Data and Information Security Classification Label Exception Guidance

Background

Implementation of the Data and Information Security Classification (DISC) Standard, originally developed in 2011, is the first step in ensuring the integrity, availability, sensitivity, and value of content. The DISC levels align with the security classification levels established by the Government of Canada and support data and information sharing across jurisdictions.

In M365, a security classification label (Protected A) will automatically be applied to all documents created or modified in Microsoft applications (Outlook, Word, Excel, PowerPoint, etc.). The DISC Standard requires an examination of both content and context when determining the correct security classification label that is to be applied. M365 allows users to select the appropriate security classification label at their own discretion—if a user does not actively select one, the application will automatically apply Protected A.

There may be specific circumstances in which an exception for applying a security classification label is desired; these circumstances may include (but are not limited to):

- emails in certain business areas that frequently interact with the public and other external bodies; and
- specific types of content (e.g., legislation published by Queen's Printer).

Removing the security classification label does not negate legislative and policy-based obligations to manage content (e.g., the Records Management Regulation, Metadata Core Content Standard, DISC Standard).

NOTE: Security classification labels cannot be deliberately removed without first seeking approval from Enterprise Information Management. Users and/or business areas that remove security classification labels without approval are potentially accepting accountability of greater risk.

Obtaining an Exception from Enterprise Information Management

To request an exception, contact Enterprise Information Management (EIM). An email documenting the situation will be sufficient to obtain the exception in most cases; however, in the event EIM determines that the risks caused by the exception are significant, further collaboration and review may be necessary to ensure that risks are well understood by all stakeholders and accepted by the Information Controller.

For more information on the exceptions process, please refer to Appendix A – DISC Exceptions Process.

Considerations and Risks

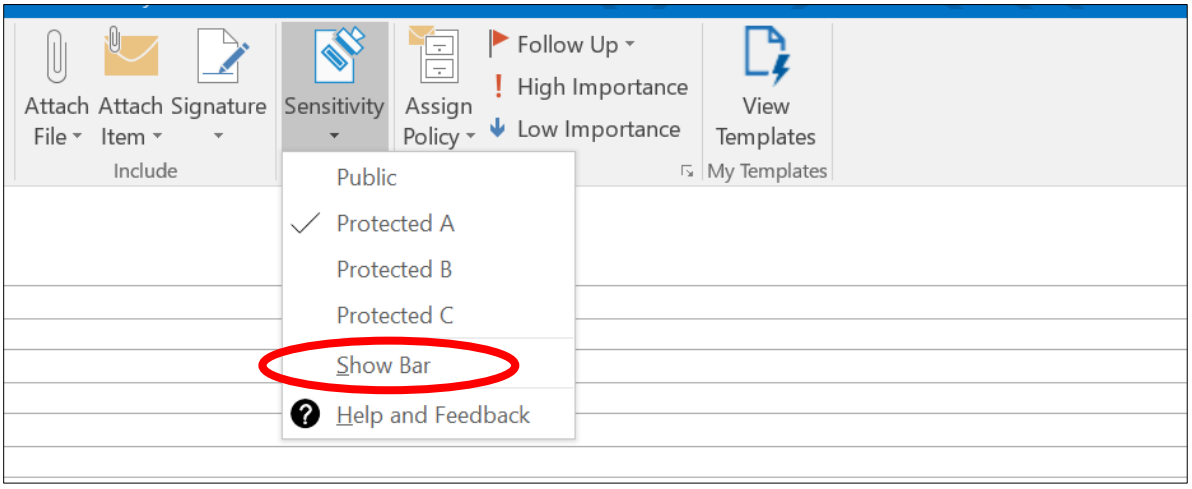
Before seeking an exception from EIM, it is recommended that business areas consider the following:

- Exceptions are not intended for entire systems or applications (e.g., removing security classification labels for all emails). A business area seeking an exception should consider establishing user-level processes that ensure consistent removal of security classification labels.
- Business areas that have received an exception are still subject to the DISC Standard, and must manage content appropriately (e.g., Protected B content must be maintained in a system that can support the management of Protected B content); refer to the DISC Guideline for additional information.
    - Alternatives to document labelling include (but are not limited to):
        - metadata;
        - secure fields in a document (e.g., Protected C columns in a Protected A spreadsheet); and/or
        - secure systems and/or applications (e.g., a SharePoint site classified as Protected A).
- An exception to applying the security classification label is not an exception from information management obligations.
- By obtaining an exception, the business area is explicitly assuming any risk and responsibility for non-compliance.
    - Consequences of non-compliance with security classification could result in damage to the Government of Alberta's reputation, loss of government content, exposure of Albertans to harm and/or incurrence of unnecessary costs.
    - Legislated disciplinary action (i.e., *Public Service Act*) may be taken, depending on the severity of non-compliance.
- Protected A as a default security classification label mandates a level of obligation on the part of the user to manage the associated content appropriately.
    - Using Protected A as a default label is based on experience with past breaches where there was confusion regarding which content may be disclosed to third parties—these breaches are discussed in OIPC reports F2016-IR-01 and F2019-IR-01.

