# Protection of Data-at-Rest

## Objective

Protect data at rest by default (e.g. storage) for cloud-based workloads.

## Key Considerations

* [ ] Seek guidance from privacy and access to information officials within institutions before storing personal information in cloud-based environments.
* [ ] Implement an encryption mechanism to protect the confidentiality and integrity of data when data are at rest in your solution's storage.
* [ ] Use CSE-approved cryptographic algorithms and protocols, in accordance with [40.111](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111) and [40.062](https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.062-eng.pdf).
* [ ] Implement key management procedures.

## Validation

* [ ] Confirm policy for encryption (e.g. storage and/or VM based on risk-based assessment).

## 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 6.2.4
2. Refer to the cryptography guidance in [40.111](https://cyber.gc.ca/en/guidance/cryptographic-algorithms-unclassified-protected-and-protected-b-information-itsp40111) and [40.062](https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsp.40.062-eng.pdf).
3. Refer to the guidance in [Considerations for Cryptography in Commercial Cloud Services](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/cloud-services/government-canada-consideration-use-cryptography-in-cloud.html).
4. Related security controls: SC‑12, SC‑13, SC‑17, SC‑28, SC‑28(1)