Corporate Privacy Impact Assessment for

Use of Third-Party Applications and Tools to Maintain Operations During COVID-19 Emergency

Part 1 – General

Name of Ministry:	Ministry of Citizens' Services		
PIA Drafter:	Cole Lance		
Email:	Cole.Lance@gov.bc.ca	Phone:	**778 698-5837**
Program Manager:	**Quinn Fletcher**		
Email:	Quinn.Fletcher@gov.bc.ca	Phone:	**778 698-5849**

1. Description of the Initiative

The COVID-19 pandemic demands a shift in delivering provincial government services and communicating necessary information to the citizens. Ministries will be leveraging available technologies in order to most efficiently continue service delivery and communication during a time of rapid change and public health emergency.

The use of available technologies to meet this demand requires digital tools that may be hosted outside of Canada. Ministerial Order #M085 (The MO) authorizes the disclosure of personal information outside of Canada under section 33.1(3) of *The Freedom of Information and Protection of Privacy Act* (FOIPPA). For context, section 33.1(3) allows the Minister of Citizens' Services to allow, by order, the disclosure of personal information outside of Canada under a provision of section 33.2 of FOIPPA in specific cases or specified circumstances. This order is subject to any restrictions or conditions that the minister considers advisable.

There are conditions on this MO concerning the disclosure as a result of using third-party applications and tools. The exact conditions are noted in the MO; however, generally the third-party tools or applications should be only used in these circumstances:

a. The third-party tools or applications are being used to support and maintain the operation of programs or activities of the public body or public bodies.
b. The third-party tools or applications support public health recommendations or requirements related to minimizing transmission of COVID-19 (e.g. social distancing, working from home, etc.)
c. Any disclosure of personal information is limited to the minimum amount reasonably necessary for the performance of duties by an employee, officer or minister of the public body.

In addition, the MO specifically notes that the head of the public body must be satisfied that the application has reasonable security measures and that the public body must manage and maintain records according to other applicable legislation, such as the *Information Management Act.*

The intent of this PIA is to stand as, and set out, a compliance framework. This PIA does not contemplate any new processes or operations, but is rather about the tools newly needed to support current operations and processes. The Ministerial Order will ensure that the authorities are in place for any (new) disclosures outside of Canada as a result of using a new application or tool. These new authorities therefore shift the focus and need for assessment predominantly to ensuring reasonable security. Additionally, if security measures are reasonable, most other risks are related to ensuring clear communication of any risks/appropriate use to end-users. This PIA will therefore ensure that the immediate legislated need for an assessment is completed, and that resources are appropriately focussed on targeted guidance and iterative review of tools that government employees are using/intending on using.

Guidance materials will be appended to this PIA, on an iterative, ever-green basis. As use of tools matures, the Privacy, Compliance and Training Branch will consider development of stand-alone PIAs for specific, broadly used tools. Otherwise, efforts to communicate appropriate use of third-party applications and tools will be either logged or attached in this PIA (see Appendices).

2. Scope of this PIA

This assessment applies to any application, technology or method leveraged by Ministries to continue adequate service delivery, to collaborate, and communicate information while dealing with the COVID-19 pandemic.

The intent of this PIA is to ensure that during government's response to the COVID-19 pandemic, that resources are focussed on highly nimble and efficient assessments of tools and applications. Human health and safety is of the utmost concern and administration of privacy requirements should accommodate this, where possible.

3. *Related Privacy Impact Assessments*

N/A

4. Elements of Information or Data

The following list is not presumed to be comprehensive but general.

Personal information related to necessary communication methods: Streamed video and sound, contact information (both personal and business), tombstone information to confirm identities as required.

Personal information related to necessary service delivery. Disclosure of personal information should be limited to the minimum amount reasonably necessary for the performance of duties by an employee. Program areas should consider what personal information is needed to get the job done and only include that information in the application or tool.

