Data and Information Security in the Cloud

Corporate Information Security Office

Office of the Corporate Chief Information Officer & Telecommunications,

Service Alberta

Version: 1.1

Approved by: Deputy Minister Council	**Owner:** Service Alberta, Office of the Corporate CIO & Telecommunication, Corporate Information Security Office
Approval date: May 12, 2020	**Review date:** January 30, 2021
Contact: GoA IMT Policy Program at imt.policy@gov.ab.ca	**Policy Instrument type:** Standard

Contents

Standard Statement

The Data and Information Security in the Cloud standard defines the security controls that must be implemented, maintained, and leveraged to secure Government of Alberta (GoA) data and information assets stored in the Cloud.

> Note: This standard does not imply that any information or data of any particular security classification (public, protected A, B, or C) must or should be stored in the cloud. The standard is simply to be applied once a decision has been reached to store a particular data collection or system in the cloud.

Authority

For internal GoA use only.

Scope

This standard applies to all GoA data and information assets considered for storage or migration to the Cloud.

Standard Description

This security standard ensures that appropriate controls are implemented, maintained, and leveraged to protect GoA data and information assets stored in the Cloud, according to the assets' sensitivity as defined by their assigned data and information Security Classification.

The standard aligns with the GoA Information Technology Security Framework, which supports the Government of Alberta's Information Security Management Directives (ISMDs).

Standard Specification

1. All data and information assets created in, migrated to, or more generally, stored in the Cloud must be classified as per the GoA Data and Information Security Classification standard and guidelines before migration or creation in the Cloud.
2. Security controls implemented for data and information assets created in, migrated to, or more generally, stored in the Cloud must meet or exceed GoA security controls set out in GoA's ISMDs and GoA Security Standards.
3. Legislative and regulatory requirements specific to Ministries or Departments must be taken into account and complied with in addition to the controls listed in this standard. In cases where legislation/regulations conflict with this standard, the legislation/ regulations must take precedence, unless a specific exception request was granted by the Deputy Head who has authority over the specific data collection.
4. Any Information Management Technology (IMT) activity resulting in the migration of GoA Protected (A, B, and/or C) data and information to the Cloud must perform a risk assessment that conforms to the Corporate Information Security Office (CISO) IMT Risk Management processes prior to migration to the cloud.
    - 4.1. Identified and assessed residual risks must be documented in the GoA IMT Risk Register.
    - 4.2. Mitigating controls (technical, procedural, or contractual) must be documented as part of the assessment.

5. Data and information classified as Public can be stored in the Cloud without particular restrictions; however, the Information Controller may have additional integrity and availability requirements that must be considered before implementation.

6. Protected data and information assets created in, migrated to, or more generally, stored in the Cloud must be encrypted while in transit to and from the Cloud-hosted environment.

7. Protected (A, B, and/or C) data and information assets created in, migrated to, or more generally, stored in the Cloud must be secured while at rest in the Cloud.

    7.1. The most secure and appropriate security controls available from the service provider should be used, as per Appendix A: Security Controls for Data and Information at Rest in the Cloud, in accordance with the assigned data and information security classification.

8. In order to ensure adequate controls regarding access to GoA assets, Cloud-hosted services for Protected data and information must be designed to ensure that the GoA effectively controls the provisioning and revocation of credentials used to access the service.

    8.1. The GoA must always maintain administrative access to the data.

9. Cloud Service providers must be given express contractual consent from the assigned GoA Information Controller to conduct any analytics on data with a Protected classification. This applies to any use or analysis of the data beyond the stated purpose of the provisioned software or service.

10. Sensitive GoA data and information assets with a requirement to be excluded from this standard due to elevated security risks associated with the assets must receive formal exception from this standard through the GoA IMT Standard Exception process managed by the IMT Policy and Standards team.

    10.1. The request must be reviewed and approved by the Deputy Head of the Department responsible for the associated data collection.

    10.2. After approval from the Deputy Head, the request must be reviewed and acknowledged (through formal sign off) by the GoA's Corporate Chief Information Officer.

