Data and Information Security Classification Standard Guide

Office of the Corporate Chief Information Officer, Enterprise Information Management

Version: 1.0

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:** Guideline	

Contents

Guide Statement

This guide outlines the standardized approach for the application of security classification to data and information in the custody and/or under the control of the Government of Alberta (GoA). The approach detailed in this guide supports implementation of the Data and Information Security Classification Standard and aligns with the data and information security classification levels established by the Government of Canada.

Authority

The Data and Information Security Classification Standard (A000025) and supporting guide are issued under the authority of the Records Management Regulation:

> 4(2) For the purpose of providing the details for the operation of the records management program, the Minister may establish, maintain and promote policies, standards and procedures for the creation, handling, control, organization, retention, maintenance, security, preservation, disposition, alienation and destruction of records in the custody or under the control of departments and for their transfer to the Provincial Archives of Alberta.

Scope

This guide is recommended for 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 guide.

Guide Description

Security classification supports decision making regarding how data and information should be managed (e.g., storage, access permissions, etc.). In accordance with the Data and Information Security Classification Standard and the Metadata – Core Content Standard, data and information security classification is mandatory and must be applied to all data and information in the custody and/or under the control of the GoA.

Guide Specification

Security classification is determined by examining both the content of the data and information and the context in which the data and information exists. The application of security classification to data and information is a process that requires a thorough assessment of the potential for injury to individuals, governments and/or private sector institutions in the event the integrity, availability, sensitivity and/or value of the data and information is compromised.

Because the selection and application of security classification is informed by context, security classification is not static; a change in the appropriate security classification could be triggered by a reassessment of data and information (either due to prescribed review periods or as data and information moves through the information management lifecycle). Ultimately, business areas will need to establish internal processes and guidelines to enable the consistent implementation and review of security classifications.

Regardless of security classification level, data and information that are, or are reasonably anticipated to be, subject to litigation holds and/or access requests made under the *Freedom of*

Information and Protection of Privacy Act must be provided to the relevant litigation hold contact or department Freedom of Information and Protection of Privacy (FOIP) Office for evaluation.

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.

NOTE: Classifying data or information as **Public** does not require that it be made available to the public. Business areas determine if data and information will be published after considering the impact and value of publication.

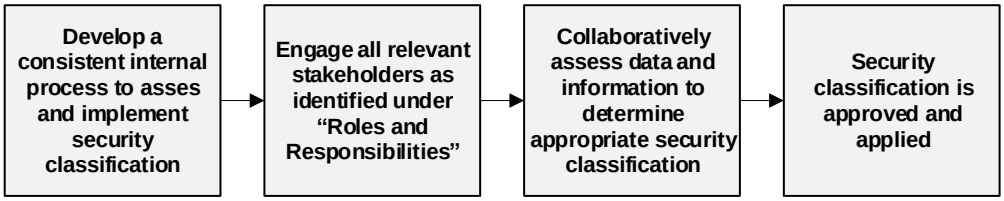
Data or information that have already been classified using levels from the now-superseded Information Security Classification Standard may need to be updated; however, the security classification selected under the superseded standard may no longer accurately reflect the context in which the data or information exists.

The following chart offers a basic comparison of the levels in the superseded standard and the levels in the current standard, but business areas must assess all data and information to ensure that the appropriate current security classifications are applied:

SUPERSEDED	CURRENT
UNRESTRICTED	PUBLIC
PROTECTED	PROTECTED A
CONFIDENTIAL	PROTECTED B
RESTRICTED	PROTECTED C

Assessing Data and Information

It is the responsibility of business areas to develop a consistent internal process to assess and implement security classification. The visual below outlines key steps that must be included in the process.



Determining security classification requires an assessment of the potential risks for individuals, governments and/or private sector institutions in the event the integrity, availability, sensitivity or value of the data or information is compromised; the more severe the risk (or the more severe the consequences of a risk), the stronger the classification. This assessment of potential risks must consider:

- the context in which data and information exists, including (but not limited to):
  - regulatory requirements;
  - the information management lifecycle stage of the data and information; and
  - factors external to government (e.g., elections, fiscal cycle, public emergencies, etc.).
- the likelihood that potential injuries may occur; and
- all potential injuries that could result from data and information being compromised.

Potential injuries can include (but are not limited to):

- loss of privacy;
- breach of confidentiality;
- loss of business continuity/interruption of GoA services;
- loss of data and information integrity;
- loss of information value;
- financial impacts;
- personal injury;
- loss of life;
- harm to business relationships; and
- damage to GoA reputation.