Note: It is important to note that the MO is tied to disclosure authorities under s.33.2(a) and (c) specifically. This means that the expectation on ministry employees is that they are not disclosing more personal information or disclosing information to new parties who would not normally be privy to it, but rather, that these routine disclosures are happening in a different venue than would otherwise be considered. For example, in the case of a social worker and a client, that client's information will not be shared with more people, however, the conversation between the client and the social worker may now occur via a third-party application (for the duration of the MO).

Part 2 – Protection of Personal Information

5. Storage or Access outside Canada

Information will be stored within Canada where possible. If not possible, information will be stored outside of Canada under section 30.1(b) of FOIPPA as a result of the MO concerning the COVID-19 emergency and only for the duration of the COVID-19 emergency as specified in the MO.

Where required, information will be stored on the applications or tools, however, ministries are encouraged to not store information. Further, any information stored on these applications and tools will be removed as soon as is reasonably possible once the order is rescinded.

Records Management guidance will be provided to employees as needed and appropriate to ensure that they are supported in carrying out this requirement. Resources to this end will also be listed in the appendices.

6. Personal Information Flow Diagram and/or Personal Information Flow Table

This PIA only contemplates the specific uses of third-party tools and applications. Therefore, it is anticipated that all data flows that are in scope of this PIA will fall in scope of the Ministerial Order. The actual programs and operations that will be using these apps and tools are not in scope of this PIA and should look to program-level PIAs for assessment of the authorities related to those data flows.

Personal Information Flow Table			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	*Third-party application is used to communicate with individuals respecting COVID-19, support a public health response to the COVID-19 pandemic, and coordinate care in response to the COVID-19 pandemic.*	*Disclosure*	*33.1(3) by MO#085 [33.2(a), 33.2(c)]*
2.	*Personal information may be disclosed outside of Canada when Ministries use a third-party application for communication or collaboration.* *Third-party application or tool used to disclose personal information may also store information outside of Canada.*	*Use* *Disclosure* *Storage*	*32(a)* *33.1(3) by MO#085 [33.2(a), 33.2(c)]* *30.1(b)/33.1(3) by MO#085*
3.	*All other data flows will be reflective of data flows that exist within business areas and are therefore out of scope of this PIA. For example, if a social worker would normally chat with a client about their whereabouts, those same conversations will take place on third-party applications, without any additional disclosures to those described above (i.e. not disclosing to any new individuals).*	*Collection* *Use* *Disclosure*	*n/a* *n/a* *n/a*

7. Risk Mitigation Table

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Third-party application doesn't have sufficient security measures.*	• *As per the MO, the head of a public body must be satisfied that the application or tool has reasonable security in compliance with section 30 of FOIPPA before any disclosures are made.* • *Any tool or application used under this MO will have to undergo an analysis of its ability to meet this security requirement.* • *Ministry Information Security Officers should advise ministry employees as to which tools are appropriate given the sensitivity of the information that can be expected to be disclosed on each tool. For example, workplace engagement tools intended for team conversation (e.g. respecting organizational strategic planning) will not require the same level of security measures in place as those required for tools/implementations intended for client-based conversations (e.g. respecting case files).* • *Information Security Branch will send out security vulnerability notices to address potential technical vulnerabilities and ensure patches are delivered or downloaded.* • *Program areas should make an effort to monitor any changes made to the privacy*	*Low*	*Moderate*

		policy of the third-party application or tool they're using. The OCIO will be monitoring changes on the most commonly used tools. • *Program areas should refresh their staff on the standard information breach protocol in the event of a possible unauthorized disclosure or information incident. Furthermore, staff should be requested to review the Appropriate Use Policy and be reminded not to share unrelated personal information about themselves and others as the use of third-party applications and tools may involve the disclosure of PI outside of Canada.* • *Employees are required to be up to date on their mandatory Government training such as IM117: Information Management: Protection of Privacy, Access to Information and Records Management.* • *Information that is highly sensitive is generally managed within government systems (e.g. ICM, CORNET). The MO, and this PIA do not impact how employees use those systems to communicate/document/otherwise administrate their respective program activities.*		
2.	*Personal information is maintained on third-party*	• *As per the MO, Ministries will make all reasonable efforts to remove personal information from the third-party application as soon as is operationally*	*Low*	*High*

