Key Messages and Questions and Answers
Government Information Protection

KEY MESSAGES:

- Government of Saskatchewan users will get a new toolbar enabled in your Microsoft Outlook and other Office applications to help you to keep information secure.
- It's called the Microsoft Information Protection toolbar – and it will let you limit the level of access you give to recipients of your documents and emails, simply by choosing a sensitivity label.
- The toolbar will allow employees to categorize and protect information by classifying the sensitivity of emails or Word documents such as Outlook, Word, PowerPoint, and Excel, as well as PDF files.
- It offers sensitivity labels – Class A, B, C, Public, and Not Classified – so you can set the right level of access to protect your documents and emails. By default, all documents are labeled "Not Classified" meaning anyone can open, edit, and read them as normal.
- The use of the new sensitivity labels toolbar and controls is optional.
- For any questions about the Government Information Protection tool, please contact the ITD Service Desk or visit the Taskroom page.

QUESTIONS AND ANSWERS:

Q1 What is the Government Information Protection (GIP) Tool?
A**:** The GIP is a tool that allows employees to categorize and protect information by classifying the sensitivity of emails or Word documents. Classification will limit who can view, print, save, and share classified items. The classification options align with the Government Information Classification standards (Class A, B, C, or Public). The Information Classification Guidelines are published on Taskroom.

This tool grants authorized users access and permissions – view, edit, print, save, share – while blocking the access of unauthorized users to sensitive information in documents and emails.

Q2 What is the Information Protection Sensitivity Labels toolbar?
A**:** The Information Protection Sensitivity Labels Toolbar helps Government of Saskatchewan (GOS) employees categorize and protect government information (sensitive data).

The toolbar offers the ability to assign a sensitivity label to an email or a document, so you can set the right level of access (permissions) to protect your data while classifying emails and documents according to Government Information Classification standards. For example, a sensitivity label determines whether recipients can forward, print, save, remove encryption, or share a document beyond the original recipients or externally.

Learn what the labels do by having a look at the Sensitivity Labels Classification Taxonomy tables for documents and emails:

- Taxonomy for Documents (printable for reference).
- Taxonomy for Emails (printable for reference).

Learn why Protect Information

- Why Protect Information (Video)

How to Protect Information using Sensitivity Labels in Documents and Emails

- How to Protect Information using Sensitivity Labels in Documents and Emails (Video)

A guide to applying Sensitivity to emails and documents

- Emails (Document 1)
- Documents (Document 2)

Q3 Is this tool mandatory?

A**:** The use of the new sensitivity labels toolbar and controls is optional at this time. If you are not comfortable using the tool or do not currently understand content classification or the sensitivity labels and their associated permissions, you do not need to apply sensitivity labels to your documents or emails, and it is business as usual. All documents and emails are assigned the default label "Not Classified", meaning the information held within has not been categorized or protected.

It remains important that you know sensitivity labels are in use at GOS in the event you receive a labeled document or email. For example, the Sensitivity Labels Classification Taxonomy charts explain why a document or email you receive is encrypted and why you may or may not be able to share it with an internal or external colleague without submitting a request.

Q4 Why is the Information Protection Sensitivity Labels Toolbar being installed for users?

A**:** This is being installed for users to give everyone the ability to classify information appropriately and apply protection based on the sensitivity of the data. Having knowledge of existing GOS classifications helps users ensure that the required protection is applied.

While we may think of the external threats that could result in a breach, it is important to consider protecting information internally, too. Internal breaches can occur in organizations by accident. Restricting, classifying, and protecting information plays a significant role when it comes to preventing internal actions that could result in a data breach.

Q5 When is it being installed, and do I need to do anything before, during or after installation?

A**:** The labels toolbar were installed on December 14,2023. No action is required by you — the new Information Protection Sensitivity Labels toolbar will appear within Outlook and Microsoft 365 applications such as Word, Excel and PowerPoint when the installation is completed.

Q6 Will the rollout take place at one time across GOS or will it be phased?

A**:** Rollout took place on December 14, 2023, and it was be government-wide, not phased. This approach is being taken to ensure there is no interruption for people who appropriately receive a classified document and need to open or view it as intended.

Q7 Which of my devices will have this new toolbar installed?

A: This will be automatically installed on your government-owned workstation (desktop/laptop) accessing government information.

