

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
Information Technology Division
Cybersecurity and Risk Management Branch

February 26, 2026

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
Information Technology Division, Cybersecurity and Risk Management Branch

Confidentiality Statement

This document is intended for the Saskatchewan Ministry of SaskBuilds and Procurement, Information Technology Division, and partner organizations. It may contain legally privileged and/or confidential information and must not be disseminated, distributed, or copied.

Contents

REFERENCES	1
1. WHAT IS INFORMATION PROTECTION CLASSIFICATION?	2
2. THREE WAYS TO CLASSIFY INFORMATION	3
WHAT IS PERSONAL INFORMATION	3
3. INFORMATION PROTECTION CLASSIFICATION GRID	4
4. APPLYING INFORMATION PROTECTION CLASSIFICATION.....	6
MANY TYPES OF INFORMATION	7
MARKING OR LABELLING INFORMATION	7
DOWNGRADING OR DECLASSIFYING OF SENSITIVE INFORMATION	7
AUTOMATIC DOWNGRADING OR DECLASSIFICATION	7
SHARED INFORMATION	8
5. DETERMINATION OF SECURITY STANDARDS.....	8
6. LIMITATION OF INFORMATION PROTECTION CLASSIFICATION	8
REVISION HISTORY	9

References

- [The Freedom of Information and Protection of Privacy Act](#) (Section 24, in particular).
- [The Health Information Protection Act](#) (HIPA), if applicable. (Section 2, in particular).
- Other relevant legislation, as applicable, to determine what is personal. You may need to consult a lawyer.

Contact the Cybersecurity and Risk Management Branch at SBPITInformationSecurityBranch@gov.sk.ca if clarification is needed for any content within this document.

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
Information Technology Division, Cybersecurity and Risk Management Branch

1. What is Information Protection Classification?

Information Protection Classification is a business tool that enables enhanced security in large organizations. When fully implemented and combined with effective security, it ensures the confidentiality, integrity, availability, and privacy of information.

Good security can be distilled down to two objectives: **Determining value and applying appropriate security.** Information Protection Classification is a formal process that completes the first objective: determining value.

The best security involves analysis and decision-making done in a structured way. The following “Household Security Grid” shows how we place value on items and make security decisions every day. For each of the four household items, the following table:

- Lists the items.
- Assigns a value.
- Indicates the cost of replacement.
- Describes security measures.

Example: Information Protection Classification for Household Security Grid

Item	Value	Cost to Replace	Security
Newspapers	Low	Low	None
Household cash	Varies; Usually low	Equal value of cash	Unlocked drawer
Receipts for income tax	No cash value	High; May be impossible to re-create	In file box in a closet
Family wills	High	Irreplaceable	Original in safety deposit box; Copy with lawyer

As you can see, we all make classification and security decisions regarding our possessions automatically. Now, let us introduce a new item into our matrix: Great-grandma’s photo album.

Item	Value	Cost to Replace	Security
Great-grandma’s photo album	High; A family heirloom.	Irreplaceable	?

If we followed the examples in the “Household Security Grid”, we would make a copy of the album for viewing and store the original in our safety deposit box because it is a valued family heirloom *and* irreplaceable.

This guide applies analysis and a structured decision-making process to determine the security requirements for Government of Saskatchewan Information Assets. Applying Information Protection Classification is the first part of complete security.

The next step – defining and applying appropriate security measures – is independent of the classification process and is conducted in collaboration with the Cybersecurity and Risk Management Branch.

Instead of a dollar amount, the factors which determine security levels in this guide are a combination of the business requirements for confidentiality, integrity, availability, privacy, and the harm that could be caused by unauthorized access, use, or release of the information.

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
Information Technology Division, Cybersecurity and Risk Management Branch

2. Three Ways to Classify Information

Classifying information is the first step in adequately protecting it. Information in the Government of Saskatchewan is classified in one of three ways:

1. Specific kinds of information that exist in every department or agency are automatically classified. Human Resources (HR) and Cabinet information are two examples.
2. Some general categories of information, like published reports and information web sites, have the same classification regardless of which department/agency owns the data.
3. The remaining information is classified at the function level by the department/agency that owns it. The most sensitive information used for a function will determine the classification of all associated information.