	applications or tools in perpetuity.	*reasonable and is retained and managed by the public body, as required by law.* • *The MO is active until June 30th. Pending any extensions or new Ministerial orders being signed, Ministries are aware of the MO expiry date and can plan the removal of personal information accordingly.* • *Communications regarding the MO have stated the end date of the MO. The MO Guidance that has been posted online and circulated broadly to stakeholders also clearly states requirements related to offboarding from the services and resources in the case that public bodies need further assistance.* • *Recordings, if required, will be saved on encrypted government LAN drives, with restricted password access. After transferring, any residual copies should be removed from the third-party application or tool as soon as possible.* • *During the COVID-19 pandemic response, the OCIO is holding daily calls with MCIOs and select staff, which provides a highly effective means of communicating to ministries any new information related to their use of third-party applications or tools.*		
3.	*Third-party application or*	• *Employees should be made aware of this possibility before signing up to use the*	*Low*	*Low*

	tool creates log of communications such as who was on what call, and when it happened. This could be personal work history information.	*third-party application or tool. Program managers could send this notification along with the invitation to use the application or tool.* • *Histories should be cleared where possible, and employees instructed to make use of clear-history functions as they offboard from these tools at the end of the ministerial order (or sooner).*		
4.	*Tools or applications are used in a way that is not secure*	• *As the leading tools begin to emerge, guidance will be developed as required in order to support responsible use of those tools/applications.* • *Ongoing communications efforts will be focussed on instructing employees on how to use tools appropriately.*	*Moderate*	*Low*
5.	*Employees will use tools not endorsed by security experts.*	• *The MO is being communicated and socialized through MCIOs, MPOs and MISOs. In this way, they will support and get ahead of demand within their ministries and drive users towards tools that are appropriate for the ministry's unique needs and data sensitivity.* • *Given the role of the OCIO and the pressing deadlines posed by COVID-19, ministries have been quick to query tools with OCIO before deployment. The OCIO is encouraging this positive behaviour with a steady stream of information on third-party tools and applications.*	*Moderate*	*Low*

8. Collection Notice

If your third-party application or tool is collecting personal information directly from individuals, you must ensure that all individuals involved are told the following:

1. The purpose for which the information is being collected
2. The legal authority for collecting it, and
3. The title, business address and business telephone number of an officer or employee who can answer questions about the collection.

OR

If your third-party application or tool will be used to disclosure personal information between public bodies. No collection notice is required as per section 27(3)(c).

Part 3 – Security of Personal Information

9. Please describe the physical security measures related to the initiative (if applicable).

N/A

10. Please describe the technical security measures related to the initiative (if applicable).

A Ministry must not disclose personal information as authorized by the MO unless the head of the Ministry is satisfied that the third-party application is reasonably secure in compliance with s. 30 of the Freedom of Information and Protection of Privacy Act.

Technical security measures will be assessed by Ministry Information Security Officers and/or Information Security Branch to ensure that it meets this test. For the purposes of this PIA, security assessments will not be required of tools where there is no use or disclosure of personal information is contemplated. Security assessments may still be otherwise required, per ministry guidelines, where information is not classified as public.

11. Does your branch rely on security policies other than the Information Security Policy?

As the tools that employees gravitate towards become clear, government will produce tool-specific guidance as needed. Guidance on the Ministerial Order has been published and

distributed to stakeholders and includes information about reasonable security and contact information should a public body require further assistance in this regard.

12. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Ministries should employ access controls such as role-based access or least privileges wherever possible. Conversations and communications will not be opened up to audiences that are broader than if the same conversations were occurring within Canada/on Canadian-based tools.

13. Please describe how you track who has access to the personal information.

Access tracking will vary by application. Ministries are encouraged to keep access logs in mind when evaluating applications for use as this feature may contribute to the assessment with respect to reasonable security.

Part 4 – Accuracy/Correction/Retention of Personal Information

14. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the ministry notify them of the update, correction or annotation?

If individuals contact the Ministry to update personal information, the Ministry must make a reasonable effort to update the personal information held by the third-party application or tool. If an update is not possible the Ministry must annotate the file to represent the requested change.

15. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

Yes, the information may be disclosed in relation to the ongoing public health emergency regarding COVID-19. These disclosures may result in direct affects to individuals by means of communication or service delivery.

16. If you answered "yes" to question 15, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

Information used for communication and service delivery relies on the accuracy of the program that collected and is using it. Program areas are reminded to make reasonable efforts to ensure

their personal information is accurate and complete. Further, information relating to decisions will be required to be ported to a more permanent storage location in order to meet retention requirements.

17. If you answered "yes" to question 15, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

Ministries will retain personal information used to make a decision for at least one year. The requirement on Ministries to make all reasonable efforts to remove personal information that is disclosed outside of Canada using a third-party application from the third-party application as soon as is operationally reasonable following the rescinding of the MO does not override this obligation.

Information relating to decisions will be required to be ported to a more permanent storage location in order to meet retention requirements.

Records management requirements have been communicated, at a high level, via a Ministerial Order guidance document. Additional guidance on records management will be reflected in the appendices.

Part 5 – Further Information

18. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No, any disclosures made under this MO involving third-party applications or tools will be temporary during the COVID-19 pandemic.

19. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

This PIA does not contemplate disclosures made under section 35 for research or statistical purposes.

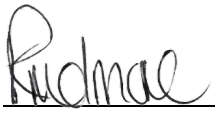
20. Will a personal information bank (PIB) result from this initiative?

Third-party applications and tools should not be used to store or establish PIBs.

Corporate Privacy Impact Assessment for

Use of Third-Party Applications and Tools to Maintain Operations During COVID-19 Emergency

Part 6 – Signatures

Matt Reed		April 15, 2020
Executive Director Privacy, Compliance and Training Branch Corporate Information and Records Management Office Ministry of Citizens' Services	Signature	Date
Kerry Pridmore		April 17, 2020
Assistant Deputy Minister and Chief Records Officer	Signature	Date

PCT will publish the ministry name, business contact details and a brief summary of the PIA to the Personal Information Directory (PID) as required by section 69(2) of FOIPPA.

Appendix A: Inventory of Mitigations

Item	Location/Distribution	Date
General guide: "Guidance on Ministerial Order 085 respecting disclosures during COVID-19 Emergency"	https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-privacy/resources/guidance_on_ministerial_order_085.pdf	April 2, 2020
General guide: "Cyber safety for mobile workers"	https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/information-security/cyber-safety_for_mobile_workers.pdf	April 14, 2020
Intranet threads on: • Workstations • Connecting • Conferencing Options • Confidential or Personal Information • Cyber security • Managing Records • Links • FAQs	https://gww.gov.bc.ca/groups/remote-work-tips-and-tricks	Updated routinely (by community and by SMEs)
General RM guide: "Bringing the Office Home"	https://gww.gov.bc.ca/groups/records-management-community/blogs/2020/0320/bringing-office-home	March 20, 2020
General RM guide: Managing Your Records Outside the Office"	https://www2.gov.bc.ca/assets/gov/british-columbians-our-governments/services-policies-for-government/information-management-technology/records-	March 19, 2020

	management/guides/managing_records_outside_the_office.pdf	
Zoom: Statement of Acceptable Risk (SoAR)	Information Security Branch, OCIO	April 10, 2020