Q8 Am I required to use these Information Protection Sensitivity Labels now or in the immediate future?

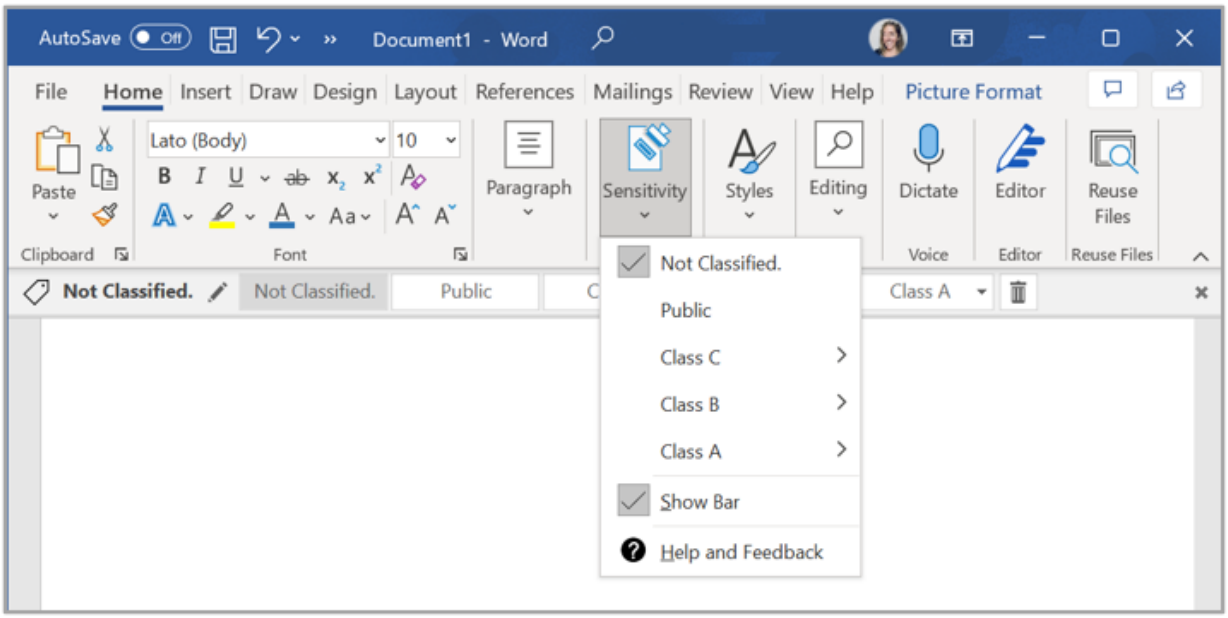
A: No, the use of Information Protection Sensitivity Labels is optional for all employees. It will be up to users whether they choose to use the Information Protection Sensitivity Labels toolbar to apply a Class A, B, C, or Public label based on the sensitivity of a document or email.

Q9 Where is the sensitivity button located?

A: The sensitivity button is located within the 'Home' ribbon of Microsoft Office applications (Word, Excel, and PowerPoint) and within Outlook.

Select the Sensitivity button and click 'Show Bar' to ensure the Microsoft Information Protection Sensitivity Labels toolbar appears at the top of documents and emails.

Example Image: Information Protection Sensitivity Labels Toolbar and Button in Word

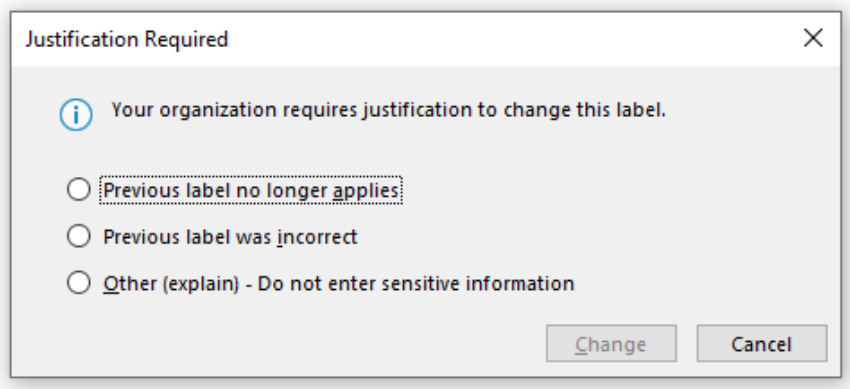


Q10 Why is the Information Protection Sensitivity Label now being applied to my documents and emails? How do I remove it?

