Information Security Classification Standard

Corporate Information and Records Management Office
Ministry of Citizens' Services

Effective: July 17, 2018

1. Purpose

Provide a common standard for security classification of government information (as defined under the *Information Management Act*).

2. Description

This standard describes four levels of security classification to be applied to government information based on the degree of harm that could reasonably be expected to result from unauthorized disclosure.

The Information Security Classification Guideline provides additional direction on how to apply this standard and examples of protective measures to apply at each classification level.

3. Application

All ministries, agencies, boards and commissions that are subject to the Core Policy and Procedures Manual.

4. Information Security Classification Levels

	Level	Description
	Public	No harm to an individual, organization or government **Examples:** Job postings, communications to claim clerks, business contact information, research and background papers (without copyright restrictions)
Confidential	**Protected A**	Harm to an individual, organization or government **Examples:** Home addresses, dates of birth, other low-risk personal information
	Protected B	Serious harm to an individual, organization or government **Examples:** Law enforcement and medical records, personnel evaluations and investigations, financial records, information subject to solicitor-client privilege or other legal privilege
	Protected C	Extremely grave harm to an individual, organization or government **Examples:** Information about police agents and other informants, Cabinet records or Cabinet-related records

5. Authority

Core Policy and Procedures Manual

6. Supporting Documents

Information Security Classification Guideline

7. Contact

IM.ITPolicy@gov.bc.ca