# Protection of Data-in-Transit

## Objective

Protect data transiting networks through the use of appropriate encryption and network safeguards.

## Key Considerations

* [ ] Implement an encryption mechanism to protect the confidentiality and integrity of data when data are in transit to and from your solution.
* [ ] Use CSE-approved cryptographic algorithms and protocols.
* [ ] Encryption of data in transit by default (e.g. TLS v1.2, etc.) for all publicly accessible sites and external communications as per the direction on [Implementing HTTPS for Secure Web Connections](https://www.canada.ca/en/government/system/digital-government/modern-emerging-technologies/policy-implementation-notices/implementing-https-secure-web-connections-itpin.html) (ITPIN 2018-01).
* [ ] Encryption for all access to cloud services (e.g. Cloud storage, Key Management systems, etc.).
* [ ] Consider encryption for internal zone communication in the cloud based on risk profile and as per the direction in CCCS 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)
* [ ] Implement key management procedures.

## Validation

* [ ] Confirm policy for secure network transmission.

## 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. [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)
3. 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).
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 [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).
6. Related security controls: SC‑8, SC‑8(1), SC‑12, SC‑13, SC‑17