Information is classified to facilitate the establishment of appropriate security controls. The objective of classification and security is to protect the confidentiality, integrity and availability of information.

- **Confidentiality** ensures that information can only be accessed by authorized individuals.
- **Integrity** ensures that only authorized and accurate changes are made to information.
- **Availability** ensures that authorized users have access to the information when required.

While integrity and availability are important considerations at all levels, confidentiality becomes increasingly important as you move up the grid.

For the purposes of Information Protection Classification, a function is defined as: all the information and information technology associated with a single service/process (or group of closely related services/processes) in a department or agency. This includes files (hard copy and electronic, including e-mail), applications, databases, data storage, hardware, networks, and procedures for the transmission of data.

Examples of functions:

- Consumption taxes in the Department of Finance.
- Income support programs in Community Resources and Employment.
- Occupational Health and Safety in the Department of Labour.
- Policy development in the Information Technology Division.

The Information Protection Classification Grid in Section 3 of this document will assist in classifying information.

What is Personal Information

Personal Information (PI) is as defined by *The Freedom of Information and Protection of Privacy Act*.

You will need to become familiar with:

- [*The Freedom of Information and Protection of Privacy Act*](#) (Section 24, in particular).
- [*The Health Information Protection Act*](#) (HIPA), if applicable. (Section 2, in particular).
- Other relevant legislation, as applicable, to determine what is personal. You may need to consult a lawyer.

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
 Information Technology Division, Cybersecurity and Risk Management Branch

3. Information Protection Classification Grid

Information Protection Classification: Class A

Information Protection Classification Grid				
Class	Definition	Information Examples	Other Information Examples	Consequences
A	<p>Could reasonably be expected to cause extremely serious personal or enterprise harm, including:</p> <ul style="list-style-type: none"> • Significant financial loss. • Loss of life or public safety. • Social hardship. • Major political or economic impact. 	<ul style="list-style-type: none"> • Highly sensitive personal information that, if compromised, could jeopardize an individual's safety. • Highly sensitive personal health information that, if compromised, could jeopardize an individual's safety. • Information on a police informant. • Information relating to a sex offender. 	<p>When <i>confidentiality</i> is the key consideration:</p> <ul style="list-style-type: none"> • Cabinet documents. • Provincial budget information (before public release). • Preliminary investigation files of a major crime. • Legislation under development. • Sealed tenders and request for proposals (RFPs) prior to the closing of a competition. <p>When <i>availability</i> is the key consideration, information that when compromised will result in:</p> <ul style="list-style-type: none"> • Extended loss of an essential government service. • Loss of crisis communications during emergencies. • Loss of essential police communications and data. • Loss of emergency health services. <p>When <i>integrity</i> is the key consideration:</p> <ul style="list-style-type: none"> • Information systems and material used for testing food or water supply that could result in loss of life or severe illness. • Law enforcement information such as that held at the Canadian Police Information Centre (CPIC). 	<p>It is difficult, if not impossible, to put a dollar value on the Government's reputation. But as an indicator of the grave consequences of compromising confidentiality, availability or integrity of information in this classification level, think of the total impact as being <i>over 10 million dollars</i> in legal costs, technical problems and loss of reputation.</p>

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
 Information Technology Division, Cybersecurity and Risk Management Branch

