Data and Information Security Classification Standard

FOIP and Information Management, Enterprise Information Management

Version: 3.1

Approved by: Maureen Towle, Executive Director, Enterprise Information Management, Service Alberta	**Owner:** Enterprise Information Management	
Approval Date: March 2017	**Last Reviewed:** September 2020	**Review Date:** August 2021
Contact: Sa.InformationManagement@gov.ab.ca	**Policy Instrument type:** Standard	

Contents

Standard Statement
The appropriate application of security classification is the first step in ensuring the integrity, availability, sensitivity and/or value of data and information.

Authority
- *Government Organization Act*
- Records Management Regulation

Scope
This standard applies to all departments defined under section 14 of Schedule 11 of the *Government Organization Act* and agencies, boards and commissions as defined in schedule 1 of the Freedom of Information and Protection of Privacy Regulation.

Agencies, boards and commissions that are not contained within schedule 1 of the Freedom of Information and Protection of Privacy Regulation are encouraged to align with this standard.

Departments requiring an exception must contact Enterprise Information Management to discuss the exceptions process.

Standard Description
This standard describes the four security classification levels from which departments must select when applying data and security classification. This standard aligns with the data and information security classification levels established by the Government of Canada, and supports data and information sharing across jurisdictions.

Standard Specification
This standard describes the four data and information security classification levels that will be used to classify all data and information that are received, created, held by or retained on behalf of the Government of Alberta.

Information Security Classification Levels

Level	Description
PUBLIC	Applies to data and information that, if compromised, will not result in injury to individuals, governments or to private sector institutions.
PROTECTED A	Applies to data and information that, if compromised, could cause injury to an individual, organization or government.
PROTECTED B	Applies to data and information that, if compromised, could cause serious injury to an individual, organization or government.
PROTECTED C	Applies to data and information that, if compromised, could cause extremely grave injury to an individual, organization or government.

Roles and Responsibilities

Please see the Data and Information Security Classification Guide for details on roles and responsibilities.

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. Depending on the severity of non-compliance:

- either informal or formal requests and/or follow-ups may be made by Enterprise Information Management, Corporate Internal Audit Services, Corporate Information Security Office, Office of the Information Privacy Commissioner, and/or Public Service Commission; and
- legislated disciplinary action (i.e., Public Service Act) may be taken.

References and Supporting Resources

- Data and Information Security Classification Guide
- Technical Guide: Appropriate Access to Data and Information
- Technical Guide: Labeling Data and Information
- Technical Guide: Storing Data and Information
- Technical Guide: Transmitting Data and Information