



Government of Canada
Privy Council Office

Gouvernement du Canada
Bureau du Conseil privé

STANDARD ON THE SECURITY OF CABINET CONFIDENCES

APRIL 2024

Table of Contents

1. Effective Date.....	1
2. Application.....	1
3. Statement.....	1
3.1 Objectives.....	1
3.2 Expected Results.....	1
4. Requirements	2
4.1 Application of Marking, Consultations and Categorization	2
4.2 Access – Need-to-know, Clearance and Additional Controls	3
4.3 Handling, Transmission and Travel.....	4
4.4 Retention and Destruction.....	5
4.5 Unauthorized disclosure.....	5
5. References.....	6
6. Enquiries.....	7
ANNEX A – ASSESSMENT AND CATEGORIZATION EXAMPLES.....	8

1. Effective Date

1.1 This Standard on the Security of Cabinet Confidences (hereinafter “the Standard”) takes effect on April 1, 2024¹ and must be read in conjunction with the 2024 Privy Council Office Policy on the Security of Cabinet Confidences.

1.2 At a minimum, a review of the Standard is to be initiated within twenty-four (24) months of its effective date.

2. Application

2.1 The Standard applies to all Departments and agencies that deal with Cabinet Confidences, including the Privy Council Office as the lead security agency responsible to establish the policy direction for the security of Cabinet Confidences.

3. Statement

3.1 Objectives

3.1.1 The objectives of this Standard are to:

- Ensure that information identified as Cabinet Confidences is appropriately protected and safeguarded from the time it is marked as a Cabinet Confidence and that those protection measures continue to apply for as long as the information remains a Cabinet Confidence.
- Enable greater flexibility within Departments when drafting Cabinet Confidences and consulting on information that will become part of Cabinet Confidences.

3.2 Expected Results

3.2.1 The expected results of this Standard are:

- Documents identified as “Confidence of the King’s Privy Council” are assessed, categorized and subsequently handled and safeguarded in a consistent manner across the Government of Canada to ensure that they remain strictly confidential and are only shared with those who need to know.
- Allegations of leaks and breaches, as well as security events or incidents involving Cabinet Confidences, are reported and investigated in a timely manner.

3.2.2 While this Standard contemplates that Cabinet Confidences can be found in documents with varying security categorizations, nothing in this Standard should be construed as minimizing the importance of protecting Cabinet Confidentiality. Information that is a Cabinet Confidence must be kept confidential to the Government of Canada, limited to those with a need-to-know and cannot be disclosed outside the Government of Canada.

¹ Departments and agencies have a twelve-month period (until March 31, 2025) to implement the Policy.

4. Requirements

4.1 Application of Marking, Consultations and Categorization

4.1.1 The Cabinet Confidence designation will be based on the context in which the information will be presented and used, and is most usually meant to identify information that will support Cabinet discussions and decisions.

- If a document, in its early draft form, amounts to a Cabinet Confidence it should be marked as such.
- The writer must determine if the document they are creating contains information that is a Cabinet Confidence, based on factors such as the information's proximity to the Cabinet decision-making process, the purpose for which the document was created, and its intended destination.
- The writer must apply the marking of "Confidence of the King's Privy Council" if the information or document is intended to present proposals and recommendations to Ministers, or would reveal deliberations of Ministers.

4.1.2 The writer must apply the "Confidence of the King's Privy Council" marking, at a minimum, when the document has been signed or approved by the recommending Minister and transmitted for the purposes of deliberations or review by other Ministers.

4.1.3 When information in a document is designated as a Cabinet Confidence it must be marked "Confidence of the King's Privy Council" on the top right corner of each page, below the security categorization marking. The short form "Cabinet Confidence" can also be used.

- Departments and Agencies that maintain electronic marking systems for marking information with security categorization, caveat or release markings shall update these tools to include "Confidence of the King's Privy Council" marking or its short form.

4.1.4 Cabinet documents submitted to PCO's Operations, Cabinet Affairs need to have the consistent Cabinet Confidence marking of "Confidence of the King's Privy Council". Additionally, final Treasury Board documents submitted to the Treasury Board Submission Centre need to have the consistent Cabinet Confidence marking of "Confidence of the King's Privy Council."

4.1.5 When information in a document is designated as a Cabinet Confidence and consultations with third parties have been authorized, the information may be excerpted out and consultations carried out on the excerpted pieces, which would no longer, on their own without the context of the full document, be considered Cabinet Confidence and need to no longer bear the "Confidence of the King's Privy Council" marking. A version of a draft regulation or legislation that is prepared solely for consultation is not a Cabinet confidence. Where third party consultation is being considered, please ensure that pre-authorization is obtained.

4.1.6 Documents which bear the "Confidence of the King's Privy Council" marking are not automatically categorized at a certain security level; rather, they are to be assessed based on the information contained and are to be categorized as per the [TB Directive on Security Management - Appendix J: Standard on Security Categorization](#).

- The security categorization of a document which bears the "Confidence of the King's Privy Council" marking may change during its lifecycle.
- **ANNEX A** provides examples how documents marked "Confidence of the King's Privy Council" can be assessed and categorized.