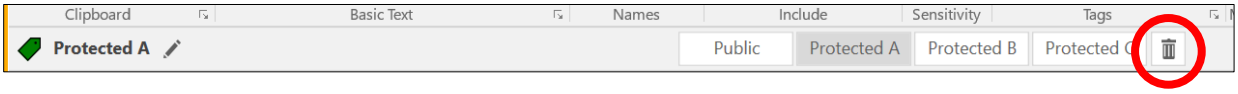
Removal of Security Classification Label

The process detailed below is applicable to Outlook, Word, Excel, and PowerPoint. The example images were taken from Outlook, but the process is identical across all four.

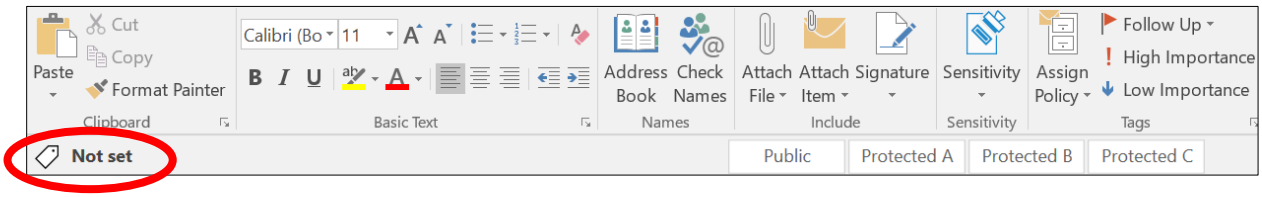
1. Obtain exception from EIM.
2. Establish a process (or processes) to ensure this exception is implemented consistently in the business area.
3. To remove the security classification label, click on the **Sensitivity** button. From the drop-down menu, click on **Show Bar**.



4. The Sensitivity bar should now be visible below the Message ribbon. Click on the trashcan icon (to the right of **Protected C**) to remove security classification.



5. Once security classification has been removed, the sensitivity tag at the left of the screen will say **Not set**.



6. Because exceptions are not granted at the system and/or application level, this process will need to be repeated every time content is modified and/or created.

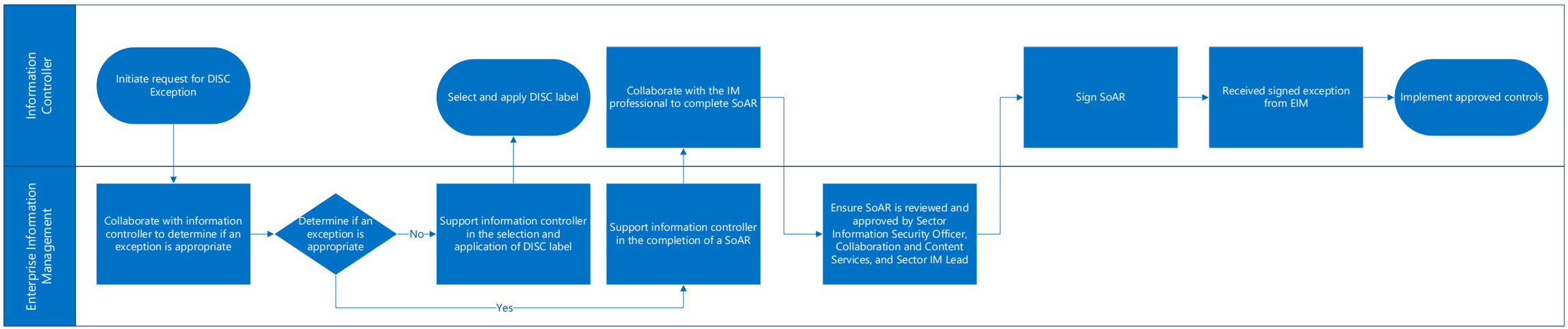
Classification: Public

Contacts

For more information regarding:

- The M365 project, please consult the Exchange Online Migration SharePoint or contact the M365 team.
- Security classification, please consult the Data and Information Security Classification Standard or contact Enterprise Information Management.
- Security classification for specific information types (e.g., whether an email should be classified as Public or Protected B), please contact your supervisor; collaboration with the appropriate Senior Records Officer may be necessary.

Appendix A: DISC Exceptions Process



https://www.alberta.ca/enterprise-information-management.aspx
September 2021

Classification: Public