Statement of Sensitivity

Last revised: April 2024
Last reviewed: April 2024
Next review: April 2026

Ministry of SaskBuilds and Procurement
Information Technology Division, Information Security Branch

This form should be completed by the Information Owner to assess the confidentiality, integrity, and availability requirements for the Ministry's information assets. For the best experience, complete the form using Adobe Acrobat. Cyber Security and Risk Management Branch (SBPITInformationSecurityBranch@gov.sk.ca) will accept completed forms and is available if clarification is needed for any content within this document.

Application/Project

Prepared by (Information Owner)

Ministry

DD/MM/YYYY

Application/Solution/Service Background

Provide background information and describe the purpose or intent of the application, solution, and/or services being assessed.

Provide project background information and describe the application, solution, and/or services being assessed.

Data Description

Describe the data contained within, processed by, or accessed by the system, application, solution, and/or services.

Describe the data contained within, processed by, or accessed by the system, application, solution, and/or services.

Government of Saskatchewan

Information Protection Classification

To gain an understanding of Information Protection Classification and for helpful information and assistance in completing this Statement of Sensitivity, you may refer to "*A Guide for Information Protection Classification*".

The three key properties of information security are confidentiality, integrity, and availability. The Information Classification is based on the assessments of these three key properties of the information. This Statement of Sensitivity is intended to assist the Information Owner in assessing the confidentiality, integrity, and availability requirements of an information system and in identifying the Information Classification.

Confidentiality

Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes. The confidentiality level assessed for information assets informs the level of protection necessary to prevent disclosure of information to unauthorized parties.

Integrity

Integrity is the property of information accuracy and completeness and refers to the level of protection necessary to prevent information assets from being modified by unauthorized parties. The information integrity level assessed for information assets informs the level of protection necessary to ensure that information is authentic and protected from alteration by unauthorized parties.

Availability

Availability is the property of information being accessible and usable upon demand by an authorized entity. The availability level assessed for information assets informs the level of protection necessary to ensure that authorized entities are able to access the information when needed. Information security controls ensure that information assets are available to authorized parties whenever they need to access them.

Government of Saskatchewan Information Classifications:

Class A

A breach or loss of information could reasonably be expected to cause extremely serious personal or enterprise injury, including significant financial loss, loss of life or public safety, social hardship, major political or economic impact.

Class B

A breach or loss of information could reasonably be expected to cause serious personal or enterprise injury, loss of competitive advantage, loss of confidence in the government, financial loss, legal action, damage to partnerships, relationships and reputation.

Class C

A breach or loss of information could reasonably be expected to cause personal or enterprise injury including limited levels of financial losses and impacts on services, performance levels, and reputation.

Public

A breach or loss of information will not result in injury to individuals, governments, or private sector institutions.

Confidentiality

Answer each of the questions in the tables that follow. The questions apply to information that is processed, transmitted, managed, and/or stored. To assist with the determination of confidentiality, conduct an injury test by asking, “Who or what will be harmed if the information is disclosed to unauthorized parties?” Remember that aggregate data can be more sensitive than an individual record or a smaller subset of records.

CRITICAL (extremely serious injury)			
Does the data contain…		**Yes**	**No**
1.	information that, if compromised, would jeopardize an individual’s safety?	□	□
2.	information about police informants or witness protection?	□	□
3.	cabinet documents?	□	□
4.	legislation or regulations under development?	□	□
5.	information that, if compromised, could cost the Government in excess of $10,000,000?	□	□
6.	other examples of CRITICAL Confidentiality information? (describe below)	□	□
Other CRITICAL Confidentiality information includes:			
	Describe the information considered to have CRITICAL levels of confidentiality requirements.		

HIGH (serious injury)			
Does the data contain…		**Yes**	**No**
7.	information that, if compromised, could cause invasion of privacy or identity theft?	□	□
8.	personal health information?	□	□
9.	ministerial briefing notes?	□	□
10.	trade secrets or intellectual property?	□	□
11.	information related to the exploration, mining, and production of mineral/energy resources?	□	□
12.	information that, if compromised, would cost the Government between $100,000 and $10,000,000?	□	□
13.	other examples of HIGH Confidentiality information? (describe below)	□	□
Other HIGH Confidentiality information includes:			
	Describe the information considered to have HIGH levels of confidentiality requirements.		

Confidentiality (continued)

MEDIUM (low injury)			
Does the data contain…		**Yes**	**No**
14.	a small amount of personal information?	□	□
15.	economic statistics, analysis, and/or forecasts?	□	□
16.	general administrative files?	□	□
17.	information that, if compromised, would cost the Government between $1000 and $100,000?	□	□
18.	other examples of MEDIUM Confidentiality information? (describe below)	□	□
Other MEDIUM Confidentiality information includes:			
	Describe the information considered to have MEDIUM levels of confidentiality requirements.		
LOW (no injury)			
Does the data contain…		**Yes**	**No**
19.	information intended to be accessed by the public on government websites?	□	□
20.	job advertisements?	□	□
21.	public reports and policy statements?	□	□
22.	job duties and pay scales?	□	□
23.	public health news and advisories?	□	□
24.	other examples of LOW Confidentiality information? (describe below)	□	□
Other LOW Confidentiality information includes:			
	Describe the information considered to have LOW levels of confidentiality requirements.		