4.2 Access – Need-to-know, Clearance and Additional Controls

4.2.1 Since Cabinet Confidences that have been disclosed outside of the Government of Canada can no longer be protected as such, they can only be disclosed outside of the Government of Canada with the prior authorization of the Prime Minister or Cabinet.

Furthermore, access to Cabinet Confidences is restricted to those individuals who have:

- a need-to-know; and,
- the appropriate security screening level and type to view the information contained in the document marked as Cabinet Confidence.

4.2.2 The following individuals are considered to have a need-to-know in relation to the development and approval of Cabinet Confidences:

- employees of the Government of Canada who are tasked with:
 - developing a policy or proposal(s) for their Minister that will be subject to collective ministerial decision-making, or for reviewing a policy or proposal(s) that are being prepared for another Minister; or,
 - developing material stemming from Cabinet Confidences such as but not limited to communications products, financial forecasts, parliamentary strategies.
- ministerial and departmental personnel supporting a Minister on a particular policy, proposal or issue that is the subject of, or may be the subject of, Cabinet discussion, or a discussion between individual Ministers;
- central agency (i.e. PCO, TBS, Department of Finance) employees who play a challenge function with respect to a specific policy or proposal, and help advance that policy or proposal as brought forward by departments or agencies of sponsoring Ministers;
- legal advisors providing advice relating to a particular policy, proposal or issue that is the subject of, or may be the subject of, Cabinet discussion or discussions between individual Ministers.

4.2.3 Employees of a Minister's riding office, members of the Minister's family and anyone without a need-to-know are not authorized to receive, handle, transmit, or access Cabinet Confidences, including electronic systems (e.g. use of E-Cabinet tablets, secure video conferencing) used to disseminate them.

4.2.4 Documents which bear the "Confidence of the King's Privy Council" marking are not *de facto* considered Canadian Eyes Only. An individual who is not a Canadian Citizen can access documents marked Cabinet Confidence if they have a need-to-know as defined in 4.2.2 above and the appropriate level of security status or clearance recognized by the Government of Canada.

4.2.5 Should a document marked Cabinet Confidence contain information that is Canadian Eyes Only or that falls under any other control systems, then the dissemination control should be added on the top right corner of each page below the categorization marking but above the Cabinet Confidence marking. The appropriate abbreviation version of the control system must be used.

4.3 Handling, Transmission and Travel

4.3.1 Individuals who have a need-to-know and have been security screened to the appropriate level to access Cabinet Confidences must abide by the following handling rules:

- use security equipment and safeguards approved for the level of sensitivity of the information to transport, transmit, store and dispose of Cabinet Confidences in paper-based or in electronic formats;
- mark Cabinet Confidence information with the requisite designation of “Confidence of the King’s Privy Council,” on the right top corner of every page of the document;
- handle sensitive information in restricted-access areas that are approved for its level of sensitivity;
- ensure that the information is not discussed with, viewed or overheard by unauthorized individuals; and,
- ensure that the information is discussed using tools and equipment that are approved for the level of sensitivity of the information being discussed.

4.3.2 Documents which bear the “Confidence of the King’s Privy Council” marking are to be stored based on their security categorization marking.

4.3.3 It is the responsibility of each department and agency to track copies (i.e. electronic, paper-based, or other) of documents marked as Cabinet Confidences and maintain the confidentiality and integrity of these documents through their lifecycle while under the purview of the department or agency (i.e. changes, access control, readings, transfers). It is also the responsibility of each department and agency to implement required tools and controls to ensure that Cabinet Confidences are only accessed by those who have a need to know and have been screened to the appropriate security level.

4.3.4 Documents marked as a Cabinet Confidence, either in paper or electronic format, are to be transmitted, transported and stored based on their security categorization, and subject to any handling and control systems.

- Individuals must ensure that they are using the appropriate tool for categorization of information and that the documents, either in paper or electronic format, are transmitted only to those who have a need to know using the approved transmittal means based on the categorization of the information.

4.3.5 Only Government of Canada approved and administered IT systems and devices are to be used to handle electronic versions of documents marked as Cabinet Confidence documents.

4.3.6 It is permissible to travel within Canada with documents, either in paper or electronic format, marked “Confidence of the King’s Privy Council “.

- The documents or electronic device must always be maintained in a positive control by an individual who has the need-to-know and a valid Government of Canada issued security screening level and type at the level required to view the information contained in the document marked “Confidence of the King’s Privy Council “.
- The document or electronic device must be carried in a container approved for the level of information contained in the document marked “Confidence of the King’s Privy Council“.
- If requested by a Canadian Air Transport Security Authority (CATSA) representative, the individual may open the container to show that it does not contain any threat items, while maintaining positive control of the contents.

- In the case on an electronic device inside a container, the holder may power on the electronic device to demonstrate that it is not threat item, but is not required go beyond the initial log-in screen to do so.
- For paper documents inside the container, the holder may display the outer folder or envelop marked 'Confidence of the King's Privy Council' to demonstrate that the documents are not a threat item, but are not required to show the actual document contents to do so.