As data or information moves through the information management lifecycle, or as the context in which it exists changes, the applied security classification may need to be re-assessed. For example, due to sensitive financial and political implications, draft versions of the provincial budget typically have a higher security classification (e.g., **Protected B** or **Protected C**); however, the finalized provincial budget that is made available to Albertans has the security classification **Public**.

Assessing data and information for the purposes of security classification involves extensive collaboration between multiple stakeholders, each of whom contributes important knowledge about the context in which data and information exists.

Security Classification Assessment Scenarios

NOTE: The scenarios below are only intended to outline the dynamic nature of security classification; as such, **these scenarios are not prescriptive** and do not elaborate on particulars (i.e., the complete context in which the data and information exists) or the manner in which security classification is applied (i.e., to a system and application, record, or specific field).

Scenario 1 – Request for Proposal

An initial Request for Proposal (RFP) may be classified as **Public**. As information is appended to an RFP, the applied classification may change to **Protected A**, **Protected B**, or **Protected C**:

- The addition of blueprints/schematics (e.g., assembly diagrams for equipment) and/or third-party financial information could result in a **Protected A** classification.

- The addition of unpublished, proprietary, or personally identifying information could result in a **Protected B** classification.
- The potential financial and/or reputational harm that could result from accidental disclosure of evaluation scoring notes means that their addition to an RFP could also result in a classification of **Protected B**.
- The addition of information that could undermine the security of the GoA (e.g., IT information regarding security systems), information that could influence political events, or sensitive/high-ranking opinions that could have grave reputational repercussions for the GoA could result in a **Protected C** classification.

Barring the inclusion of any information that would result in an elevated classification, fulfilled/completed RFPs may be classified as **Public**.

Scenario 2 – Policy Development
As a policy moves through development, from initial conceptualization to final published form, the applied security classification will change:

- An initial draft of a policy could be **Protected A**, **Protected B** or **Protected C**, depending on the context of the policy or its intended use.
- Stakeholder consultations for a draft policy may be **Public** (if there is a public consultation), **Protected A** (if there is an internal government consultation), or **Protected B** (if there is a confidential consultation with external stakeholders).
- Analysis of potential policy options based on stakeholder consultation may be **Protected A** or **Protected B**, and Cabinet deliberations may be **Protected B** or **Protected C**.
- Published policy and accompanying guidance will have the security classification of **Public**, but policy interpretations may have the security classification of **Protected A** or **Protected B**.

Applying Security Classification

Consultation and collaboration with relevant stakeholders will result in the selection of an appropriate security classification. After the security classification has been decided, it may be applied to:

- the system and/or application in which the data or information is maintained;
- an individual record; or
- a field within a system and/or application.

NOTE: At a minimum, security classification must be applied to a system and/or application.

Systems and Applications
Systems and applications are electronic platforms that perform various functions, such as enhancing productivity, maintaining records, and providing collaborative working environments. Examples may include (but are not limited to):

- collaborative electronic environments (e.g., SharePoint);
- grant and/or case management systems;
- records management systems (e.g., OpenText); and
- geographic information systems.

Barring exceptions, the security classification applied to a system or application is determined by the most sensitive data or information within the system or application (e.g., if a system

maintains both **Protected B** and **Protected C** data and information, the system is classified as **Protected C**). Consequently, applying security classification to a system or application means that all data and information maintained by the system are subject to controls established for that security classification (e.g., a record classified as **Public** maintained in a system classified as **Protected B** would be subject to **Protected B** controls).

Although the security classification of a system or application is determined by the most sensitive data and information within it, there may be exceptions. Exceptions may include scenarios where data and information of a higher security classification are maintained in a system or application with a lower security classification (e.g., data and information classified as **Protected B** is maintained in a system or application classified as **Protected A**); such exceptions would require:

- additional controls that can safeguard data and information against unauthorized access and/or potential risks (e.g., preventing users outside of a department from accessing a SharePoint site);
- a comprehensive analysis that identifies the potential risks; and
- documentation that clearly demonstrates that any potential risks have been explicitly acknowledged by the appropriate stakeholders.

Record
Classifying at the record level can be beneficial when a system or application contains many different types of records with different security classifications, ranging from **Public** to **Protected C**. For example, instead of applying a **Protected C** classification to a system or application, which would subject all data and information maintained in the system or application to **Protected C** controls, classifying at the record level will enable a system or application to fulfill multiple security and access requirements.