Definitions

- Cloud: A network of remote servers hosted on the Internet and used to store, manage, and process data in place of organization-based servers or personal computers.
- GoA Information Security Management Directives: The GoA's 10 basic security directives that all GoA systems hosting, processing, or managing GoA data and information assets must comply with.
- GoA Information Technology Security Framework: The set of artefacts describing the information management technology security environment and controls for the GoA, including service and program strategies, plans, policies, standards, procedures and templates.

- Analytics / Data Analytics: The science of analyzing raw data with a goal to make it become usable and actionable information resulting in better informed decisions.

Roles and Responsibilities

Deputy Heads will:

- Identify Information Controllers for data collections under their authority.
- Review and approve Standards Exception requests for highly sensitive GoA data and information assets with a requirement to be excluded from this standard due to elevated security risks associated with the assets.

Corporate Chief Information Officer will:

- Facilitate the review and approval of any changes to this standard through the Deputy Minister Council.
- Review and acknowledge exception requests for this standard as submitted by Deputy Heads.

Information Controllers will:

- Review and approve recommendations, risk assessments, and risk assessment results regarding all data and information assets they have been assigned.

Chief Information Security Officer will:

- Monitor compliance to the standard and escalate any non-compliance or significant issues to the Corporate Chief Information Officer.

IMT employees (including contracted resources) will:

- Apply this standard to any recommendations involving storage of GoA data and information assets in the Cloud.

GoA Employees will:

- Keep informed of current GoA IMT standards affecting their functions.

Compliance

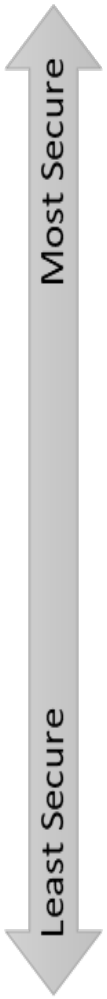
- Consequences of non-compliance with this policy could result in damage to Government of Alberta's reputation, expose Albertans to harm and/or incur unnecessary costs.
- Any exception to this standard must be documented and approved through the IMT Standard Exception process managed by the IMT Policy and Standards team, and any resulting risks must be assessed and documented using the IMT Risk Management processes managed by the CISO.

References and Supporting Resources

- GoA Data and Information Security Classification standard
- Freedom of Information and Protection of Privacy Act (FOIP)

- Alberta Health Information Act
- Records Management Regulation
- National Institute of Standards and Technology (NIST)
- The Personal Information Protection and Electronic Documents Act (PIPEDA)

APPENDIX A: Security Controls for Data at Rest in the Cloud



Storage Location and Security Controls	Appropriate for: Public	Prot. A	Prot. B	Prot. C	Residual Risk
Data Residency: Canada Authentication Service: Multi-factor Authentication Encryption Method: Complies with GoA Standard Encryption Key Control: GoA	√	√	√	√	Negligible
Data Residency: Outside of Canada Authentication Service: Multi-factor Authentication Encryption Method: Complies with GoA Standard Encryption Key Control: GoA	√	√	√	√	Very Low
Data Residency: Canada Authentication Service: Multi-factor Authentication Encryption Method: Complies with GoA Standard Encryption Key Control: Cloud Service Provider	√	√	√	√	Very Low
Data Residency: Outside of Canada Authentication Service: Multi-factor Authentication Encryption Method: Complies with GoA Standard Encryption Key Control: Cloud Service Provider	√	√	√	√	Low
Data Residency: Canada Authentication Service: Username/Password Encryption Method: Complies with GoA Standard Encryption Key Control: Cloud Service Provider	√	√			Low
Data Residency: Outside of Canada Authentication Service: Username/Password Encryption Method: Complies with GoA Standard Encryption Key Control: Cloud Service Provider	√	√			Low
Data Residency: Anywhere in the world Authentication Service: No specific requirements Encryption Method: No encryption Encryption Key Control: No encryption	√				Very Low

LEGEND:

√ : Signifies that the Storage Location and Security Controls stated on this row is acceptable for the level of Information Security Classification represented in this column.