4.3.7 To protect the security of the Cabinet process, the confidentiality of the information, and to ensure the personal safety of Government of Canada officials travelling abroad, travel outside of Canada with documents or information marked "Confidence of the King's Privy Council" is discouraged.

- If it is strictly necessary to travel outside Canada with these documents, security measures must be implemented to prevent unauthorized disclosure.
- These security measures may include the use of approved travel devices, approved secure containers and threat and risk evaluation based on the country travelled to.

4.4 Disclosure and Disposition

4.4.1 Cabinet Confidences must be protected for a period of twenty (20) years, unless stated otherwise.

- After the twenty (20) year period, the Cabinet Confidence designation can be removed and the document should be reviewed to assess if it contains any information that is protected or classified.
- If it does not, and if the document bears a protection or security categorization marking, the document can be downgraded in accordance with the injury test and the present-day injury that would result from an unauthorized disclosure of the material.

4.4.2 Governor in Council submissions, which include all Treasury Board Part B submissions, are protected as Cabinet Confidences. However, the disclosure of certain information in these submissions can be made to the public when it is approved by the Governor in Council. For Canada Gazette Part I submissions, certain Cabinet Confidence information is disclosed after the submission is approved for publication by a quorum of Ministers, which are usually Treasury Board members.

4.4.3 Discussion papers may be made public after a period of four (4) years after the decision in question has passed if the decision has not previously been made public. It is important to note that this is based on the time since the decision was made and not based on the number of years since the discussion paper was created. The Departmental Legal Services Unit should be consulted prior to any disclosure of discussion papers.

4.4.4 Documents which bear the "Confidence of the King's Privy Council" marking are to be disposed of in accordance with the LAC Act and any relevant LAC disposition authorization.

4.5 Unauthorized disclosure

4.5.1 The unauthorized disclosure of a Cabinet Confidence, either as a leak or a breach, can occur within any government department or agency. A leak or a breach may be intentional or accidental; both types of alleged leaks or breaches along with any security events/incidents

involving Cabinet Confidence must be reported to the Privy Council Office and looked into by the responsible department or agency.

4.5.2 When an alleged unauthorized disclosure of a Cabinet Confidence occurs, either intentional or accidental, it is the responsibility of the individual who uncovered the unauthorized disclosure to advise their departmental Chief Security Officer (CSO).

4.5.3 The departmental CSO will then inform the Privy Council Office CSO that an alleged unauthorized disclosure of a Cabinet Confidence has occurred.

4.5.4 PCO Security Operations will request that the department completes an injury impact assessment to determine the level of risk of the unauthorized disclosure (for example, national injury and/or personal injury). Additionally, PCO may provide assistance and guidance with the fact-finding and request known details of the unauthorized disclosure.

4.5.5 The departmental Chief Security Officer will ensure that a fact-finding exercise is conducted to uncover the source of the incident and to identify any recommendations to avoid re-occurrence. The source can range from human error, negligence, lack of knowledge, or a malicious agent.

4.5.6 The departmental CSO may also launch an administrative investigation, as they see fit.

4.5.7 Once the fact-finding or administrative investigation is completed, the vetted report approved by the senior management of the department or agency must be provided to PCO which will use the report as well as the completed injury impact assessment to prepare a written briefing to the Clerk of the Privy Council.

- PCO will determine if an unauthorized disclosure is to be reported to the Clerk as accidental; incidents that cause no injury, or a low-level of injury, may not be reported.

4.5.8 The Clerk may direct the PCO CSO to conduct a separate fact-finding and/or an administrative investigation. If that is the case, at the end of the fact-finding or investigation, an official report will be produced and forwarded to the departmental CSO. If the issue pertains to National Security, the report will also be countersigned by the National Security and Intelligence Advisor to the Prime Minister.

4.5.9 In the event that the evidence gathered during investigation points, according to the balance of probabilities, towards a known malicious actor, the case may be referred to the RCMP for a criminal investigation.

5. References

Legislation

- *Canada Evidence Act*
- *Access to Information Act*
- *Privacy Act*

Related policy instruments

- Treasury Board Policy of Government Security
- Privy Council Office Policy on the Security of Cabinet Confidences

6. Enquiries

6.1 Individuals from departments may contact the Privy Council Office, Security Operations by email at bcm-gca@pco-bcp.gc.ca for interpretation of this Standard.

ANNEX A – ASSESSMENT AND CATEGORIZATION EXAMPLES

CONTEXT

Examples are provided below to demonstrate how documents marked Cabinet Confidences could be assessed and categorized. The examples are solely meant to provide guidance and do not constitute set rules as Cabinet Confidences can be found in a wide range of documents, including presentation decks, briefing notes and emails.

Under the Standard, the presence of Cabinet Confidence information in a document **does not automatically require a certain security categorization**. However, documents containing Cabinet Confidences must be marked as such, and cannot be disclosed outside the Government of Canada.

Separately, each document or piece of information is to be assessed and categorized as per the [TB Directive on Security Management - Appendix J: Standard on Security Categorization](#). Departmental Security can provide advice and guidance on the appropriate type of tool and security measures to be observed based on the categorization of a document.