Field
Within certain types of systems and applications, security classification may be applied to fields (such as specific Excel columns or certain metadata fields in a database). There may be a need to classify at this level if certain fields require a higher security classification. For example, a Human Resources spreadsheet may have the security classification of **Protected A**, but feature a column that contains **Protected C** information.

Applying security classification at a field level enables additional security and access controls to be applied as required without restricting access to data and information with a lower security classification.

Data and Information from Other Jurisdictions

Data and information that have been received from another jurisdiction must:

- maintain the classification level applied by the originating jurisdiction; and
- be handled according to the rules and procedures established by the originating jurisdiction.

If the data or information received from another jurisdiction lacks security classification, the data and information may be subject to the GoA security classification standard—meaning it must be properly assessed and classified in collaboration with the originating jurisdiction.

Roles and Responsibilities

Determining the security classification for data and information is a collaborative process that involves multiple stakeholders. While the selection of a security classification is ultimately the responsibility of the information controller, determining the appropriate security classification should involve consultation with the following stakeholders:

- information controllers
- information custodians
- Corporate Information Security Office (CISO)
- Sector Information Security Officers (SISOs)
- Information Management and Technology (IMT) Professionals
- GoA employees

Information controllers (often the head of a program or branch) have the responsibility and decision making authority for data and/or information throughout its lifecycle, including creating, classifying, restricting, regulating and administering its use or disclosure. Information controllers are responsible for:

- determining security classification after appropriate collaboration and/or consultation;
- ensuring adherence to the Information Security Management Directives;
- providing advice on legislative and policy requirements for data and information security; and
- ensuring that data and information and systems/applications are entrusted to appropriate information custodians.

Information custodians maintain or administer data and information on behalf of the information controller. Custody of data and information may be temporary or permanent, depending on the data and information and the applicable information management lifecycle stage. Information custodians are responsible for:

- implementing the data and information security requirements determined by the information controller (e.g., developing processes/procedures for the application of security classification);
- ensuring that data and information are accessible, managed, maintained and preserved;
- providing and managing security for both a system/application and the data and information maintained therein;
- assisting in the design, implementation, maintenance and operation of the security infrastructure protecting both the system/application and the data and information maintained therein; and
- implementing and administering appropriate security measures to sustain a level of data and information security consistent with:
    - GoA requirements; and
    - the direction set by information controllers and CISO.

NOTE: Depending on the situation, the role of information controller and information custodian may be occupied by the same person/business area/department/etc.

Corporate Information Security Office (CISO) is responsible for:

- providing guidance and assistance on the implementation of the Data and Information Security Classification Standard;
- reviewing the security design of all information technology systems;

- working collaboratively with SISOs to regularly audit information technology systems for compliance with GoA data and information security policy instruments, applicable legislation and business requirements; and
- reporting information technology system audit findings to departments and executive management.

Sector Information Security Officers (SISOs) are responsible for:

- being the single point of contact for data and information security issues in their sector;
- coordinating assessments to verify that the sector is in compliance with data and information security management policy instruments;
- developing sector benchmarks, guidelines or processes that support enterprise data and information security policy instruments;
- contributing to the development and adoption of enterprise standards for data and information security;
- developing and delivering a data and information security awareness and training program directed at sector personnel that is based on complementary enterprise programs;
- providing security advice and expertise to sector business units; and
- communicating security challenges and issues with relevant sector executives and managers.

IMT Professionals in each department are responsible for:

- implementing developed sector benchmarks, guidelines or processes for the security and management of data and information;
- identifying opportunities to leverage relevant sector and enterprise security classification training and awareness programs;
- liaising with SISOs and business areas to facilitate application of security classification;
- actively working with business areas to identify gaps in security classification; and
- identifying methods and means for applying security classification (e.g., headers/footers on documents).

GoA employees are responsible for:

- understanding their data and information security obligations, which may include (but are not limited to):
    - applying security classification at the direction of the information controller and/or information custodian; and
    - taking reasonable steps to safeguard data, information and systems/applications, such as:
        - applying labels to data and information;
        - ensuring that data and information are uploaded to secure digital repositories;
        - securing workstations when not in use; and
        - securing physical data and information in locked cabinets and/or drawers.
- participating in enterprise and/or department training and awareness programs;
- communicating with management and their SISO regarding security issues.

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.
- Legislated disciplinary action (i.e., Public Service Act) may be taken depending on the severity of non-compliance.

References and Supporting Resources

Detailed guidance on implementing data and information security classification is available in the following technical guides:

- 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