Information Security Classification Standard

Office of the Chief Information Officer
Ministry of Citizens' Services

Effective: Oct. 31, 2023

1. Purpose

Provide a common standard for security classification of government information (as defined in Chapter 12 of the Core Policy and Procedures Manual).

2. Description

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

3. Application

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

4. When to Apply this Standard

Ministries may use this Standard to:

a. determine the appropriate access management and security controls to apply to different categories of government information);
b. determine appropriate physical and electronic storage requirements; or
c. facilitate information sharing with other Canadian jurisdictions.

NOTE: Security classification should be determined by examining both the content of the information and the context in which the information exists.

5. Information Security Classification Levels

	Level	Description
	Public	No harm to an individual, organization or government
Confidential	**Protected A**	Harm to an individual, organization or government
	Protected B	Serious harm to an individual, organization or government
	Protected C	Extremely grave harm to an individual, organization or government

6. Authority

Core Policy and Procedures Manual

7. Supporting Documents

Chapter 12 of the Core Policy and Procedures Manual
Information Security policy

8. Contact

For questions about the Standard IM.ITPolicy@gov.bc.ca
For information about how to apply the Standard contact your Ministry Information Security Officer