A: By default, all documents and emails will be labeled as "Not Classified". This implies that the author of the content did not classify the document or email according to "A Guide for Information Protection Classification". Users will have to make educated decisions to classify appropriately. This is to ensure sensitive documents are properly categorized and protected from unauthorized access or modification.

Complete removal of a label is not an option – It can only be downgraded as low as "Not Classified". The sensitivity labels can only be changed by document owners. A permission request can be made by a recipient using the controls offered by the sensitivity labels toolbar and owners will need to provide justification when changing a label.

Example image: Justification Prompt for Changing a Sensitivity Label



Q11 What types of information can this tool label (i.e., emails, Microsoft Office documents… any others?)
A: This tool labels all Microsoft Office documents including emails, Word documents, Excel documents, and PowerPoint documents.

Q12 How are levels of access (permissions) granted by this tool?
A: Levels of access, or permissions, determine what the recipient of the document can do with it. Examples include whether recipients can forward it, print it, save it, remove encryption from it, share it beyond the original recipients or share it externally.

The sensitivity label that is applied to the document defines a recipient's level of access, **not** an individual recipient's title or role.

The author of the document and or email sets the label and coinciding control/s that go along with that label. See the taxonomy tables on the Taskroom page to better understand the labels and their associated permissions. Information needs to be aligned with the data classification rules.

Q13 How do I determine if my information should be Class A, B, C, or Public?
A: A document's class of information is based on the sensitivity of the content within the document. For more detailed information about these classifications, refer to the document: A Guide for Information Protection Classification.

Q14 Where can I learn more about Information Protection Classification, so I can be sure to apply the right label?
A: For more information refer to the document: A Guide for Information Protection Classification on Taskroom.

Q15 I am having trouble opening a document that I need access to and was labelled as Class B or A. How can I open it?
A: Either you have not been granted access to the document or you are not authenticated to enable your access. Use the following steps to request access:

- Ensure you have been granted access to the document by following up with the document owner.
- If your issue is not resolved, contact the IT Service Desk at 306-787-5000.

Q16 What is the scope of GIP data classification?

A: We are enabling the tool in Microsoft applications that will allow users to apply appropriate classification labels to documents and emails. In the crawl phase this tool is optional to use by users.

According to A Guide for Information Protection Classification, all individuals who have access to sensitive information need to be aware of its classification so they can ensure the information has appropriate protection and security. This tool will enable users to classify and protect documents and emails from unauthorized user access.

Q17 How do I change the classification on a document if it is classified incorrectly?
A: If you are the owner or co-owner, you can reclassify content with justification. If you are not the current owner or co-owner, please direct this request to the owner/creator of the document. The document creator/owner and co-owner can reclassify the document and provide a reason when prompted by the tool.

Q18 How do labels that are applied to an email and a document interact?
A: Email and document labels are independent of one other. An email label will not change a document's label (and vice versa), except when a document is labeled as Not Classified. This means that when you label an email as Class A, Class B, Class C, or Public, the Not Classified document will inherit the protection of the labeled email.

It is best practice to not mix sensitivity labels when emailing out – use one file type per email for simplicity.

Q19 Who do I call for support for using this new tool?
A: For any questions or issues, please contact the IT Service Desk at 306-787-5000.

Q20 Is information classification related to *The Local Authority Freedom of Information and Protection of Privacy Act*?
A: They are two separate processes. This will not affect how the Freedom of Information and Protection of Privacy is accessed today.

Q21 Is this different from Administrative Records Management System (ARMS) and Operational Records Systems (ORS) records systems and retention schedules?
A: Yes, Government Information Protection Classification Security labels are applied based on the sensitivity of the contents in a document or an email. These labels provide the ability to apply security controls based on classification labels. Records Management Classifications are applied based on the function of the record. Records Management Classifications come from an approved ARMS or ORS which provide a retention and disposal classification to the record and are a requirement for SBP to be compliant according to legislation.

Q22 Who should I contact if I have any questions regarding this tool?
A: For any questions about the GIP tool, please contact the ITD Service Desk.