-privileged and privileged users, and configure access restrictions for endpoint devices accordingly. **Note:** Some service providers may offer configuration options to restrict endpoint device access. Alternatively, organizational policy and procedural instruments can be implemented to restrict access.

## Validation

* [ ] Confirm policy for MFA is enabled through screenshots and compliance reports.
* [ ] Confirm that a privileged account management plan and process has been documented.
* [ ] Confirm password policy aligns with [GC Password Guidance](https://www.canada.ca/en/government/system/digital-government/password-guidance.html) as appropriate.

## Additional Considerations

* [ ] Leverage enterprise services such as Administrative Access Control System (AACS) for Privileged Access Management (PAM), Attribute-based access control (ABAC).

## Applicable Service Models

* IaaS, PaaS, SaaS

## 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 6.2.3
2. CSE Top 10 #3
3. Refer to [CCCS ITSP.30.031 V2 User Authentication Guidance for Information Technology Systems](https://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. Related security controls: AC‑2, AC‑2(1), AC‑3, AC‑5, AC‑6, AC‑6(5), AC‑6(10), AC‑7, AC‑9, AC‑19, AC‑20(3), IA‑2, IA‑2(1), IA‑2(2), IA‑2(11), IA‑4, IA‑5, IA‑5(1), IA‑5(6), IA‑5(7), IA‑5(13), IA‑6, IA‑8