Integrity

CRITICAL Integrity			
Does the data contain…		**Yes**	**No**
1.	information that, if compromised, would impact critical infrastructure in the Province of Saskatchewan?	□	□
2.	information that, if compromised, would impact the food or water supply resulting in illness or loss of life?	□	□
3.	information on extremely large financial transactions?	□	□
4.	other examples of CRITICAL Integrity information? (describe below)	□	□
Other CRITICAL Integrity information includes:			
	Describe the information considered to have CRITICAL levels of integrity requirements.		

HIGH Integrity			
Does the data contain…		**Yes**	**No**
5.	information that, if compromised, would impact the food or water supply without causing death or illness?	□	□
6.	information related to non-emergency health care?	□	□
7.	information on financial transactions and payments?	□	□
8.	ownership and disposition of Crown minerals, lands, and oil and gas rights?	□	□
9.	other examples of HIGH Integrity information? (describe below)	□	□
Other HIGH Integrity information includes:			
	Describe the information considered to have HIGH levels of integrity requirements.		

MEDIUM/LOW Integrity			
Does the data contain…		**Yes**	**No**
10.	information with integrity requirements that do not fall into the categories above? (describe below)	□	□
MEDIUM or LOW Integrity information includes:			
	Describe the information considered to have MEDIUM or LOW levels of integrity requirements.		

Availability

CRITICAL Availability			
Would loss of the data or information system…		**Yes**	**No**
1.	result in an extended loss of an essential government service?	□	□
2.	cause a loss of crisis communications in an emergency?	□	□
3.	cause a loss of emergency health services?	□	□
4.	disrupt financial systems resulting in losses exceeding $10,000,000?	□	□
5.	cause loss of a critical service identified in a Service Level Agreement?	□	□
6.	other examples of CRITICAL Availability? (describe below)	□	□
Other CRITICAL Availability information includes:			
	Describe the information considered to have CRITICAL availability requirements.		
HIGH Availability			
Would loss of the data or information system…		**Yes**	**No**
7.	cause unavailability of payments of benefits or income support to Saskatchewan citizens?	□	□
8.	cause unavailability of financial and reporting systems?	□	□
9.	cause unavailability of senior management information systems?	□	□
10.	disrupt financial systems resulting in losses between $100,000 and $10,000,000?	□	□
11.	cause loss of a medium availability service identified in a Service Level Agreement?	□	□
12.	other examples of HIGH Availability? *(describe below)*	□	□
Other HIGH Availability information includes:			
	Describe the information considered to have HIGH availability requirements.		
MEDIUM/LOW Availability			
13.	Does the data contain information with availability requirements that do not fall into the categories above? (describe below)	□	□
MEDIUM or LOW Availability information includes:			
	Describe the information considered to have LOW or MEDIUM availability requirements.		

Crown Jewel Declaration

A Ministry Crown Jewel is critical processes, data, applications, services, and infrastructure that, if compromised, could cause extremely serious injury to public safety, Government reputation, and public trust. Crown Jewels are:

- Essential to the operations and/or survival of the government.
- Necessary to recreate the government's legal, regulatory, competitive, or financial position.
- Necessary to preserve the government's claims and/or rights.
- Highly sensitive or privileged in nature.

Crown Jewel	Yes	No
Does the Ministry consider this system a Crown Jewel? Note that ITD will evaluate to determine if the system should be included in Government's Crown Jewel list.	□	□

Information Classification Declaration

Using results from the Confidentiality, Integrity, and Availability tables above, the Information Owner now declares the appropriate Information Classification of the data contained within or processed by the system. Select the appropriate radio button below.

Information Classification		
Class A	A breach or loss of information could reasonably be expected to cause extremely serious personal or enterprise injury.	○
Class B	A breach or loss of information could reasonably be expected to cause serious personal or enterprise injury.	○
Class C	A breach or loss of information could reasonably be expected to cause low injury to individuals or enterprises.	○
Public	A breach or loss of information will not result in injury to individuals, governments, or private sector institutions.	●

Signatures

At a minimum, the Information Owner and Security Officer should sign below. If the information includes Personally Identifiable Information (PII), the Ministry Privacy Officer should also sign below.
Electronic signatures are accepted.

Information Owner:	**Security Officer:**	**Privacy Officer:**
Signature	Signature	Signature
Name (type or print)	Name (type or print)	Name (type or print)
Title (type or print)	Title (type or print)	Title (type or print)
Date (day/month/year)	Date (day/month/year)	Date (day/month/year)