Information Protection Classification: Class B

Information Protection Classification Grid				
Class	Definition	Information Examples	Other Information Examples	Consequences
B	Could reasonably be expected to cause serious personal or enterprise harm, loss of competitive advantage, loss of confidence in the government program, financial loss, legal action and damage to partnerships, relationships and reputation.	<ul style="list-style-type: none"> • Most personal information. • Most personal health information as defined by the Health Information Protection Act. • Information relating to an individual's racial or ethnic origin. • Information describing a citizen's finances. • Case files and information on eligibility for social benefits. • Details of an Employee Family Assistance Plan (EFAP) file. • Human Resources files. 	<p>When <i>confidentiality</i> is the key consideration:</p> <ul style="list-style-type: none"> • Information compiled as a part of a violation of law. • Ministerial briefing notes. • Information on a company's credit rating. • Disclosure of trade secrets or intellectual property. • Information on competitiveness reviews and investment attraction. • Information/data related to the exploration, mining and production data of mineral/energy resources. • Inaccurate money transfers to a municipality due to loss of integrity. • Information received from another government relative to its position on a particular trade issue. • Drafts of department policy. <p>When <i>availability</i> is the key consideration:</p> <ul style="list-style-type: none"> • Payments of benefits or income support to Saskatchewan citizens. • Financial and reporting systems. • Senior management information systems. <p>When <i>integrity</i> is the key consideration:</p> <ul style="list-style-type: none"> • Information related to food or water supply that would not meet expected standards of quality but would not cause illness. • Information related to nonemergency health care. • Financial transactions and payments. • Ownership and disposition of Crown minerals, lands, and oil and gas rights. • Information that could be used for Criminal purposes. 	If it could be measured in dollar terms, the significant consequences of compromising confidentiality, availability or integrity of this information would be <i>between one hundred thousand and 10 million dollars</i> in legal costs, technical problems and loss of reputation.

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
 Information Technology Division, Cybersecurity and Risk Management Branch

Information Protection Classification: Class C

Information Protection Classification Grid				
Class	Definition	Information Examples	Other Information Examples	Consequences
C	Could reasonably be expected to cause significant harm to individuals or enterprises with limited: <ul style="list-style-type: none"> Financial losses. Impact in service/performance levels and reputation. 	Some limited personal data like mailing and phone lists. The data does NOT fit the definition of personal information or personal health information as defined in legislation.	<ul style="list-style-type: none"> The availability/integrity of government web sites. General information databases such as a listing of Saskatchewan manufacturers. Economic statistics/analysis/forecasts. General administrative files. 	If it could be measured in dollar terms, the consequences of compromising the confidentiality, availability or integrity of this data would be <i>between one thousand and one hundred thousand dollars.</i>

Information Protection Classification: Public

Information Protection Classification Grid				
Class	Definition	Information Examples	Other Information Examples	Consequences
Public	Will not result in harm to individuals, governments or private sector institutions	Personal information cannot be classified as "Public"	<ul style="list-style-type: none"> Information on government web sites. Job advertisements. Public reports and policy statements. Public health information. Job duties and pay scales. 	The type of information, if lost, changed or denied, would not result in harm to an individual or government organization and the financial loss would be <i>under one thousand dollars.</i>

4. Applying Information Protection Classification

Typically, the people responsible to classify information include the information owner (those in possession and/or control of the information), a member of the organization’s senior management (Executive Director or Director), the Ministry’s Security and Privacy Officers, Cybersecurity staff with knowledge of security issues, and an individual responsible for Records Management. Staff from the Cybersecurity and Risk Management Branch are available to assist departments in the application of Information Protection Classification.

The first step in classifying information is to do an inventory of all information in an application, solution, system, and/or service being assessed.. The next step is to determine if an information/records system includes personal information. The legal definition of personal information (PI) is in section 24 of [The Freedom of Information and Protection of Privacy Act](#) (the FOIPP Act). The legal definition for personal health information (PHI) is in section 2 of [The Health Information Protection Act](#) (HIPA). Ministry or Agency specific legislation may also apply.

If it is determined that the information being classified falls within the scope of legislation, and is therefore personal information or personal health information, classification should only proceed with the assistance of the Ministry’s Privacy Officer. Regardless of whether information is or is not considered personal information or personal health information, a Ministry’s Privacy Officer must sign off to signal their acceptance on all Statements of Sensitivity.

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
Information Technology Division, Cybersecurity and Risk Management Branch

Many Types of Information

Some types of information that will be included in classification levels are:

- information received in confidence from other governments or organizations (possibly private sector entities).
- information prepared by or obtained by a federal or provincial investigative body (could be law enforcement).
- personal information as defined in the FOIPP Act.
- business information.
- budget details prior to the delivery of the Budget Address.
- advice and recommendations involving Cabinet or confidences of the public that would affect the operations or integrity of government.
- personal health information as defined in HIPA.
- information shared between departments.

Marking or Labelling Information

Information that is deemed to be sensitive should be classified/marked at the time that it is created. This will ensure that the information has appropriate protection as it enters government hands. All individuals who have access to this sensitive material need to be made aware of its classification so they can be part of its security. Additionally, any information that is transferred beyond the organization in which it was created must be appropriately couriered and marked. Information that is exchanged under formal Memorandum of Agreement must be marked and the recipient organization must be able to translate its security classification into appropriate protective measures.

The [Government Information Protection](#) initiative of the Cybersecurity and Risk Management Branch aims to work with ministries to deploy technology that will facilitate the labelling of information via Government's primary application suites such as Microsoft Office.

Downgrading or Declassifying of Sensitive Information

Information should only be classified for the period that it requires protection after which it should be downgraded or declassified. This requirement recognizes that information can lose its sensitivity with the passage of time or the occurrence of specific events. This process contributes to the overall integrity of the security system and will ensure that information can safely be made available to those who need to have it quickly and safely.

Automatic Downgrading or Declassification

Organizations should, when applicable, provide for automatic downgrading or declassification of information by selecting a specific year or event or, a review period at the time the record is created. When such information is received under a Memorandum of Agreement, the recipient should ask if a declassification or downgrading date has been selected by the originating organization for the information.

It is suggested that a period be identified for all categories of information, along with the date or "event-specific triggers" that will indicate downgrading or declassification. However, it is also suggested that an automatic expiry date not be selected for information classified in level "A". Downgrading information as appropriate will be a regular part of information handling. This does not mean downgrading the Information Protection Classification level is synonymous with making it publicly available. The normal FOIPP application review process would still apply.

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
Information Technology Division, Cybersecurity and Risk Management Branch

Shared Information

The requirement to downgrade or declassify sensitive information applies not only to information within an organization but also to information provided from one department to another, or from one jurisdiction or partner to the government under agreement. Before declassifying or downgrading any such information, the originator must be contacted. If need be, the information can be sent to the “office-of-origin” for downgrading or declassification. In certain circumstances, it may not be possible to consult the originator. In such cases, consultation with other appropriate officials such as the Privacy Officer for that organization should occur.

5. Determination of Security Standards

This guide supports the process of determining correct safeguards for each classification by clearly indicating potential consequences of loss for each level; however, it will not dictate specific security standards or controls. The Cybersecurity and Risk Management Branch will work with organizations to ensure the appropriate security standards and controls are applied.

6. Limitation of Information Protection Classification

This guide is limited to identifying the proper indicator to place on information so that it is clear what set of protective standards and controls are required.

Specific security standards that apply to information in each classification level (A, B, C and Public) are developed independently of this document. While these security standards and controls will change over time, as technology evolves and the cybersecurity landscape changes, the process of classification of information should not change.

Establishing “protective profiles” or “minimum baseline strategies” in communities of interest such as the “health area” can be alternative strategies that will provide assurance that information is being protected at an appropriate, secure level.

Similar to this “community of interest” example, the Canadian Payments Association may also establish minimum protective standards in the area of finance or payments. This will allow the exchange of financial information during ESD given that an “industry best practice” has been established for information safety. This will apply equally to private and public sector organizations.

Generally, access to information is separate from Information Protection Classification. Granting access is a procedure internal to the support of your organization. When access requests are made from outside government, the existing FOIPP process still applies.

A Guide for Information Protection Classification

Ministry of SaskBuilds and Procurement
Information Technology Division, Cybersecurity and Risk Management Branch

Revision History

Version ID	Date of Change	Author	Rationale
0.1	13 September 2018	CSRM	Transferred document into new visual format. No content has been changed.
0.2	12 November 2018	CSRM	Reviewed document; Minor changes to punctuation.
0.3	02 January 2019	CSRM	Reviewed document; Minor changes to punctuation. Sent request to ISB for full peer review.
0.4	02 March 2023	CSRM	Removed irrelevant information, clarified and provided links to references, and added additional explanations and clarity to guide.
1.0	26 February 2026	CSRM	ANNUAL REVIEW UPDATED: Minor grammatical and formatting corrections. Some terminology updated to align with other documentation.